



ADDRESSING DATA SECURITY GAPS IN DRUG MANUFACTURING: INSIGHTS  
FROM NIGERIA

Dissertation Manuscript

Submitted to UNICAF University in Zambia  
in partial fulfillment of the requirements  
for the degree of

Doctor of Philosophy (Ph.D.)

By Nnamdi Nwosu

May 2025

## Approval of the Thesis

### ADDRESSING DATA SECURITY GAPS IN DRUG MANUFACTURING: INSIGHTS FROM NIGERIA

This Thesis by Nnamdi Nwosu has been approved by the committee members below, who recommend it be accepted by the faculty of Unicaf University in Zambia in partial fulfillment of requirements for the degree of

Doctor of Philosophy

Thesis Committee:

Dr Hatem Trabelsi, supervisor

Dr Nathan Musonda, chair

Prof. Sunday Olusanya Olatunji, external examiner

Dr Saheed Yakub Kayode, internal examiner

## Abstract

### ADDRESSING DATA SECURITY GAPS IN DRUG MANUFACTURING: INSIGHTS FROM NIGERIA

Nnamdi Nwosu

Unicaf University in Zambia

The pharmaceutical industry's growing reliance on data-driven initiatives intensifies the risk of breaches involving proprietary formulations and patient information. Despite guidance from WHO and PIC/S, data security in pharmaceutical manufacturing, particularly in Nigeria, remains inadequate. This study examines data security gaps in both regulatory guidelines and operational practices within Nigeria's pharmaceutical sector. Previous research has focused on personal data protection, often overlooking business-critical data and the alignment between standards and practice in developing economies. To address this gap, a qualitative multiple-case study was conducted with 31 IT and cybersecurity professionals from five Nigerian pharmaceutical firms seeking WHO cGMP prequalification. Semi-structured interviews and a document analysis of three international guidelines enabled triangulation of regulatory and operational insights. Thematic and content analyses revealed recurring issues such as poor data classification, weak encryption, insufficient data recovery tests, and inadequate audit trails, factors that increase vulnerability to breaches and compromise data integrity. In response, the study proposes the PhIDS Model, a contextual data security model tailored to pharmaceutical manufacturing in low- and middle-income countries. This model contributes to global discourse on pharmaceutical data governance by highlighting the need for harmonized yet adaptable standards. It also emphasizes the importance of aligning local operational realities with regulatory expectations. Future research should explore the PhIDS Model's integration with technologies such as AI and industrial IoT to enhance data resilience in the sector.

## Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where stated otherwise by reference or acknowledgment, the work presented is entirely my own.

### AI Acknowledgment

I acknowledge my use of Chat GPT (<https://openai.com/chatgpt/>) to proofread Chapter 1 and Chapter 5 of my thesis. This action was completed on 18.02.2025. The prompts used included proofreading, correcting grammar, and checking punctuation for the text below.

### Copyright Page

I confirm that I retain the intellectual property and copyright of the thesis submitted. I also allow Unicaf University in Zambia to produce and disseminate the contributions of the thesis in all media forms known or to come as per the Creative Commons BY License (CC BY).

## Dedication

I dedicate this dissertation to Yahweh, who sits at the four corners of the universe and continually inspires me. I also dedicate this dissertation to my parents, Sunday and Justina Nwosu, whose unwavering love made this journey possible. I also dedicate this dissertation to my siblings—Ijeoma, Chidozie, Ngozi, Ezioma, and Eze—whose support has been invaluable. Finally, I dedicate this dissertation my beloved sons, Gilead and Bethel, and to my unborn baby, Eden.

## Acknowledgements

I express my sincere gratitude to the UNICAF School of Doctoral Studies, Center for Cyber Safety & Education, and Dr. Hatem Trabelsi, whose guidance has profoundly shaped this research.



## Table of Contents

List of Abbreviations .....	xviii
List of Tables .....	xxi
List of Figures .....	xxii
CHAPTER 1: INTRODUCTION .....	1
1.1 Statement of Problem .....	2
1.2 Purpose of the Study, Research Aims, and Objectives .....	4
1.3 Nature and Significance of the Study .....	6
1.4 Research Questions .....	8
CHAPTER 2: LITERATURE REVIEW .....	10
2.1 Theoretical/Conceptual Framework .....	14
2.1.1 Pharmaceutical Industry Good Manufacturing Practices .....	14
2.1.2 Data Governance and Data Integrity .....	15
2.1.3 Data Integrity Principles .....	16
Attributable. ....	16
Legible. ....	17
Contemporaneous. ....	17
Original. ....	17
Accurate. ....	17
2.1.4 Management Control Theory .....	18
2.1.5 Data Security .....	20
2.2 Classification and Security Considerations of Data Assets .....	22
2.2.1 Hierarchy of Data .....	22
2.2.2 Scope of Data Asset .....	23
Traditional Data. ....	24
Big Data. ....	24
2.2.3 Data Location and States .....	25
2.2.4 Data Types, Threats, and Risks .....	25
Intellectual Property .....	26
Legal. ....	26
Strategic Planning. ....	27
Sales. ....	27
Customer. ....	28
Marketing. ....	28
Operational. ....	28

Financial.....	28
Human Resource.....	29
Personal.....	29
Personally Identifiable Information.....	29
Country/Government.....	29
Information Technology.....	29
2.2.5 Data Security Threats and Risks in Pharmaceuticals .....	30
Unauthorized Alteration.....	30
Unauthorized Disclosure.....	33
Unauthorized Denial of Use.....	36
2.3 Governance and Management of Information Technology .....	39
2.3.1 Information Technology Governance.....	40
Information Technology Governance Models.....	40
Information Technology Governance Implementations .....	43
Information Technology Governance and Management.....	44
2.3.3 Enterprise Governance of IT .....	45
2.3.4. Enterprise Governance of IT Frameworks .....	47
Enterprise, IT-related, and Alignment Goals.....	48
Enablers and Governance Components.....	52
Performance Outcome.....	54
2.4 Data Life Cycle, Management, and Governance .....	58
2.4.1 Manufacturing Product Life Cycle and Big Data.....	58
Concept Generation .....	58
Product Design.....	60
Raw Material Procurement .....	60
Manufacturing.....	60
Transportation.....	60
Sales.....	60
Utilization.....	61
After-sales Service.....	61
Recycle/Disposal.....	61
2.4.2 Data Life Cycle.....	61
Data Collection.....	62
Data Storage.....	62
Data Processing.....	62

Data Visualization.....	63
Data Transmission. ....	63
Data Applications.....	63
2.4.3 Data Management.....	64
Data Creation. ....	68
Data Storage.....	69
Data Usage. ....	69
Data Transmission. ....	70
Data Sharing.....	70
Data Destruction. ....	70
2.4.4 Data Governance .....	70
Data Governance Framework. ....	72
Data Governance Mechanisms. ....	72
Data Decision Domains .....	75
Organizational Scope of Data Governance.....	79
Data Governance Consequences.....	79
Data Creation. ....	80
Data Storage.....	80
Data Usage. ....	80
Data Transmission. ....	80
Data Sharing.....	80
Data Destruction. ....	80
2.5 Data Security .....	82
2.5.1 Layers of Security and Data Security .....	82
Human Layer. ....	83
Perimeter Security Layer. ....	84
Network Security Layer.....	84
Endpoint Security Layer. ....	84
Application Security Layer.....	84
Data Security Layer. ....	84
Mission Critical Assets. ....	85
2.5.2 Data Security Models .....	85
Confidentiality, Integrity, and Availability Model. ....	86
Parkerian Hexad Model. ....	89
The Five Pillars of Information Assurance Model .....	90

International Organization for Standardization Model .....	91
The Traditional 4-Steps Model and the Pentagon of Trust Model .....	91
The Evolutionary Circles of Information Security Model.....	92
2.5.3 Data Security Management and Governance .....	94
Risk Assessment .....	94
Data Security Policy and Standards.....	95
Control Objectives and Controls for Data Security.....	96
Data Security Controls for Cyber Defense.....	100
Data Security Auditing.....	111
Data Security Officer.....	112
2.5.4 Data Leakage and Prevention .....	114
Data Loss Prevention.....	116
Data Loss Prevention Solutions.....	116
Data Loss Prevention Solution Deployment.....	117
Data Loss Prevention Methods.....	118
2.5.5 Data Security in Drug Manufacturing: Gaps in Empirical Literature .....	121
2.6 Nigeria's Pharmaceutical Industry .....	123
2.6.1 Characteristics .....	124
Industry Regulation.....	124
Low Entry Barrier.....	133
Highly Fragmented, Low-capacity Utilization.....	133
Mergers and Acquisitions.....	134
Government Interventions for Sustained Industry Growth.....	134
2.6.2 Challenges and Trends.....	135
Substandard and Falsified Medicinal Products.....	136
Weak Regulatory Systems.....	137
Scientific and Technological Advancement.....	138
Poor Infrastructure.....	140
Supply Chain Disruptions.....	140
World Health Organization Prequalification.....	141
2.7 Summary .....	142
CHAPTER 3: RESEARCH METHODS AND DATA COLLECTION .....	146
3.1 Introduction .....	146
3.2 Research Approach and Design .....	149
3.2.1 Research Approach.....	149

3.2.2 Case Studies.....	153
3.3 The Triangulation Strategy .....	154
3.4 Triangulation Methods for Data Collection .....	159
3.4.1 Document Analysis.....	160
3.4.2 Qualitative Interviews.....	163
3.5 Sampling Design .....	165
3.5.1 Sampling Strategy.....	166
3.5.2 Sample Characteristics and Size.....	171
Participating Organizations.....	171
Subject Matter Experts.....	171
Institutional Documents.....	172
3.6 Research Tools .....	173
3.7 Study Procedures and Ethical Assurances .....	174
3.7.1 Ethical Assurances.....	175
Scientific Validity.....	175
Gatekeeper's Permission and Participant's Consent.....	177
Informed Consent and Participant's Rights .....	177
Data Collection and Management.....	178
Data Dissemination.....	178
3.7.2 Study Procedures .....	179
Literature Search and Review .....	179
Research Methodology and Design .....	179
Ethical Approval .....	181
Research Participant Selection.....	181
Data Collection .....	181
Data Validation, Analysis, and Interpretation.....	182
Reporting and Dissemination.....	182
3.8 Triangulation Methods and Software for Data Analysis.....	182
3.8.1 Selected Data Analysis Method.....	183
Familiarization.....	185
Establishing a Thematic Framework.....	185
Indexing.....	185
Charting.....	185
Mapping and Interpretation.....	185
3.8.2 Excluded Approaches .....	186

3.8.3 Software for Qualitative Data Analysis.....	188
3.9 Data Collection and Analysis.....	189
3.9.1 Data Collection and Qualitative Content Analysis.....	189
Decontextualization. ....	190
Recontextualization.....	190
Categorization and Compilation. ....	191
3.9.2 Data Collection and Thematic Analysis .....	191
Collect the Interview Data. ....	191
Transcribe the Audio Recordings. ....	192
Transfer the Text from Word Documents to Excel Spreadsheets.....	193
Code in Excel.....	193
Sort the Coded Interviews.....	193
Transfer Quotes and References to Word.....	194
Analyze Interview Data. ....	194
Summary .....	194
CHAPTER 4: DISCUSSION OF RESEARCH FINDINGS .....	197
4.1 Reliability and Validity of Data .....	198
4.2 Trustworthiness of Data .....	199
4.2.1 Confirmability .....	200
4.2.2 Credibility .....	202
Triangulation.....	202
Member Checks. ....	203
Prompts, Probes, and Iterative Questioning.....	204
Reflexivity and Reflective Commentary .....	204
Debriefing Sessions .....	205
4.2.3 Dependability.....	205
4.2.4 Transferability .....	206
4.3 Results and Evaluation of Findings.....	207
4.3.1 Data Security Measures and Gaps in Reference Guidelines .....	212
Data Management Process.....	215
Data Inventory .....	215
Data Flows .....	216
Data Access Control Lists.....	216
Role-based Access Control .....	217
Data Retention .....	218

Data Backup.....	218
Data Recovery.....	219
Data Disposal.....	219
Service Provider Logs.....	220
Monitor Service Providers .....	221
Data Encryption .....	221
Unspecified Elements.....	222
4.3.2 Data Security Gaps in Drug Manufacturing Practices.....	223
Challenges in Data Classification and Loss Prevention .....	225
Ineffective Data Risk Assessment .....	226
Immature Tech-centric Data Management.....	227
Data Ownership Assumptions and Unchecked Data Sharing.....	228
Data Governance Challenges and Risks in a Globally Distributed Environment.....	230
Deficiencies in Software Integrity Assessment .....	233
Inconsistencies in Network Security Measures and Monitoring Practices.....	234
USB Security Risks.....	236
Challenges System Validation and Configuration Control.....	237
Data Resilience Challenges in Modern IT Ecosystems.....	238
Data Privacy Vulnerabilities in External Systems.....	243
Data Integrity Gaps in Operations and Supply Chain.....	244
Inadequate Data Security Monitoring.....	246
Challenges Prioritizing Data Security and Response.....	247
4.3.3 Alignment between Guidelines and Practices .....	250
Data Management Process.....	253
Data Inventory.....	253
Data Flow.....	253
Data Access Control Lists.....	254
Role-based Access Control.....	254
Data Retention.....	254
Data Backup.....	254
Data Recovery Process.....	254
Data Recovery Test.....	254
Protection of Recovery Data.....	254
Isolation of Data Recovery Instance.....	255
Data Disposal.....	255

Service Provider Logs.....	255
Monitoring of Service Providers.....	255
Decommissioning of Service Provider. ....	255
Data Classification. ....	256
Data Loss Prevention. ....	256
Data Encryption. ....	256
Segmentation of Data Processing and Storage. ....	256
Service Provider Logs.....	256
4.3.4 Root-Cause Analysis of Data Security Gaps.....	257
Summary .....	258
CHAPTER 5: IMPLICATIONS, RECOMMENDATIONS, AND CONCLUSION.....	267
5.1 Implications .....	270
5.1.1 Implications of Data Security Gaps in Reference Guidelines.....	270
5.1.2 Implications of Data Security Gaps in Drug Manufacturing Practices.....	271
Challenges in Data Classification and Loss Prevention .....	271
Ineffective Data Risk Assessment .....	272
Immature Tech-centric Data Management Process. ....	274
Data Ownership Assumptions and Unchecked Sharing. ....	275
Data Governance Challenges and Risks in a Globally Distributed Environment .....	275
Deficiencies in Software Integrity Assessment. ....	276
Inconsistencies in Network Security Measures and Monitoring Practices. ....	276
USB Security Risks.....	277
Challenges in System Validation and Configuration Control.....	277
Data Resilience Challenges in Modern IT Ecosystems. ....	277
Data Privacy Vulnerabilities in External Systems .....	278
Data Integrity Gaps in Operations and Supply Chain Security. ....	278
Inadequate Data Security Monitoring.....	279
Challenges in Prioritizing Data Security and Response .....	279
5.1.3 Alignment between Guidelines and Practices .....	279
5.2 Recommendations for Application.....	281
5.2.1 International Health Organizations, Industry Consortia, NAFDAC .....	281
5.2.2 Nigerian Drug Manufacturing Organizations.....	282
Data, Software, Firmware Integrity Controls. ....	284
Data Availability Controls. ....	292
Third-Party Data Security Controls. ....	293



Data Protection Controls.....	295
5.2.3 Standards-Based Validation and Scalability of the PhIDS Model .....	298
5.2.4 Model Validation through Pilot Implementation and Refinement .....	301
Pilot Implementation in a Select Pharmaceutical Organization. ....	303
Simulation of Use-Case Scenarios.....	303
Iterative Refinement and External Consultation.....	303
5.2.5 PhIDS Model Implementation Strategy .....	303
5.2.6 National Culture and PhIDS Model Implementation .....	306
Power Distance. ....	306
Individual versus Collectivism. ....	307
Masculinity versus Femininity.....	308
Uncertainty Avoidance. ....	309
Long-term versus Short-term Orientation.....	309
Indulgence versus Restraint. ....	309
5.3 Recommendations for Future Research .....	310
5.4 Conclusions .....	313
5.4.1 Implications for Theory and Practice .....	313
5.4.2 Contribution to Knowledge .....	316
5.4.3 Closing Statement.....	317
REFERENCES.....	318
APPENDICES.....	379
Appendix A: Questionnaire Template for Demographic Information .....	379
Appendix B: Interview Guide with a Proposed Sequence .....	379
Appendix C: University Research Ethics Committee Provisional Approval.....	383
Appendix D: University Research Ethics Committee Final Approval .....	391
Appendix E: Gatekeeper Letter Template.....	392
Appendix F: Informed Consent Form Template .....	393

## List of Abbreviations

AAI - Align, Plan and Organize

AI – Artificial Intelligence

APO - Align, Plan and Organize

BAI - Build, Acquire and Implement

BIOS - Basic Input Output System

CAQDAS - Computer-Assisted Qualitative Data Analysis Software

CD – Compact Disk

CDMO - Contract Development and Manufacturing

CET - Common External Tariffs

cGMP - Current Good Manufacturing Practices

CIA - Confidentiality, Integrity, and Availability

CMMI - Capability Maturity Model Integration

COBIT - Control Objectives for Information Technologies

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CSCs - Cloud Service Clients

CSPs - Cloud Service Providers

CTD - Common Technical Document

DEG - Diethylene glycol

DoS - Distributed Denial of Service

DDoS - Distributed Denial of Service

DLP - Data Loss Prevention

DLPSs - Data Loss Prevention Solutions

DPCO - Data Protection Compliance Organizations

ECOWAS - Economic Community of West African States

EDM - Evaluate, Direct and Organize

EPP - Endpoint Protector

GDPR - General Data Protection Regulation

GenAI - Generative Artificial Intelligence

GL - General Ledger

GMP – Good Manufacturing Practices

HIPPA - Health Insurance Portability and Accountability Act

HIV/AIDS - Human Immunodeficiency Virus/ Acquired Immunodeficiency Syndrome

ICS - Industrial Control System

IPS - Intrusion Prevention System

IT - Information Technology

ITIL - Information Technology Infrastructure Library

IoT - Internet of Things

IIoT - Industrial Internet of Things

MCT – Management Control Theory

MEA - Monitor, Evaluate and Assess

MHRA - Medicines and Healthcare products Regulatory Agency

ML - Machine Learning

NAC - Network Access Control

NAFDAC - Nigeria’s National Agency for Food and Drug Administration

NIST - National Institute of Standards and Technology

NITDA - National Information Technology Development Agency

PCN - Pharmacist Council of Nigeria

PMG-MAN - Pharmaceutical Manufacturing Group of Manufacturers Association of Nigeria

PO - Plan and Organize

RPO - Recovery Point Objective

RTO - Recovery Time Objective

R&D – Research and Development

SLA - Service Level Agreement

SOX - Sarbanes-Oxley Act

TLS - Transport Layer Security

TTPs - Tactics, Techniques, and Procedures

UML - Unified Modeling Language

UREC - University Research Ethics Committee

USB - Universal Serial Bus

WHO - World Health Organization

## List of Tables

<b>Table 1</b> Data Assets of the Manufacturing Product Life Cycle .....	59
<b>Table 2</b> Comparison of Data Life Cycle Stages across Different Models .....	64
<b>Table 3</b> Secure Data Management for Manufacturing .....	69
<b>Table 4</b> Data Decision Domains and Governance Mechanisms .....	78
<b>Table 5</b> Secure Data Management and Governance in Manufacturing .....	81
<b>Table 6</b> Relevance and Impact of Data Security Models in Pharma.....	93
<b>Table 7</b> Distinction between Data Protection and Data Privacy .....	138
<b>Table 8</b> Demographics of Respondents.....	210
<b>Table 9</b> Health Authorities' Guidance Documents Reviewed .....	211
<b>Table 10</b> Evaluation of Data Management Guidelines based on Data Security Controls.....	212
<b>Table 11</b> Evaluation of Data Management Practices in terms of Data Security Controls ....	223
<b>Table 12</b> Alignment of Guidelines and Practices in terms of Data Security Controls.....	250
<b>Table 13</b> Implications of Data Security Gaps in Drug Manufacturing Practices.....	274
<b>Table 14</b> Solutions to Data Security Gaps in Drug Manufacturing Practices .....	285
<b>Table 15</b> Policy Mapping Aligned PhIDS and Manufacturing Data Life Cycle .....	286
<b>Table 16</b> PhIDS Model Validation and Scalability .....	302
<b>Table 17</b> Implementation Phases of the PhIDS Model .....	304
<b>Table 18</b> Ranking of Nigeria's Cultural Dimensions .....	308

## List of Figures

<b>Figure 1</b> Theoretical Framework.....	14
<b>Figure 2</b> Concept Map of Theoretical Framework.....	21
<b>Figure 3</b> Relationship between Data, Information, Knowledge, and Wisdom .....	22
<b>Figure 4</b> Categorization of Data.....	23
<b>Figure 5</b> Data Locations (States).....	26
<b>Figure 6</b> Data Types .....	27
<b>Figure 7</b> Classification of Data Invasion.....	31
<b>Figure 8</b> Evolution of IT Governance Models .....	42
<b>Figure 9</b> IT Governance Subsystems .....	43
<b>Figure 10</b> Enablers of IT Governance.....	45
<b>Figure 11</b> (a) COBIT 5 Goals and (b) COBIT 2019 Goals Cascades.....	49
<b>Figure 12</b> COBIT Reference Model.....	50
<b>Figure 13</b> COBIT 2019 Core Model.....	51
<b>Figure 14</b> (a) COBIT 5 Enablers and (b) COBIT 2019 Governance Components.....	53
<b>Figure 15</b> Capability Levels for Processes.....	54
<b>Figure 16</b> Metrics for (a) Enterprise Goals, (b) IT-related Goals, and (c) Managed Risk.....	56
<b>Figure 17</b> Metrics for (a) Enterprise Goals, (b) Alignment Goals, and (c) Managed Data ....	57
<b>Figure 18</b> Data Governance Mechanisms .....	73
<b>Figure 19</b> Data Decision Domains .....	75
<b>Figure 20</b> Layers of Security.....	83
<b>Figure 21</b> Data Security Models and Concepts.....	87
<b>Figure 22</b> Major Cybersecurity Frameworks .....	88
<b>Figure 23</b> COBIT 5 Data Security Governance Practices.....	97
<b>Figure 24</b> Centre for Internet Security Critical Security Controls .....	102

<b>Figure 25</b> Structure of a Critical Security Control.....	104
<b>Figure 26</b> Data Security Controls Framework for Cyber Defence .....	105
<b>Figure 27</b> Regulatory Framework of Nigeria's Pharmaceutical Industry and Data .....	125
<b>Figure 28</b> Research Philosophy and Approach.....	150
<b>Figure 29</b> Triangulation Strategy .....	157
<b>Figure 30</b> Selected Research Methods .....	159
<b>Figure 31</b> Sampling Strategy Considerations.....	169
<b>Figure 32</b> Category of Ethical Principles.....	176
<b>Figure 33</b> Study Procedures and Ethical Assurance .....	180
<b>Figure 34</b> Framework Analysis Stages .....	184
<b>Figure 35</b> Qualitative Content Analysis Process.....	190
<b>Figure 36</b> Thematic Analysis Process.....	192
<b>Figure 37</b> Coding List for Interview Data.....	193
<b>Figure 38</b> Sorted Interview Data.....	194
<b>Figure 39</b> Constructs of Data Trustworthiness .....	201
<b>Figure 40</b> Distribution of Degree of Guideline/Practice Alignment.....	253
<b>Figure 41</b> Root Causes of Data Security Gaps.....	258
<b>Figure 42</b> Implications of Data Security Gaps in Guidelines .....	273
<b>Figure 43</b> Implications of Standards-Practices Misalignment on Data Security .....	280
<b>Figure 44</b> Topic-specific Policies for Secure Data Management .....	289
<b>Figure 45</b> The PhIDS Model.....	290
<b>Figure 46</b> Data, Software, and Integrity Controls of the PhIDS Model.....	291
<b>Figure 47</b> Data Availability Controls of the PhIDS Model .....	294
<b>Figure 48</b> Third-Party Data Controls of the PhIDS Model.....	294
<b>Figure 49</b> Data Protection Controls of the PhIDS Model .....	297
<b>Figure 50</b> Overview of Nigerian Culture .....	307

## CHAPTER 1: INTRODUCTION

Data, as the lifeblood of modern digital economies, fuels innovation, strengthens enterprises, and shapes society, with its significance continually growing over time. The Fourth Industrial Revolution is propelled by data, highlighting its essential role in influencing the course of our interconnected world (Prasad, 2024). The advent of cost-effective and flexible data collection, processing, and storage solutions like the Internet of Things (IoT) and cloud computing empowers manufacturing organizations of varying scales, including small and medium-sized enterprises (SMEs), to capitalize on the data value (Kamble et al., 2020). As the fusion of IT and manufacturing deepens, manufacturers enhance operational sophistication, resulting in richer manufacturing data. The volume of data generated in the manufacturing sector is rising exponentially. As of 2018, manufacturing systems produced over 1000 EB of data annually (Xu et al., 2020). However, the true value of big data lies not only in its volume but in the insights and knowledge it enables. Systematic computational analysis of manufacturing data has facilitated more informed decision-making processes, allowing manufacturers to better understand products, suppliers, customers, employees, and internal processes. This data-driven approach enhances agility and competitiveness in global markets. Effective data management is now essential for operational efficiency. Organizations that successfully manage data can extract insights, enhance decision-making, and gain a competitive edge. Yet, with the increasing amount of sensitive information, securing this data has become paramount (Kelley, 2024). However, manufacturing-specific challenges, particularly in data security, pose significant threats. From automotive plants to pharmaceutical labs, cyberattacks threaten data integrity and disrupt operations. Notable incidents, including sabotage of additive manufacturing processes, damage to German steel mills, and production halts at Toyota (Rahman et al., 2023), highlight the vulnerability of this sector.



The integration of Industry 4.0 technologies—cyber-physical systems, industrial control systems (ICS), IoT, and cloud computing—has expanded attack surfaces, increasing risk (Johansson et al., 2022; Sai & Kumar, 2022). The convergence of operational technology (OT) and IT has blurred traditional boundaries, enabling cyber threats to cross from digital systems into physical infrastructure. These integration, while advancing manufacturing capabilities, has exposed interconnected systems to cascading effects in the event of breaches. Sophisticated adversaries, including nation-states and cybercriminals, exploit vulnerabilities using tactics such as phishing, ransomware, and social engineering. By 2022, 72% of ransomware incidents targeted manufacturing entities across diverse subsectors. In 2021 alone, the sector accounted for 23.2% of all cyberattacks (IBM Security, 2022). Sharing sensitive data with third parties across global supply chains compounds these risks, making data security a priority for manufacturers and regulators alike.

Drug manufacturing, in particular, faces amplified data security challenges due to stringent regulatory demands, complex supply chains, and highly sensitive intellectual property. Rapid digitalization has driven efficiency but also introduced vulnerabilities. Researchers, including Leal et al. (2021) and Sohan et al. (2022), emphasize that safeguarding data in pharmaceutical manufacturing is essential not just for competitiveness but for patient safety and regulatory compliance.

### **1.1 Statement of Problem**

Medicines are critical to public health, and medicine security ensures availability, authenticity, and safe distribution across supply chains (Adigwe & Onavbavba, 2024; Medicine security, n. d.). A key dimension of medicine security is the protection of sensitive data, including proprietary drug formulas, clinical trial data, and manufacturing protocols. Pharmaceutical companies invest heavily in research and development, making their intellectual property essential to maintaining their competitive advantage (Khan et al., 2025).

Insecure data environments can lead to breaches that enable the circulation of counterfeit drugs, disrupt supply chains, and hinder patients' access to life-saving treatments. These breaches not only compromise patient safety and endanger public health but also inflict significant harm on economic stability. As Rahman et al. (2023) note, 60% of small businesses impacted by a data breach shut down within six months, illustrating the profound financial consequences of poor data security.

The significant worth of pharmaceutical discoveries makes intellectual property theft a prominent target for cyberattacks. In the last decade, global pharmaceutical firms have experienced damaging data breaches. Incidents at Merck, Pfizer, and Genentech show how intellectual property theft and data breaches continue to endanger pharmaceutical assets (Mims & Perelman, 2021; Souza, 2018). These breaches point to underlying vulnerabilities and gaps in data management practices within pharmaceutical organizations. Despite guidelines from authorities, such as the Medicines and Healthcare Products Regulatory Agency ([MHRA], 2015), Pharmaceutical Inspection Convention/Pharmaceutical Inspection Co-Operation Scheme ([PIC/S], 2021), U.S. Food and Drug Administration ([FDA], 2018), and World Health Organization (WHO) ([WHO], 2016, Annex 5; 2021, Annex 4), breaches persist, suggesting that current guidance may lack sufficient clarity, depth, or adaptability to address the evolving nature of cyber threats. The surge in attacks during the COVID-19 pandemic (Okereafor & Adebola, 2021) further exposed weaknesses in data management practices and highlighted the gap between established standards and practical implementation in real-world pharmaceutical environments.

In Nigeria, these challenges are magnified. The country ranks fourth globally for cybercrime (Wang et al., 2020), with escalating breach incidents (Babalola, 2022; Chika & Tochukwu, 2020; Ekhaton, 2024; Major data breach, 2024; Tunji, n. d., Udo Udoma & Belo-Osagie, 2023) and inadequate documentation of non-personal data exposures. Regulatory

enforcement remains weak, and the Nigerian Data Protection Act (NDPA) (Nigerian Data Protection Act [NDPA], No. 37, 2023) does not address the protection of business-critical pharmaceutical data (Adigwe & Onavbavba, 2024). The legal emphasis on personal data fails to protect intellectual property central to pharmaceutical innovation and patient care.

Literature on Nigerian data security focuses heavily on personal data under the Nigerian Data Protection Regulation (NDPR) compliance (Adeoti, 2023; Akinwunmi, 2024; Babalola, 2022; Chika & Tochukwu, 2020; Olukoya, 2022). However, in high-risk sectors like pharmaceuticals, safeguarding business-critical data is equally vital. Other empirical studies (Imasuen, 2021; Waziri, 2020; Adenekan et al., 2023; Aguboshim & Ezeasomba, 2022; Ikusika, 2023) critique regulatory and cybersecurity frameworks but do not address the intersection of intellectual property protection, data infrastructure, and the pharmaceutical sector's unique vulnerabilities. A significant gap persists: How are current data management guidelines and practices falling short in protecting pharmaceutical intellectual property?

## **1.2 Purpose of the Study, Research Aims, and Objectives**

The purpose of this qualitative study is to examine data security gaps in drug manufacturing standards and practices, specifically focusing on the Nigerian pharmaceutical industry. In recent years, the pharmaceutical sector has increasingly depended on data-driven processes, which emphasizes the importance of data protection. Safeguarding sensitive information, such as drug formulas, research and development (R&D) data, and other proprietary assets, is crucial for ensuring the integrity and competitiveness of pharmaceutical companies. In light of the increasing need to protect regulated and business-critical data in the pharmaceutical industry, global and regional health authorities and industry consortia have issued guidance on data management for drug manufacturing. Most regional pharmaceutical industries look to their national regulators, regulatory consortia, or international organizations for guidance on data management, and guidance documents generally align with each other.

Perfect: The National Agency for Food and Drug Administration and Control (NAFDAC), the Nigerian pharmaceutical industry regulator, and indigenous drug manufacturers depends on international health organizations, such as WHO, for guidance and certifications.

This study explored data security gaps in drug manufacturing standards and practices, as they relate to the Nigerian pharmaceutical industry. The research aims to critically evaluate the guidelines published by health authorities, assess real-world manufacturing practices employed by pharmaceutical companies, and determine how these practices align with the guidelines. The following research objectives, defined to achieve the stated aims, drive this study:

- To examine how existing guidelines address data security in drug manufacturing.
- To assess the extent to which Nigerian drug manufacturing practices align with established data security best practices.
- To evaluate the level of alignment between data security practices in drug manufacturing and the recommendations outlined in current guidelines.

The first objective examines health authorities' data management guidelines to evaluate their coverage of data security and identify any gaps that may leave pharmaceutical companies vulnerable to security threats. The second objective assesses the actual data security practices of Nigerian pharmaceutical companies, identifying any weaknesses in data storage, handling, and transmission that heighten security risks. The third objective compares published guidelines with industry practices to determine whether drug manufacturing organizations adhere to good practices. Based on the findings, the study offers recommendations to pharmaceutical companies and regulatory bodies to address the identified data security gaps and promote compliance.

### 1.3 Nature and Significance of the Study

Drug manufacturing involves sensitive information such as patient records, proprietary formulas, research data, and manufacturing processes. Personal details, including patient data, are protected by data protection laws that are essential for maintaining privacy. In Nigeria, data protection is regulated by the Nigeria Data Protection Act, which primarily focuses on safeguarding privacy (Chika & Tochukwu, 2020). In addition to the need for privacy regarding personally identifiable information, drug formulas are valuable intellectual property, and research and development data are critical for new drug development. Safeguarding this data is essential for preserving patient trust and protecting critical research efforts (Khan et al., 2025). Cybersecurity threats, such as malicious actors, can engage in industrial espionage, gain unauthorized access to systems, replicate sensitive information, and disrupt manufacturing operations. A breach in data security not only harms a drug manufacturer's reputation but also results in a loss of public trust, given the pharmaceutical industry's high level of regulation. The emphasis on data protection solely on personal data creates a significant gap in the literature. A review of existing studies revealed a lack of research that thoroughly and comprehensively addresses data security issues in the context of the current challenges facing Nigeria's pharmaceutical sector. Therefore, there is a need for exploratory research to fill this gap.

This study adopted a qualitative approach to explore the adequacy of data management guidelines and practices within this sector and their impact on medicine security. Understanding these guidelines and practices is crucial for developing a contextual strategy to address data security gaps in the industry. This paper presents findings from such research, focusing on a small-scale, exploratory study. The study begins by identifying gaps in the pharmaceutical industry's data management guidelines, examining the industry's current data

security practices, and assessing the alignment between guidelines and practices, which threats could exploit and result in data breaches.

This study contributes to the growing body of research on data governance. A structured review of data governance literature undertaken by Abraham et al. (2019) highlighted domain scope, which encompasses data security, as an area of data governance requiring detailed research. The findings and responses to the research questions will provide valuable insights into data security within the pharmaceutical industry's highly regulated environment, identifying key factors that lead to the compromise of data integrity, confidentiality, availability, and other critical security dimensions.

Also, the study enriches the field of data governance by introducing a data security model. The resulting model will prompt industry regulators, such as NAFDAC and Nigerian pharmaceutical organizations to re-examine the current system framework to prevent data security failures. Moreover, this study builds upon the prior research efforts of De Haes et al. (2013) on enterprise governance and management of information and technology, incorporating new knowledge from a best-practice model into data management tailored to the specific needs of drug manufacturing. By proposing a data security model, this study improves protection of information, along with the systems that store and process drug manufacturing data. Moreover, this study informs data integrity assessment, a crucial aspect of good manufacturing practices inspections (Adigwe & Onavbavba, 2024). Additionally, this research addresses the requirements of health authorities for modern control strategies in data management within the pharmaceutical industry (WHO, 2016). The research will prompt regulators and industry players to revisit data security controls they overlooked, resulting in robust strategies that adequately address data security. Additionally, the study provides governments with a data security model to enhance the critical cybersecurity infrastructure for pharmaceutical industries.

The study employed a qualitative approach to guide the research process due to its exploratory nature. This approach was well-suited to the study, which investigates data security failings and their causes in Nigeria's pharmaceutical industry, an underexplored area where existing knowledge is insufficient to formulate hypotheses (Lacey, 2015). The research followed qualitative case study design, utilizing an exploratory multiple-case study analysis of five pharmaceutical organizations, thirty-one professionals, and three institutional documents from health authorities. The research methods involved analyzing health authorities' guidance documents on data management and conducting face-to-face interviews with experts as data collection methods. Given the greater control over the sample structure and data (Easterby-Smith et al., 2015), collecting primary research data from respondents ensures that the data aligns with the study's objectives. In addition to the ease of obtaining documents from the public domain in a non-reactive, discreet manner without authors' authorization, the combination of document analysis and interviews facilitated triangulation. Consequently, employing multiple data methods and sources of evidence permitted the corroboration and convergence of this study (Aguilar-Solano, 2020). The analysis procedures also included content and thematic analyses. Content analysis involves scrutinizing, reading, and interpreting documents, while thematic analysis reveals the key themes found in interview transcripts (Bowen, 2009). In summary, the design effectively addressed the study's research questions and objectives, supported by document analysis and in-person interviews, along with the execution of content-based, thematic analysis procedures.

#### **1.4 Research Questions**

The exploratory nature of this research necessitates formulating research questions, as its purpose is not to predict the outcome of an experiment or focus on the possible associations of the studied phenomenon. Investigating data security gaps involves questions that address

deficiencies from all sources within the pharmaceutical context. Three research questions emerged to support the research purpose:

- Q1.** How do existing guidelines address data security in drug manufacturing?
- Q2.** What are the current data security practices in Nigerian drug manufacturing organizations, and what gaps exist compared to data security best practices?
- Q3.** How closely do the data security practices in drug manufacturing align with the recommendations outlined in these guidelines?

The first research question explores shortcomings in the guidance provided by relevant health authorities, while the second research question focuses on data security lapses that could be exploited in drug manufacturing operations, suggesting a different research method. The third research question focuses discrepancies between industry standards and drug manufacturing practices concerning data security. Collectively, these questions highlight multiple sources of data security gaps, offering a more comprehensive understanding of the issue. To address these questions, qualitative data must be collected and analyzed from an adequately sized sample using multiple methods.



## CHAPTER 2: LITERATURE REVIEW

This research aims to identify and address data security gaps in existing data management guidelines and practices, as well as the alignment between guidelines and practices within drug manufacturing, with a focus on the Nigerian pharmaceutical industry. As the industry increasingly relies on data-driven processes, ensuring the security of sensitive data, such as drug formulas and research data, becomes critical. A literature review provided a structured foundation for this study and is organized in the following manner:

The chapter begins with an extensive exploration of the theoretical and conceptual framework underpinning data security in the pharmaceutical industry (2.1). This section delves into good manufacturing practices in the pharmaceutical sector (2.1.1), highlighting their role in ensuring product quality and regulatory compliance. This section further examines data governance and data integrity (2.1.2), two critical components for maintaining trust and transparency in pharmaceutical operations. The discussion then shifts to data integrity principles (2.1.3), encompassing attributability, legibility, contemporaneity, originality, and accuracy—core attributes necessary for reliable regulatory submissions and quality control. Building on this foundation, the theoretical perspective of Management Control Theory (2.1.4) is explored as a strategic framework for aligning data security posture with enterprise goals. Furthermore, data security (2.1.5) is examined as a fundamental concept within this framework, reinforcing the need for robust security mechanisms to protect sensitive pharmaceutical information.

The chapter then progresses to an in-depth review of classification and security considerations of data assets (2.2). This begins by outlining the hierarchy of data (2.2.1) and defining the scope of data assets (2.2.2), which include both traditional data and big data. The discussion moves to data locations and states (2.2.3) and a comprehensive analysis of data types, threats, and risks (2.2.4), categorizing sensitive data into intellectual property, legal

documents, strategic planning records, financial information, personally identifiable information, and so on. These data categories face various vulnerabilities, including unauthorized alteration (2.2.5), unauthorized disclosure, and unauthorized denial of use, each posing significant threats to data confidentiality, integrity, and availability.

A significant portion of the chapter is dedicated to the governance and management of information technology (2.3). This section explores IT governance models and implementations (2.3.1), illustrating their role in aligning IT strategies with business goals and ensuring accountability. The discussion distinguishes between IT governance and IT management (2.3.2), clarifying their respective roles in policy enforcement and operational execution. Furthermore, the Enterprise Governance of IT (2.3.3) is analyzed, focusing on its framework (2.3.4), focusing on enterprise goals, IT-related goals, alignment goals, enablers, governance components, and performance outcomes. This section highlights how these governance models contribute to improved security practices and risk mitigation in pharmaceutical manufacturing.

The chapter then transitions into data life cycle, management, and governance (2.4). It begins with an overview of the manufacturing product life cycle and big data (2.4.1), detailing stages such as concept generation, product design, raw material procurement, manufacturing, transportation, sales, utilization, after-sales service, and recycling or disposal. A more technical review follows in the data life cycle section (2.4.2), covering data collection, storage, processing, visualization, transmission, and applications. The data management segment (2.4.3) further analyzes how data is created, stored, used, transmitted, shared, and eventually destroyed, underscoring the importance of structured management practices. Data governance (2.4.4) is then examined in detail, focusing on frameworks, mechanisms, decision domains, organizational scope, and the consequences of weak governance.

The next major section is a critical examination of data security (2.5). It begins with a review of security layers and data security (2.5.1), covering human, perimeter, network, endpoint, application, and data security layers, as well as the protection of mission-critical assets. This section underscores the importance of a multi-layered security approach to mitigate evolving cyber threats. Following this, a review of data security models (2.5.2) is presented, including the Confidentiality, Integrity, and Availability model, Parkerian Hexad Model, Five Pillars of Information Assurance Model, ISO security model, Traditional Four-Step Model, and Pentagon of Trust Model. Each framework is analyzed for its effectiveness in addressing data security concerns within pharmaceutical manufacturing. The section also discusses data security management and governance (2.5.3), including risk assessments, security policies, control objectives, cyber defense controls, data security auditing, and the critical role of a data security officer in driving ongoing compliance. Additionally, the chapter explores data leakage and prevention (2.5.4), detailing data loss prevention solutions, deployment strategies, and methods to combat insider threats and external breaches. A final subsection (2.5.5) identifies gaps in empirical literature on data security within pharmaceutical manufacturing, highlighting areas for future research.

The chapter concludes with an extensive review of Nigeria's pharmaceutical industry (2.6), providing context for the study's focus on data security challenges in this sector. The discussion begins with industry characteristics (2.6.1), exploring regulatory frameworks, market entry barriers, capacity utilization, mergers, acquisitions, and government interventions aimed at sustaining industry growth. This section emphasizes the unique regulatory landscape within Nigeria's pharmaceutical sector and its implications for data governance. The final segment, challenges and trends (2.6.2), provides a critical examination of industry-specific obstacles, including substandard medicinal products, weak regulatory systems, scientific and technological advancements, poor infrastructure, and disruptions. The section also examines

Nigeria's efforts toward WHO prequalification, a crucial factor in ensuring international compliance and pharmaceutical credibility.

This comprehensive review in Chapter 2 lays a solid foundation for understanding the complexities of data security in pharmaceutical manufacturing. It integrates insights from management theories, IT governance frameworks, data governance principles, and industry-specific challenges, offering a thorough perspective on securing pharmaceutical data. This literature review serves as a cornerstone for identifying existing security gaps and proposing a structured model to enhance data protection within the industry.

Literature review involved accessing various library databases and search engines to retrieve relevant academic and industry-related materials. The review entailed sourcing peer-reviewed journals and conference proceedings from databases such as IEEE Xplore and ScienceDirect, while broader searches were conducted using Google Scholar and ResearchGate to identify additional scholarly articles. Consulting standards and practitioner publications, including ISO standards and industry reports, minimize biases. Targeted searches for equity research reports on Nigeria's pharmaceutical industry offered insights into market trends and security challenges, while seminal literature on IT governance and data security provided essential historical context.

Key search terms and combinations included "Data security in drug manufacturing," "Drug manufacturing data protection," "Nigerian pharmaceutical industry security", and "Challenges and trends in Nigeria's pharmaceutical industry". Broader searches also included "IT governance in pharma", "IT management in pharmaceuticals", "Data governance in drug manufacturing", and "Data management in drug production". The scope of the literature review covered the past five years, ensuring that the analysis incorporates recent developments and emerging trends in data security. This review synthesizes insights from both academic research

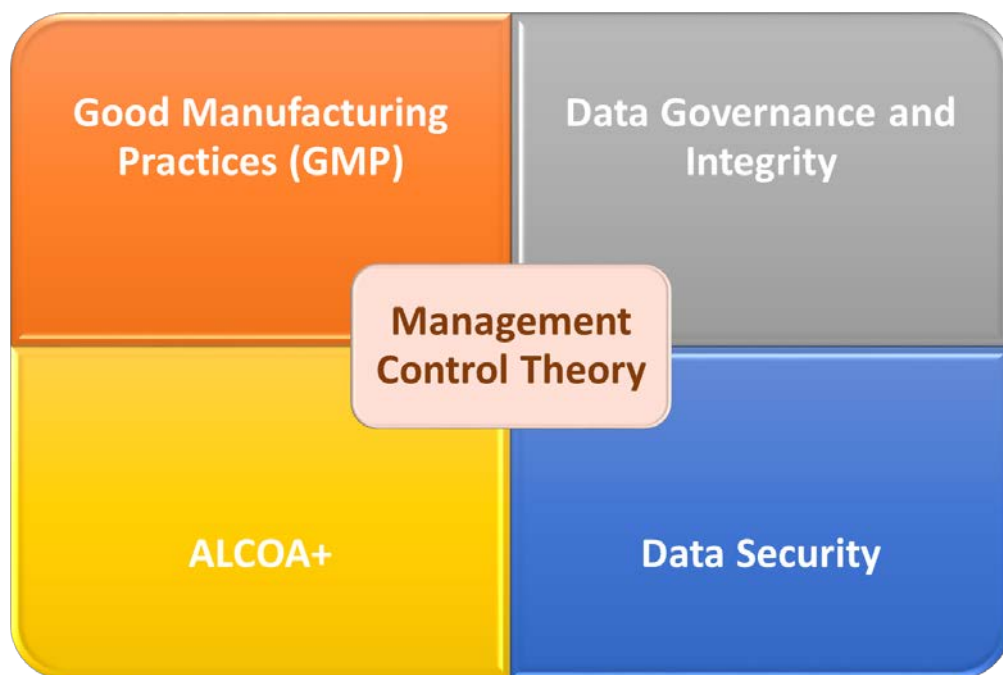
and industry practices to describe the current state of data security in pharmaceutical manufacturing and identify critical gaps that need to be addressed.

## 2.1 Theoretical/Conceptual Framework

This study adopts management control theory as its theoretical framework. Additionally, it incorporates good manufacturing practices and related concepts. Alongside good manufacturing practices, the study's conceptual framework also includes data governance, data integrity, and data security, as shown in Figure 1.

**Figure 1**

*Theoretical Framework*



### 2.1.1 Pharmaceutical Industry Good Manufacturing Practices

The pharmaceutical industry is one of the most highly regulated manufacturing environments. The need for consistent precision in drug manufacturing within this sector led to Good Manufacturing Practices (GMP). Pharmaceutical Inspection Co-Operation Scheme ([PIC/S], 2019) defines GMP as “that part of Quality Assurance which ensures that products are consistently produced and controlled to the quality standards appropriate to their intended

use and as required by the marketing authorization or product specification” (p.1). GMP outlines the essential requirements for manufacturing medical devices, chemical products, pharmaceuticals, and other regulated items according to quality standards. WHO first implemented GMP in the 1960s (Tabersky et al., 2018). The PIC/S (2019) GMP guide, which originated from the WHO GMP Guide, was established in 1970 to harmonize GMP standards and guidance documents. Following this guide, the European Union (EU) adopted and implemented its GMP Guide in 1989 (PIC/S, 2019; Tabersky et al., 2018). The adoption of GMP concept in the early 1990s standardized chemical production (Tabersky et al., 2018). Since then, the rules and regulations governing the pharmaceutical industry have evolved. Generally, good practices (GxP), including GMP, are implemented across all aspects of pharmaceutical manufacturing. These practices include the production of active pharmaceutical ingredients, drug substances, drug products, device manufacturing, and other technical areas (Tabersky et al., 2018). GxP guidelines also address additional areas, such as outsourcing activities, distribution of medicinal products, quality risk management, documentation, and data governance.

GMP plays a vital role in ensuring product quality and regulatory compliance within the pharmaceutical industry by focusing on quality assurance and minimizing risks to product integrity that may arise from data breaches and regulatory deficiencies. According to PIC/S (2019), GMP requires that products are consistently manufactured and controlled to meet established quality standards. The insufficient regulatory oversight in Nigeria’s pharmaceutical sector, highlighted in the problem statement, underscores the necessity for GMP-compliant practices to prevent counterfeit drugs and safeguard patient safety.

### **2.1.2 Data Governance and Data Integrity**

Data governance is crucial for the trustworthiness of data and records in GMP activities and regulatory submissions. According to the WHO (2016), data governance encompasses all

arrangements that “ensure that data, irrespective of the process, format or technology in which it is generated, recorded, processed, retained, retrieved and used will ensure a complete, consistent and accurate record throughout the data life cycle” (p. 171). Thus, data governance refers to the measures that uphold data integrity.

Data integrity is evident in almost every aspect of drug manufacturing. Drug manufacturing lines consist of various automated systems, some of which are built-in, that control multiple processes of medicine production (Leal et al., 2021). These production lines generate a wide range of heterogeneous data sets, which are susceptible to data integrity violations. Data integrity violations involve the introduction of bias that can be deliberate or accidental; in either case, it can negatively impact the quality system (Jain, 2017). However, there is no room for bias in drug manufacturing. Data integrity is fundamental to a pharmaceutical quality system and ensures that medicinal products meet requisite quality standards since data informs product quality decisions (Jain, 2017). Therefore, pharmaceutical organizations should retain the electronic data generated by production processes and associated activities without compromising the integrity of medicines and the safety and well-being of patients. Consequently, the computerized systems essential in pharmaceutical production lines must be verifiable as the industry becomes increasingly regulated for product quality and patient health reasons (Leal et al., 2021).

### **2.1.3 Data Integrity Principles**

A key aspect of data integrity is the principle of ALCOA+. ALCOA is “attributable, legible, contemporaneous, original, and accurate” (WHO, 2016, p. 169). ALCOA is generally associated with data quality, as it defines the essential properties of data integrity and documentation (Tabersky et al., 2018).

**Attributable.** Data should be traced back to its source and attributed to the person who observed and recorded it. According to Tabersky et al. (2020), it is feasible to trace electronic

data through rigorous user access management, an audit trail, and an electronic signature. The foundation of the attributable feature of ALCOA+ is who acquired the electronic data, who acted, and when (Jain, 2017).

**Legible.** The legible feature ensures that data is readable. All recorded data must be human-readable, permanent throughout the data life cycle, and include metadata such as the audit trail (Tabersky et al., 2020). The legible characteristic highlights the ease of reading electronic data (Jain, 2017).

**Contemporaneous.** The contemporaneous feature requires recording information at the time of the activity, during data generation, and in chronological order. This attribute reduces the risk of individuals recalling incorrect information. In an electronic system, maintaining the audit trail helps mitigate this risk by creating time stamps for all data inputs and changes (Tabersky et al., 2020). This feature focuses on documenting electronic data at the time of the event (Jain, 2017). The implication of this expectation is that pre-dating or post-dating is not acceptable.

**Original.** The original attribute refers to the initial capture of data. Information should be accessible and preserved as it was originally created (Tabersky et al., 2020). According to Jain (2017), the original characteristic of electronic data emphasizes the printout or written observation, or a certified true copy of it.

**Accurate.** The data and records must be error-free, complete, truthful, and consistent with the observation. According to Tabersky et al. (2020), sufficient information must exist to recreate the chain of events unambiguously. Expectations for electronic data accuracy assume no errors or modifications without documented changes (Jain, 2017).

The ‘+’ highlights the qualities of data as being “complete, consistent, enduring, and available” (WHO, 2016, p. 169) throughout the data life cycle and retention period. These



additional terms stem from the EU Eudralex guidelines (European Commission, 2011) and PIC/S (2021). ALCOA+ supports adherence to the data integrity requirements of GMP.

As defined by WHO (2016), data governance ensures that data remains complete, consistent, and accurate throughout its life cycle. Data integrity principles, including ALCOA+, are essential for maintaining trustworthiness in pharmaceutical data. Violations of data integrity, such as unauthorized record changes, directly threaten these fundamental principles. The data breaches in Nigeria highlight the need for adherence to ALCOA+ to ensure reliable records and safeguard against unauthorized access and manipulation. The lack of commitment to these principles, as illustrated in the problem statement, undermines regulatory compliance and jeopardizes public health.

#### **2.1.4 Management Control Theory**

Management Control Theory (MCT) is essential for successful strategy implementation. It presents control as a set of tools that help an organization achieve its strategic objectives (Simons, 1990; 2000). This theory originated in commerce, particularly with the rise of private corporations and the evolution of enterprises that separated ownership from management. It also draws from theories in Organizational Theory, Stafford Beer's Cybernetics, and Fayol's General Theory of Management (De Haes et al., 2013). The scientific management approaches of Anthony and others (Anthony, 1965) strongly shaped previous perspectives of management control and focused mainly on resource acquisition and use for achieving organizational objectives. Later, MCT became more inclined to regard control as a set of tools for achieving enterprise strategic objectives (Simons, 1990; 2000).

The main theoretical principles of MCT include enterprise goals, management controls, management control systems, and business outcomes. According to Simons (1990; 2000), management controls connect the organization's strategic goals to business outcomes through a combination of formal processes and informal mechanisms. Hewege (2012) identified

strategic systems planning, budgeting, organizational structure, operational controls, standard operating procedures, and reward systems as formal management control processes; whereas informal mechanisms include leadership, values, norms, and culture. Simons (1990; 2000) also defined diagnostic control systems as formal feedback systems designed to monitor and correct unexpected organizational outcomes toward predetermined performance standards. Thus, management controls comprise a set of control systems aimed at executing management control, while management control systems represent the entirety of an organization's interdependent controls to achieve desired outcomes.

MCT examines how organizations guide employee behavior and resources to achieve strategic goals, often through formal structures like policies, performance indicators, and evaluation systems. It is widely applied in accounting, operations management, and organizational studies to understand how internal controls align with organizational objectives. However, despite its usefulness, MCT has several limitations. Firstly, the theory often emphasizes formal and hierarchical control mechanisms, potentially overlooking informal and emergent behaviors that can significantly influence performance. Secondly, it tends to assume rational decision-making processes and compliance, which may not fully capture the complexity of human behavior in dynamic environments. Moreover, in rapidly changing fields such as IT, rigid control structures can hinder innovation or delay responses to emerging threats. Despite these limitations, MCT offers a valuable lens for analyzing data security in the pharmaceutical sector. The industry is heavily regulated and risk-averse, necessitating well-defined control structures to ensure data integrity and compliance. Furthermore, the increasing sophistication of cyberattacks, the rise in pharmaceutical intellectual property theft, incidents of data breaches, and supply chain disruptions stemming from those breaches, along with their economic consequences, as highlighted in the problem statement, indicate a failure to establish and implement effective management control systems. As Simons (1990; 2000) explains, these

controls are essential tools for achieving strategic enterprise goals by aligning organizational objectives with business outcomes through diagnostic control systems. The foundational insights of MCT are crucial in identifying gaps between strategic intent and operational execution, as well as in safeguarding data assets, intellectual property, and production processes against cyber threats.

### **2.1.5 Data Security**

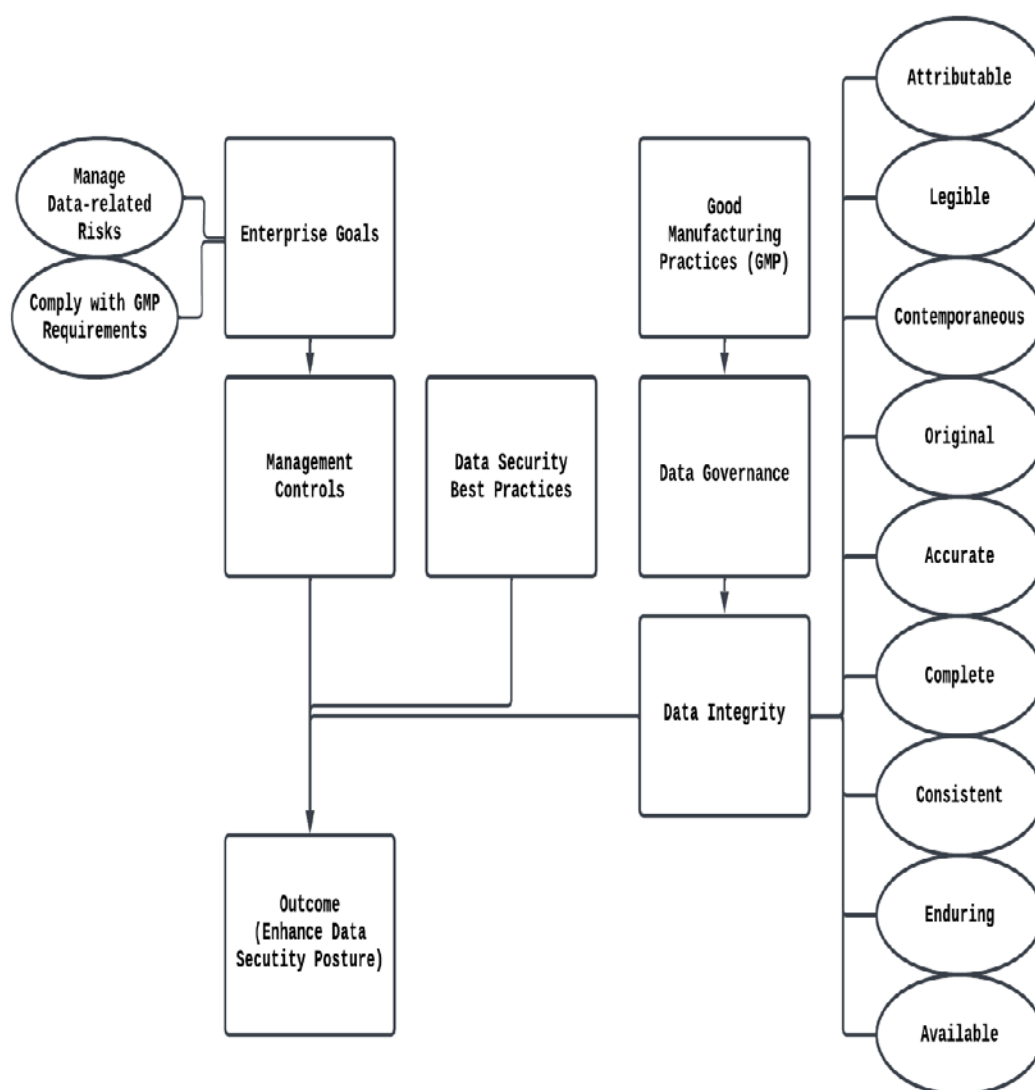
Data security focuses on protecting data stored within and beyond network boundaries. Abraham et al. (2019) define data security as the preservation of security requirements, including confidentiality, integrity, privacy, availability, accessibility, authenticity, and reliability of data. As Elijah et al. (2021) noted, data security emphasizes data protection during both storage and transmission. Consequently, it includes protocols and measures designed to prevent unauthorized access, modification, exposure, or destruction of sensitive data, whether the data is stationary or in transit. Incidents like the Pfizer employee copying over 12,000 confidential files reveal significant weaknesses in the pharmaceutical data security framework. Furthermore, events such as the theft of cancer therapy development methods, along with the increase in ransomware attacks and data breaches in Nigeria, highlight the urgent need for robust data security measures to protect against the disruptive effects of cyber threats.

Using a concept mapping, Figure 2 visually represents the theoretical/conceptual framework of this study, illustrating the interrelationships among key concepts of GMP, MCT, data governance, data integrity, and data security. MCT articulates sound management practices, GMP standards are vital for maintaining product quality and regulatory compliance, especially in the pharmaceutical industry. Data governance and integrity principles ensure data accuracy and reliability within this context. The ALCOA+ principles, emphasizing attributes such as attribution, legibility, contemporaneousness, originality, accuracy, completeness, consistency, endurance, and availability, are essential for upholding data integrity within this

framework. Strong data security measures are also necessary to protect sensitive data and prevent unauthorized access or manipulation, thereby enhancing data integrity. By integrating theory, principles, and concepts, the pharmaceutical industry can effectively achieve not only data integrity but also a stronger data security posture.

**Figure 2**

*Concept Map of Theoretical Framework*



**Note.** Theoretical framework synthesized by the author linking Management Control Theory, good manufacturing practices, data governance, data integrity, ALCOA+, and data security based on PIC/S (2019), Simons (1990; 2000), and WHO (2016).

## 2.2 Classification and Security Considerations of Data Assets

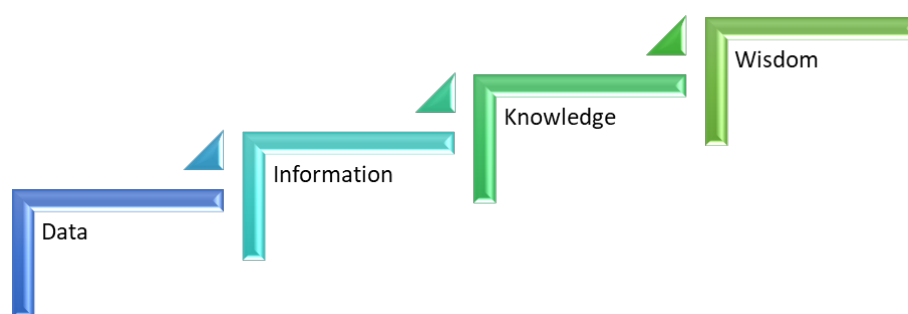
Data assets form the backbone of modern organizations. Clearly defining the hierarchy, scope, states, and types of data is essential for managing risks to these assets. This section outlines the key categories of data, associated threats, and potential impacts of unauthorized alteration, disclosure, or denial of use.

### 2.2.1 Hierarchy of Data

Data consists of raw or simple facts. According to Mosely et al. (2009), data represents facts in various formats, including text, numbers, sound, images, and videos. Data becomes information within a specified context that informs governance, management, and operations decision-making. Once the context is established, the data can be reported or queried in greater depth to provide logical inferences, probabilities, insights, or patterns inherent in the data, whether they exist within or outside the enterprise. Rowley's (2007) knowledge hierarchy illustrates how data evolves across four distinct stages: "data, information, knowledge, and wisdom" (Deepu & Ravi, 2021, p.2), as shown in Figure 3.

**Figure 3**

*Relationship between Data, Information, Knowledge, and Wisdom*



**Note.** Adapted from “A Conceptual Framework for Supply Chain Digitalization Using Integrated Systems Model Approach and DIKW Hierarchy,” by T. S. Deepu, & V. Ravi, 2021, *Intelligent Systems with Applications*, 10, p. 6. Copyright 2021 by the Intelligent Systems with Applications. Adapted with permission.

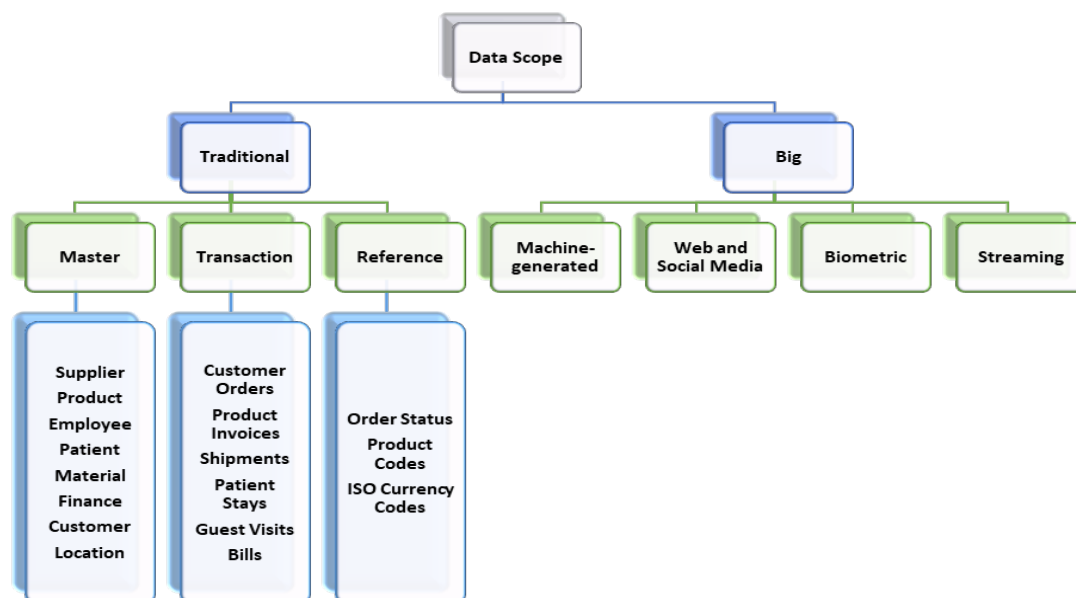
Meaning is applied when data is accessed and processed. According to the Information Systems Audit Association (ISACA) (2019), data transforms into information when it is made meaningful, which is crucial for the functioning of an enterprise. Given that information is derived from data, it can be used to generate organizational knowledge—a relevant set of facts. Knowledge results in a deeper understanding of an issue and greater insight. Thus, the efficient use of data helps achieve enterprise objectives.

### 2.2.2 Scope of Data Asset

The scope of a data asset refers to the specific category of data being examined. According to Abraham et al. (2019), the scope of data assets can include both traditional data and big data, as shown in Figure 4.

**Figure 4**

*Categorization of Data*



**Note.** Based on the data categorization discussion in “Data governance: A Conceptual Framework, Structured Review, and Research Agenda,” by R. Abraham et al., 2019, *International Journal of Information Management*, 49(1), pp. 424-438 (<https://doi.org/10.1016/j.ijinfomgt.2019.07.008>)

**Traditional Data.** Traditional data is the foundation for organizational operations (Lee et al., 2014). This category encompasses master, reference, and transaction data. Master data identifies an entity's key business objects (Soares, 2013). Common master data domains include supplier, product, material, finance, customer, employee, location, and patient data (Khatri, 2016). Transactional data represents records related to business transactions in various domains. These include customer orders, product invoices, shipments, patient stays, guest visits or bills (Ballard et al., 2014). Reference data is an agreed-upon set of shared values used across an organization (Dreibelbis et al., 2008). Internally defined reference data includes order status and product codes, while the ISO currency codes are examples of externally defined reference data (Dreibelbis et al., 2008). Traditional data is the foundation for the operations of an organization (Lee et al., 2014).

**Big Data.** Big data has various definitions. However, the Meta Group provided a more notable definition for big data. According to a 2001 Meta Group report, the three dimensions of big data are data variety, velocity, and volume (Laney, 2001). Data variety refers to a data format that can be unstructured, semi-structured, or structured (Ballard et al., 2014; Information Systems Audit and Control Association [ISACA], 2013a). Data velocity denotes the high throughput that enables organizations to respond quickly to events as they happen (ISACA, 2013a). Data volume pertains to big data's rapid growth rates (Tallon, 2013), its veracity, and its value (Khatri, 2016). Ballard et al. (2014) describe veracity as the trustworthiness of data and value as any big data application that drives revenue growth. The Information Systems Audit and Control Association (ISACA) (2013a) offers a broader definition of big data as a "common term for a set of problems and techniques concerning the management and exploitation of very large sets of data" (p. 46). Big data includes machine-generated data (Brous et al., 2016b), web and social media data (Brous et al., 2016b), biometric data (Malik, 2013), and streaming data (Ballard et al., 2014). Although Abraham et al. (2019) categorized these

sources as big data, their classification did not account for those generated by manufacturing processes. Such an exclusion from the scope of big data could lead to an incomplete inventory of data assets. Nevertheless, big data generated by manufacturing processes can be categorized into product, equipment, user, manufacturing information systems, and public data (Tao et al., 2018).

### **2.2.3 Data Location and States**

Data exists both within and outside an organization's boundaries. Mosely et al. (2009) refer to data as the content that flows through application systems and IT infrastructure. They further highlight that information technologies capture, process, provide, and store data. Thus, application systems and IT infrastructure serve as the conduits through which data flows. Wlosinski (2018) identifies the locations where data exists: data in use, data at rest, and data in motion. Data at rest is found in intranet/internal websites, organizational data and email archives, internal directory shares, local computers, databases, controlled access ports, mobile devices, CDs and DVDs, fax machines, copiers, file cabinets, and printed/hard-copy reports. Data in motion can be found on the web or Internet, website postings, email (organizational and personal), blogs (Internet and intranet), social media, file transfers, data sharing, instant messaging (IM), and paper mail containing sensitive data. Data in use resides in servers, workstations, and mobile devices or endpoints. Wlosinski (2018) identifies these locations as areas of concern from an IT perspective and, therefore, require protection. Chapple et al. (2018) regard these three areas as data states, as illustrated in Figure 5.

### **2.2.4 Data Types, Threats, and Risks**

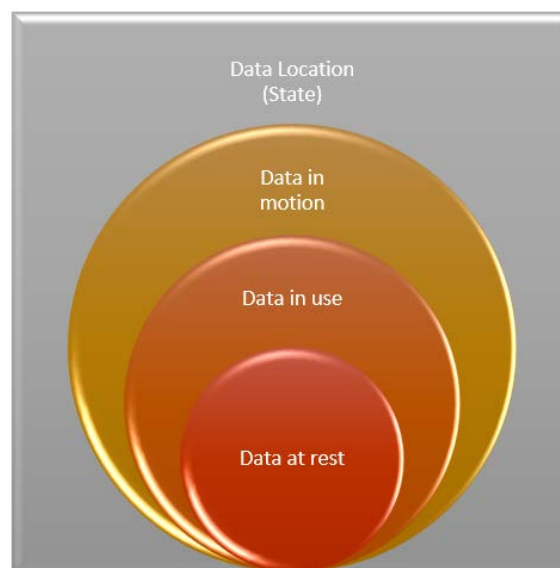
Risks exist for different types of data, regardless of their location. Khan (2016) posits that all data are at risk of being compromised, irrespective of their state. According to Pearce (2017), data at risk are those that, if placed in unauthorized hands, could jeopardize a company and/or its clients. Wlosinski (2018) categorized types of data at risk, including strategic



planning, customer, marketing, sales, human resources, personal, personally identifiable information, intellectual property, legal documents, operations, finance, information technology, and government or country data. Each data type, shown in Figure 6, faces security and privacy threats and risks, which can have serious repercussions for a company.

**Figure 5**

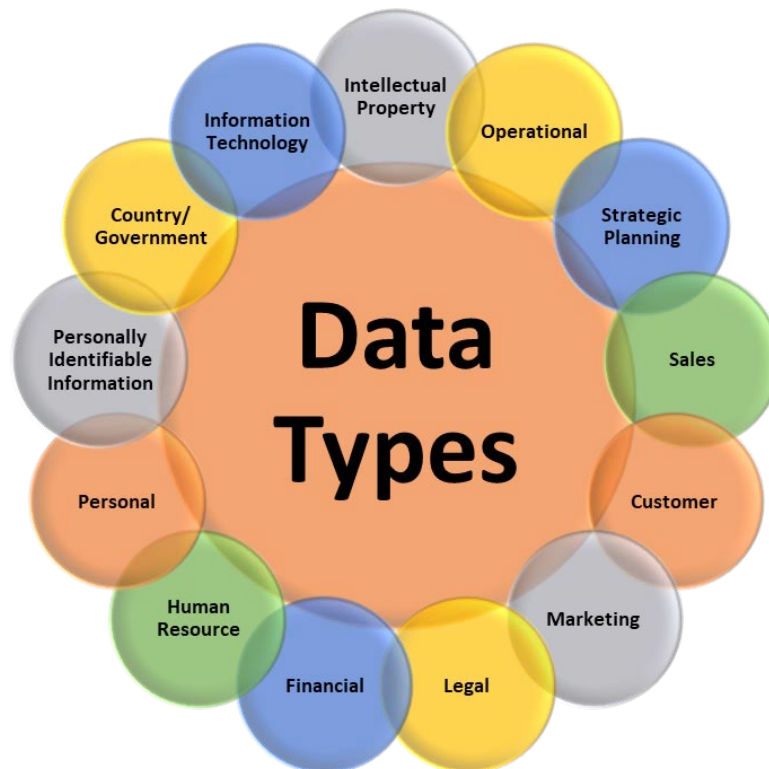
*Data Locations (States)*



**Note.** Based on content from *CISSP (ISC) <sup>2</sup> Certified Information Systems Security Professional Official Study Guide*, by M. Chappel et al., 2018, Wiley.

**Intellectual Property.** Intellectual property (IP) includes the development and management of patent portfolios, as well as unpublished patent applications, invention disclosures, presentations about inventions, formulas, and related communications. Threats to IP arise from competitors, foreign governments, and dissatisfied employees. Risk factors associated with IP encompass loss of competitive advantage and brand damage.

**Legal.** Legal documents, such as memos, correspondence, presentations, notes related to pre-litigation, litigation, corporate governance, internal investigations, and contracts, contain legally relevant information. Competitors pose threats, while risk factors tied to legal documents include litigation and having a weak position in court.

**Figure 6***Data Types*

**Note.** Based on the data types discussion in “Data loss prevention—Next steps,” by L. G. Wlosinski, 2018, *ISACA Journal*, 1, pp. 1-11 (<https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/data-loss-preventionnext-steps>)

**Strategic Planning.** Strategic planning leads to various critical outcomes, such as pending patents, new designs, strategic plans, sales plans, insights into purchasing power, research on mergers and acquisitions, undisclosed details about potential mergers or acquisitions, and preliminary versions of press releases or announcements. Competitors represent significant threats, while risks associated with strategic planning outcomes include a weakened market position in relation to competitors and erosion of shareholder value.

**Sales.** Sales information entails lists of target customers, price and cost lists, discount ratios, potential revenue, sales volume and projections, records of business-to-business orders, and vendor data. Sales information is threatened by various sources, particularly rival

companies and discontented employees. Risk factors related to sales information include insider trading, regulatory fines or sanctions, and competitors entering the market with lower prices.

**Customer.** Customer-related information includes a wide range of data such as customer lists, profiles, user preferences, internal spending habits, contact details, interaction histories, pricing information, sales quotes, transaction volumes, account balances, payment statuses, payment or contractual terms, and purchase or transaction history. Competitors present a threat to the security of customer data. Risks related to customer data include competitors exploiting this information to the organization's detriment, customer attrition, and significant costs associated with notifying affected parties.

**Marketing.** Marketing information includes various types of data, such as business forecasts, competitive insights, product design specifications, business plans, and marketing and business roadmaps. Competitors present a threat to marketing data, with risk factors that include the entry of competitors into a company's market with lower prices and the potential loss of market share.

**Operational.** Operational information includes the advantages of processes and procedures, as well as strategies designed to improve efficiency and productivity. Competitors also present a threat. Risk factors associated with operational information involve the chance of competitors retooling and modifying processes to replicate those of an enterprise, thus becoming more competitive.

**Financial.** Financial data includes various types of information, such as pre-earnings releases, financial statements, periodic performance filings from companies, bank statements, and payroll and equity data. Competitors pose a significant threat to the security of this financial data. The potential loss of competitive advantage represents a notable risk factor.

**Human Resource.** Human resource data includes the organization's reporting structure, recruitment lists, salaries, and job titles and responsibilities. Competitors present a threat, and the loss of key talent along with internal conflicts are significant risk factors related to human resource data.

**Personal.** Personal information encompasses various types of data, including bank account numbers, financial statements, personal health information (PHI), credit card details, health records, personal preferences, vehicle registration numbers, and related demographic data. Criminals and criminal organizations often target personal data, presenting significant threats. Potential data breaches endanger not only individuals' privacy and security but also their families' overall well-being.

**Personally Identifiable Information.** Personally identifiable information (PII) encompasses full names, birthdays, birthplaces, passport numbers, national identification numbers, social security numbers, driver's license numbers, biometric data, and passwords. PII is at risk from criminals and criminal organizations. The potential threats linked to PII include impersonation, loss of savings, fraud, and a decline in credit rating.

**Country/Government.** Country and government data encompass agency information, such as border protection and law enforcement, program design data, such as space initiatives, citizen data, such as criminal investigations, cybersecurity program data, such as scan results, and network infrastructure sector data, like power companies. This data faces threats from criminal organizations, foreign countries, and insiders. Such data involves risk factors that endanger the safety of citizens and the overall security of the nation.

**Information Technology.** Information technology (IT) data includes software source code, Outlook offline files (such as PST and MSG), network diagrams, configuration files for applications, spreadsheets containing Internet Protocol addresses, wireless access keys, database systems, and networks, encrypted files including .zip, .pdf, and .xls, files with names

such as “Passwords”. Threats to IT data comprise malware, hackers, and employee dissatisfaction. The associated risk factors encompass the loss of data confidentiality, integrity, availability, and potential damage to a company's mission and reputation.

Furthermore, repositories, media, and documents associated with these data types may contain sensitive information. As outlined by Chapple et al. (2018), sensitive data refers to information that is not unclassified or intended for public access. This sensitive data can include proprietary, confidential, or protected information or any other data that an organization must safeguard due to its intrinsic value or to comply with relevant laws and regulations.

Since Wlosinski (2018) excluded manufacturing data from his classification systems, he failed to identify the threats and risks associated with it. Despite this omission, manufacturing data faces risks similar to those of other data types. Nevertheless, researchers such as Fu et al. (2018), Malik et al. (2021), Sai and Kumar (2021), Flindon and Divya (2022), and Halder and Newe (2022) have recognized and identified various risks related to manufacturing data. As a result, manufacturing organizations might neglect to protect their manufacturing data adequately.

### **2.2.5 Data Security Threats and Risks in Pharmaceuticals**

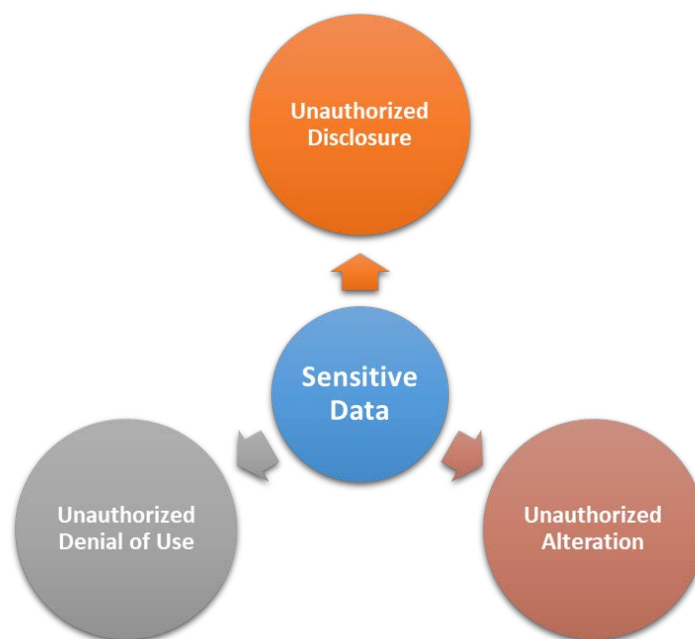
Pharmaceutical companies transmit, process, and store sensitive data. At the same time, data security is becoming an increasingly important concern for drug manufacturers. The threats to data security in the pharmaceutical industry are discussed below according to Moghaddasi et al. (2016) classification of invasions, as shown in Figure 7: unauthorized disclosure, alteration, and denial of use.

**Unauthorized Alteration.** Electronic data and computer systems have introduced new challenges in preserving data integrity. Data integrity becomes at risk when attackers position themselves between systems, allowing data traveling in both directions to pass through them. This vulnerability enables them to steal valid session information, use it to gain unauthorized

access, and capture and manipulate data, thus compromising its integrity. Therefore, data security systems should be a fundamental component of the pharmaceutical quality system mandated by regulators. However, industry regulators have emphasized the importance of data integrity due to the discovery of significant breaches in this area (Jain, 2017). Several health authorities have published specific rules and regulations on GMP for data management. Tabersky et al. (2020) identified three key documents that had a significant impact on the industry namely: PIC/S 'Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments' (2021), UK 'MHRA GMP Data Integrity Definitions and Guidance for Industry' (2015), and US FDA 'Guidance on Data Integrity' (2018).

### Figure 7

#### *Classification of Data Invasion*



**Note.** Based on the classification of data invasion discussion in “Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model,” by H. Moghaddasi et al., 2016, *The Open Medical Informatics Journal*, 10, pp. 4-10 (<https://doi.org/10.2174/1874431101610010004>)

These documents provide guidance and direct the industry to establish tightly controlled systems to ensure data integrity throughout the entire manufacturing and analysis process, as well as the life cycle of a product, from development to production shutdown. These documents require that the integrity of pharmaceutical data resources be aligned with international regulatory and data quality principles, specifically the ALCOA+ principles. For data to meet the characteristics defined by ALCOA, Leal et al. (2021) emphasize that data must be securely collected and maintained, ensuring that they are: attributable to the individual who generates the data; legible and permanent; contemporaneous, meaning the data is created or stored during the execution of the activity; original records (or ‘true copies’) and accurate. Additionally, data records and all new software and hardware systems implemented in pharmaceutical production lines are legally required to comply with ALCOA (Leal et al., 2021). The updated interpretation of data integrity requirements places greater emphasis on the overall data handling process and the stages of the data life cycle, including data creation, processing, review, reporting, and preservation (Tabersky et al., 2020). Consequently, the industry is constantly seeking effective technological solutions to improve the manufacturing process to adhere ALCOA+ principles. Several solutions have increased the integrity of the data used in drug production. For instance, Novartis, the Swiss pharmaceutical company operating in Nigeria, implemented data process mapping to gain insights into data flow, life cycle, and processing. This exercise helped identify vulnerabilities in manual data recording, processing, and storage within equipment and systems (Tabersky et al., 2018). The findings led to the adoption of procedural controls and digital solutions that eliminated or reduced the identified data integrity risks to acceptable levels.

Data integrity regulatory requirements have driven the modernization of control strategies among pharmaceutical organizations to manage risks to data integrity. However, there is no guarantee that existing tools and methods are free from potential falsification or that

the data within pharmaceutical data flows cannot be falsified (Leal et al., 2021). Furthermore, data integrity may be at risk when attackers exploit vulnerabilities that allow them unauthorized access, capture, and manipulation of data, thereby compromising its integrity.

The pharmaceutical industry has undoubtedly placed significant emphasis on data integrity. Pharmaceutical organizations regularly establish standards and controls to ensure compliance with legislation and regulations regarding data integrity. However, a robust data security framework requires these organizations to integrate additional aspects of data security controls early in system design to prevent failures in data protection. Control owners will need to reevaluate existing controls that may have been overlooked in the past.

**Unauthorized Disclosure.** Malevolent persons attempt to exploit vulnerabilities in a network implementation to intercept user or corporate data, which may be used to penetrate the network or impersonate target users. Urciuoli et al. (2013) envisioned that certain vulnerabilities could be exploited by attackers collaborating with insiders and terrorist groups to steal data related to drug formulations, alter documents, and carry out other malicious activities. Malicious individuals, malware, and criminal organizations pose threats that have ravaged many companies by capturing their confidential data. Events like the 2007 Pfizer incident, where an employee's unauthorized installation of file-sharing software on a company laptop exposed the personal data of 17,000 current and former employees, are classified as data breaches (Roberts, 2014). Unauthorized access to data leads to the disclosure of information to individuals who are not permitted to access it (Bertino & Sandhu, 2005) and puts affected individuals at significant risk. Common vectors exploited by threat actors tend to be simple and low-level, taking advantage of small vulnerabilities that can lead to severe consequences. These include malware, stolen credentials, SQL injection, social engineering, and brute force attacks (Khan, 2018). Threat actors also employ cyberattacks such as spear-phishing, cyber espionage, and insider threats (Khan et al., 2015). For instance, Moderna was targeted by cyberespionage



efforts, potentially involving state actors, aimed at accessing its vaccine development data, while Pfizer experienced a spear-phishing attack focused on its clinical research (Rust-Nguyen et al., 2023). In a separate incident, an insider at GlaxoSmithKline (GSK) disclosed trade secrets, and another breach resulted in the theft of the COVID-19 vaccine formula from Pfizer and BioNTech (Aamir & Zaidi, 2019). Threat actors use a systematic approach to access sensitive data. According to Stolfo (2019), they conduct reconnaissance to identify a target and points of entry, followed by an initial breach, usually by spear-phishing users within the target organization. Once they successfully steal the credentials of a legitimate user, they position themselves to maintain control for extended periods. They move systematically, searching for additional credentials, servers, files, logs, and documents of interest. Documents and data are aggregated and 'exfiltrated' using common protocols and third-party websites, allowing them to download their stolen data assets. Establishing a foothold enables long-term data exfiltration at a rate that suits their needs. The National Institute of Standards and Technology (NIST) (2012) describes these methods, defined by tactics, techniques, and procedures (TTPs), as characteristics of threat events in cyber or physical attacks. Data exfiltration is one of the threat events they identified in their publication, specifically referring to data theft. Threat scenarios, such as those designed by AlKilani et al. (2019), are modeled, developed, and analyzed based on threat events.

Furthermore, there is an unintended loss of data when confidential information exits a company's borders without explicit approval from authorized personnel. Van Stone and Halpert (2018) identified sources of unintentional data loss, including shadow IT, lost USB devices, lost mobile phones, stolen laptops, data distribution, social media, instant messaging, email, third-party data rights, online disclosure, asset disposal, and clicking on email malware. Shadow IT particularly raises the risk that data will be transmitted and stored outside of organizational-wide standards and controls.

Pharmaceutical organizations play a vital role in developing lifesaving drugs and vaccines, making them prime targets for cybercriminals looking to steal their IP by compromising the corporate credentials of executives and employees. Constella (n. d.) reported that in 2020, AstraZeneca was targeted by North Korean hackers, who attempted to breach the company's systems using fake online recruitment schemes. Constella (n.d.) also noted that hackers tried to steal information from Novavax and Johnson & Johnson, both of which were developing COVID-19 vaccines at the time. Nonetheless, the sensitive corporate credentials of executives and employees at large pharmaceutical companies are exposed and circulated online. According to Constella (n.d.), PII exposures of pharma executives are common, and the distribution of various types of PII is empowering threat actors, who have intensified their attacks. The significant increase in data breaches, leaks, and exposed records during the COVID-19 pandemic coincided with a rise in cyberattacks. The pandemic-driven shift to digital operations and remote work significantly expanded the attack surface of pharmaceutical companies, increasing their vulnerability to security threats. Identity theft, account takeovers, disinformation campaigns, and other cybercrimes rose following the pandemic, along with the security challenges faced by remote workforces. Alongside new challenges, persistent issues such as Universal Serial Bus (USB) drives, mobile devices, and employee loss of computers also jeopardize data security. Unintentional data loss may also occur when employees enter incorrect email addresses, neglect to lock their computers, use unsecured peer-to-peer messaging, share data inappropriately with unauthorized partners, or take high-resolution photos that reveal sensitive hardware or information in the background (Van Stone & Halpert, 2018).

Apart from internal employees, contractors are often a source of data loss. When a third party stores, accesses, transfers, or conducts business for and with a company, there is a potential risk to the organization. The level of risk and the significant impact are closely linked

to the sensitivity and volume of transactions. Putrus (2017) argues that 63 percent of all data breaches are directly or indirectly associated with third-party access; that is, contractors and suppliers who require access to enterprise applications to complete their work pose a risk to any enterprise. The risk of potential data loss is heightened by the shift to the cloud and the increased ease of use of cloud service providers (CSPs) (Van Stone & Halpert, 2018).

Data loss is indicative of a weak security posture. Wlosinski (2018) identified the people, processes, and technological areas of potential weakness that lead to data loss or theft. The people weaknesses or insider threat may be intentional or unintentional. Process weaknesses can be due to poor oversight or negligence. Technological weaknesses are intentional, unintentional, or result from problems associated with design, implementation, or tool limitation. These weaknesses can be seen as organizational vulnerabilities and reflect the ease with which data can be copied, transmitted, stolen, and accessed by unauthorized persons or large state actors. From the foregoing, the data security defenses put in place by pharmaceutical organizations to prevent data loss are not completely effective. Drug manufacturers and their regulators share responsibility for data security and bear the financial and reputational consequences of a breach.

**Unauthorized Denial of Use.** Drug manufacturing organizations and their industry regulators require their systems to be available at all times due to the essential services they provide. Consequently, they are turning to cloud services, platforms, and data that can be accessed anytime and anywhere (Aljawarneh & Yassein, 2016). The current regulatory review process for some pharmaceutical companies involves the transmission of data sets, documentation, and regulatory submissions from the drug manufacturer to the relevant regulatory bodies (Robertson et al., 2020). However, the drug regulatory submission and review process is evolving with the transition to a globally accessible information-sharing cloud platform. Also, some drug manufacturers are creating internal cloud-based solutions to

manage regulatory information and clinical research data (Robertson et al., 2020). These complex automation solutions took years to reach acceptable maturity. Similarly, major regulatory agencies, such as the European Medicines Agency and the FDA, have announced initiatives to upgrade their IT infrastructure and have integrated cloud-based platforms into their strategies (Robertson et al., 2020).

Cloud computing provides cost-effective computing services and data storage. The expense associated with this emerging technology is more appealing compared to establishing an IT infrastructure (Aldossary & Allen, 2016). Cloud service providers (CSPs) offer resources that are shared among multiple cloud service clients (CSCs). As the popularity of the cloud grows, cloud-based enterprise resource planning (ERP) and Software-as-a-Service systems have emerged as alternatives to traditional on-premises ERP systems (Saa et al., 2017). BioDerm, a medical device manufacturer, and TriRx Pharmaceutical Services, a contract development and manufacturing organization, are examples of life science companies that have adopted cloud ERP solutions (BioDermByDesign customer, n.d.; TriRx success story, n.d.). However, the pharmaceutical industry's increasing reliance on cloud computing for data storage, processing, and application deployment presents emerging cybersecurity challenges (Khan et al., 2025). According to Aljawarneh and Yassein (2016), the cloud exposes businesses to potentially greater software security threats, especially when the cloud is Internet-based as opposed to being hosted on an organization's platform. Cloud solutions present an unacceptably high risk (Nye, 2015), along with data security issues and concerns, particularly for pharmaceutical companies that migrate their ERP systems to the cloud. According to Saa et al. (2017), unavailability is often a significant drawback of any cloud-based ERP system. When an attacker exhausts all available resources, other tenants cannot utilize them, potentially delaying access. Also, cloud service customers affected by a botnet may negatively influence

the availability for others. Nye (2015) notes that challenges related to service availability in today's extended enterprises also manifest in the cloud, similar to other outsourced solutions.

Furthermore, data storage on a remote server raises security concerns regarding data availability when needed. Data availability entails a commitment that whenever data is required by CSCs, it will be promptly accessible (Kumar et al., 2018). However, when storage is outsourced, CSCs lose physical control of the data while it is stored on a remote server and entrusted to untrusted CSPs or third parties. Loss of availability can occur due to data loss and inaccessible information (Kumar et al., 2018). Some unreliable vendors may create free space by deleting less frequently used or accessible data. Such threats can jeopardize data availability.

Furthermore, malicious individuals consistently attempt to temporarily or permanently disrupt or halt the services of prominent web servers and other Internet-connected hosts, negatively impacting data availability. These attacks render computers, network resources, and data inaccessible to users. For instance, a former employee of Shionogi, a Japanese pharmaceutical company, exploited previously obtained credentials to delete the contents of fifteen virtual servers. The cyberattack was so disruptive that it brought the company's operations to a standstill for several days, halting product shipments, payroll processing, and even email communication. The incident caused an estimated \$800,000 in damages (Robert, 2014). Such an attack may be classified as a denial-of-service (DoS) attack. As Chapple et al. (2018) explain, a DoS attack is "an attack that attempts to prevent authorized use of a resource" (p. 109), effectively blocking legitimate access to critical systems and information.

Ransomware attacks, such as NotPetya and WannaCry, also function as DoS attacks, although they target computer data rather than network connections. Merck, the pharmaceutical giant, was one of the public enterprises directly affected by the NotPetya attack. NotPetya temporarily disrupted research, manufacturing, and sales operations, preventing Merck from fulfilling orders for some products, including vaccines for the Centers

for Disease Control and Prevention and cancer prevention (Chopra, 2021; Crosignani et al., 2023; Khan et al., 2025). Operations were interrupted for two weeks (Chopra, 2021), resulting in significant catastrophic damage. By the end of 2017, Merck estimated \$870 million in damages due to the attack (Chopra, 2021; Khan et al., 2025). Merck's share price also dropped 5% after revealing NotPetya's impact (Crosignani et al., 2023). According to Bertino & Sandhu (2005), where data is unavailable, information essential to the organization's proper functioning is not readily accessible as required.

The unauthorized disclosure, modification, or unavailability of data resulting from the growing wave of security breaches in the pharmaceutical industry not only has an economic impact but also poses a health concern. Failing to protect data could diminish the value of a pharmaceutical company's products, services, and brand, restrict consumers' access to life-saving products and services, and negatively impact the health of the economy. The types of data at risk—PIIs, IPs, and sensitive business-critical information—underscore the growing need for robust security frameworks and governance strategies.

### **2.3 Governance and Management of Information Technology**

The growing reliance on technology has made IT vital for daily operations. In addition to reducing costs and fostering better-informed employees, organizations are seeking competitive advantages through IT investments. However, businesses have frequently struggled to realize the anticipated value of strategic IT investments (Wende & Otto, 2007). Henderson and Venkatraman (1993) suggest that this challenge stems from inadequate alignment between business and IT strategies. Successful initiatives necessitate the collaborative efforts of business and technology experts that are directed, coordinated, and governed through IT governance arrangements (Sambamurthy & Zmud, 1999). Weill and Ross (2004) describe IT governance as the clarification of decision-making rights and accountability framework to promote appropriate behavior in IT use. Therefore, governance defines who

will be responsible for key IT decisions and how they will be held accountable. IT governance aims to enhance the alignment of business activities with IT (Van Grembergen et al., 2003a).

### **2.3.1 Information Technology Governance**

The concept of IT governance has existed for less than four decades. In the early 1990s, key aspects of IT governance were identified in academic literature. The first aspect examined alternative ways of organizing the IT function and their impact on business outcomes (Jarvenpaa & Ives, 1993). Another aspect explored the nature and impact of alignment between businesses, i.e., enterprise consumers of IT services and the IT function (Henderson & Venkatraman, 1993; Luftman, 1996; Venkatraman et al., 1993). The third aspect focused on the linkages between enterprise strategy, IT investment, and corporate performance (Andreu & Ciborra, 1996; Chan et al., 1997; Weill, 1990; 1992). This aspect gained considerable momentum, with researchers reacting to Brynjolfsson's (1993) study that highlighted an apparent paradox between the high levels of IT investment and a lack of evidence regarding the return on that investment. It was not until the late 1990s that the title or abstract of articles mentioned IT governance (Brown, 1997; Sambamurthy & Zmud, 1999), although these documents primarily addressed debates about the most effective form of IT organization.

**Information Technology Governance Models.** Previous research on IT governance highlights the importance of aligning IT governance arrangements with the broader context of the enterprise. Researchers explored the relationship between an organization's IT governance design and its contextual factors. The underlying proposition is that there is no one-size-fits-all design for IT governance applicable to all enterprises, and contextual factors influence how IT governance enhances business performance (Wende & Otto, 2007). In response to this contingency approach, IT governance research produced models tailored to different sets of contingencies. Wende and Otto (2007) presented two IT governance models: centralized and

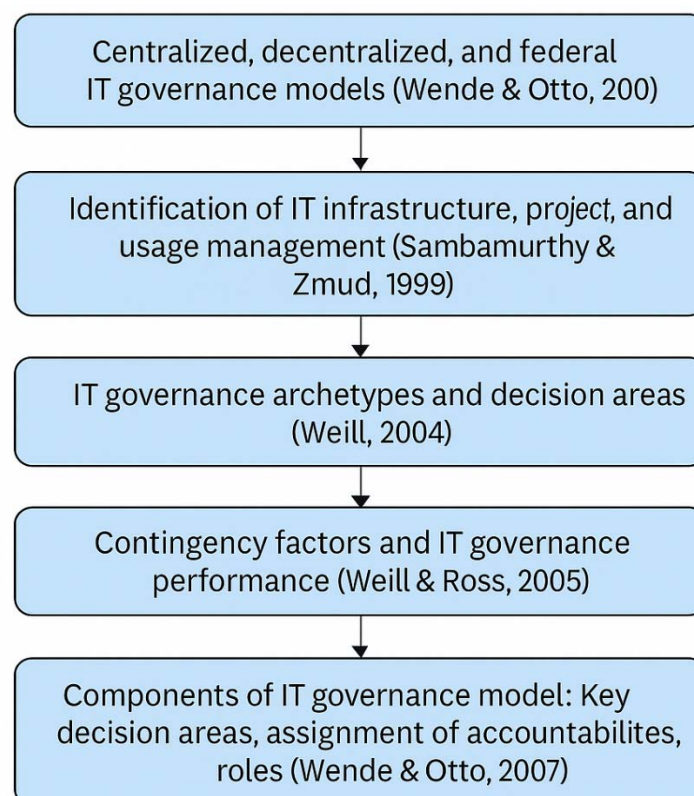
decentralized. In the centralized model, corporate IT handles all IT functions, while in decentralized models, those tasks are managed by the business units' IT (Ein-Dor & Segev, 1982). The federal model is a third option that differentiates between two types of IT functions—IT management is centralized, whereas IT usage management is decentralized to business units (Boynton & Zmud, 1987). According to Earl (1989), the federal form is associated with multi-division enterprises' hybrid (including matrix) structures. Subsequent research identified more precise IT governance models, recognizing diverse IT functions and the participation of various organizational levels. Sambamurthy and Zmud (1999) introduced a third type of IT function, distinguishing between IT infrastructure management, project management, and IT usage management. The rationale for IT governance evolved from focusing on the performance of IT functions to emphasizing authority over IT decision-making within those functions. Brown (1997) shifted the focus from the organizational level to the business unit level. The hybrid model she proposed specified that the IT usage function is decentralized to certain business units within an enterprise, but not all. Furthermore, Weill's (2004) IT governance archetypes provide a more detailed view of IT governance models. First, instead of corporate IT and line IT organizational units, he considers senior business executives, business unit heads/process owners, and corporate and business unit IT professionals as having decision-making authority for IT management functions. Second, he identifies five key decision areas: IT principles, infrastructure strategies, IT architecture, IT infrastructure strategies, and the prioritization of business application IT investments. He also enhances IT governance models by introducing a third element: the distinction between decision-making and entry rights. However, he limited the range of potential combinations of these three dimensions to six mutually exclusive archetypes (Wende, 2007). Although the archetypes define IT governance at the enterprise level, Weill suggested that governance of IT in large organizations should be designed and evaluated by regional groups or business units



at the business unit level. Weill (2004) also identified several factors that influence IT governance but did not clarify how these factors affect the IT governance archetypes. Subsequently, Weill and Ross (2005) partially addressed this gap by analyzing the performance of contingency factors. Wende (2007) summarizes the IT governance research proposal with three components of IT governance model: key decision areas, assignment of accountabilities, and roles. IT governance models can be designed with these components across various organizational levels (Wende & Otto, 2007). Once an IT governance model is chosen and put into practice, it is anticipated to enable IT to support and enhance business objectives, meaning it facilitates business/IT alignment. The evolution of IT governance models is illustrated in Figure 8.

**Figure 8**

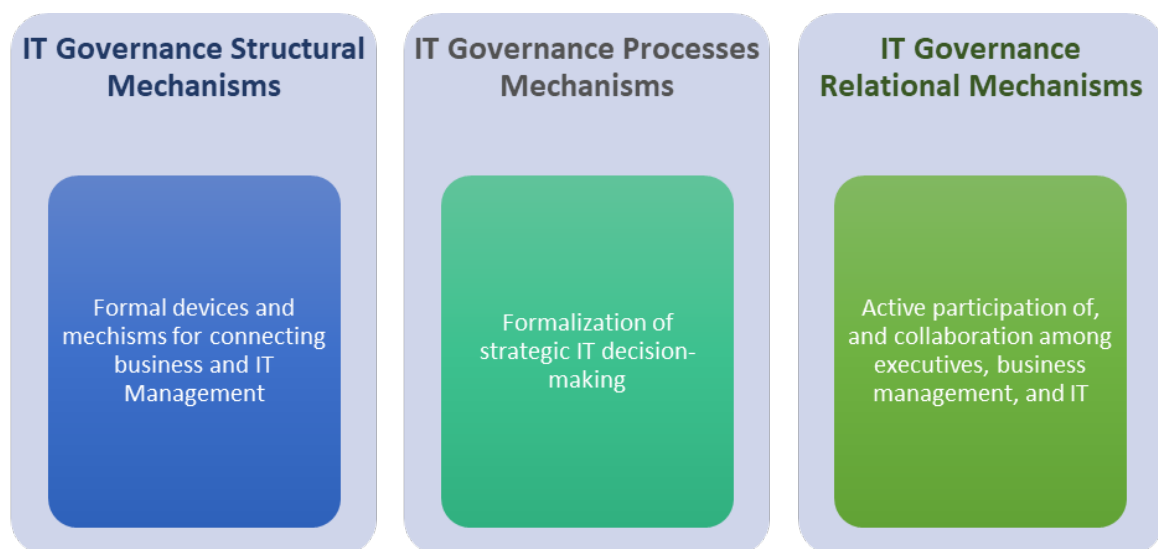
*Evolution of IT Governance Models*



**Information Technology Governance Implementations.** IT governance encompasses leadership, organizational structures, and processes that enable an organization's IT to support and sustain its strategy and objectives (Van Grembergen, 2001). A comprehensive view of IT governance recognizes its complex and dynamic nature, consisting of interdependent subsystems that form a powerful whole (Peterson, 2004; Sambamurthy & Zmud, 1999). Peterson et al. (2002), Van Grembergen et al. (2003a), and Weill and Ross (2004) have all indicated that IT governance can be achieved by integrating structural, process, and relational mechanisms, as shown in Figure 9.

**Figure 9**

*IT Governance Subsystems*



**Note.** Based on the IT governance implementation discussion in “Crafting Information Technology Governance,” by R. Peterson, 2004, *Information systems management*, 21(4), pp. 7-22 (<https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2>)

According to Peterson (2004), who studied IT governance design at Johnson & Johnson, IT governance structures include “structural (formal) devices and mechanisms for connecting and enabling horizontal, or liaison, contacts between business and IT management (decision-making) functions” (p. 14), such as IT steering committees and IT project

committees. IT governance processes involve the "formalization and institutionalization of strategic IT decision-making or IT monitoring procedures" (p. 15), such as balanced scorecard analysis. Relational mechanisms relate to "the active participation of, and collaborative relationship among, corporate executives, IT management, and business management" (p.15), such as business/IT job rotation and co-location.

IT governance occurs at multiple levels within an organization. As Van Grembergen et al. (2003a) notes, IT governance is strategically positioned at the board level, within senior management and the C-suite, and finally at the operational level involving business management and IT operations. Effective implementations of IT governance enhance enterprise performance. Companies with strong IT governance outperform their competitors, achieving a 40% higher return on IT investments (Weill & Ross, 2004).

**Information Technology Governance and Management.** IT governance and IT management are distinct. Peterson (2004) clearly differentiates IT governance from IT management. He asserts that IT management focuses on the efficient and effective provision of IT products and services internally, as well as the management of current IT operations. According to ISACA (2019), IT management involves overseeing IT operational and resource concepts. This description implies day-to-day decision-making and implementation activities related to the enterprise's use of IT. Generally, management plans, develops, executes, and monitors activities as directed by the governing body to achieve corporate objectives. Thus, IT management ensures that IT continues to support these objectives.

In contrast, IT governance enables the enterprise to maintain and extend its strategies and goals. Korac-Kakabadse and Kakabadse (2001) note that IT governance, as a subset of enterprise governance, "assists in the achievement of corporate success by both efficiently and effectively deploying secure and reliable information through the application of technology" (p. 9). Furthermore, IT governance is broader in scope, focusing on IT performance and

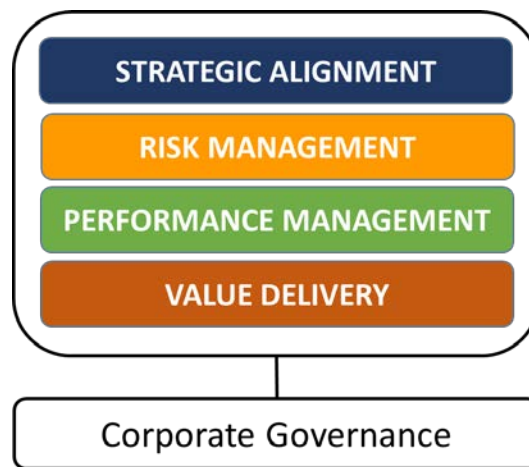
transformation to meet both current and future business needs, addressing internal and external requirements (De Haes & Van Grembergen, 2009). As a critical component of a comprehensive enterprise and corporate governance program, IT governance aims to provide strategic direction, ensure objectives are met, manage risks effectively, and verify the responsible use of resources (ISACA, 2019).

### 2.3.3 Enterprise Governance of IT

IT governance has evolved significantly in recent years. Wilkin and Chenhall (2010) established a taxonomy of IT governance in an IT governance survey. They identified key enablers of IT governance as strategic alignment, risk management, performance measurement, and value delivery, as shown in Figure 10.

**Figure 10**

*Enablers of IT Governance*



**Note.** Based on the IT governance enablers discussion in “A Review of IT Governance: A Taxonomy to Inform Accounting Information Systems,” by C. L. Wilkin & R. H. Chenhall, 2010, *Journal of Information Systems*, 24 (2), pp. 107-146.

(<https://doi.org/10.2308/jis.2010.24.2.107>)

Additionally, they recognized corporate governance as a crucial influence on how IT is governed. According to De Haes et al. (2013), this focus on corporate governance was driven

by two trends in academic and professional circles. First, the rising importance of corporate governance in general management, academic literature, and professional guidance has impacted IT governance research. Second, the increasing significance of IT in achieving business objectives, along with the inherent tension in aligning business and IT management, led to a recognition of the necessity for establishing IT goals and decision-making rights at the governance level. These factors prompted a shift in terminology from IT governance to enterprise governance of IT (EGIT). Van Grembergen and De Haes (2009) defined EGIT as the “board overseeing the definition and implementation of processes, structures, and relational mechanisms in the organization that enable both business and IT to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled investments.” (p. 3). This definition specifies that EGIT's responsibility lies with the board of directors and executive management. According to ISACA (2019), the governance of IT is the board's responsibility, while the delivery lies with senior management. Therefore, the board of directors overseeing this stewardship will rely on management for the implementation of the necessary IT systems and controls. Thus, EGIT focuses on the stewardship of IT resources on behalf of all stakeholders who expect their interests to be considered.

At its core, EGIT emphasizes delivering business value and effectively managing risk. Achieving this value hinges on the strategic alignment between business and IT. As ISACA (2019) explains, the purpose of EGIT is to guide IT efforts so they align with enterprise goals and contribute to the realization of expected benefits. IT should empower organizations to seize opportunities, maximize benefits while responsibly managing resources. Furthermore, effective IT risk management requires embedding corporate accountability into governance practices. Ultimately, value creation through IT depends on balancing benefits, risks, and resources. ISACA (2019) underscores that fulfilling stakeholder needs and generating value is

the central aim of any IT governance system, an objective that necessitates the implementation of an EGIT framework.

#### **2.3.4. Enterprise Governance of IT Frameworks**

An organization's success or failure often hinges on how effectively it adopts and utilizes technology. Implementing a well-structured EGIT framework enables enterprises to address business challenges by ensuring proper governance and management of IT. De Haes et al. (2013) analyzed various corporate governance, IT governance, and IT management frameworks in terms of their level of abstraction and the extent to which they comprehensively address the IT life cycle—from governance system design to tactical IT management. They found that multipurpose corporate governance frameworks, such as COSO, are highly relevant but primarily address governance and organizational issues. They also observed that standards such as TickIT—which focuses on quality software development—are positioned at the tactical end of the spectrum, addressing only specific aspects of IT. While traditional frameworks like ITIL and CMMI have historically emphasized governance and operational tactics over strategic direction and management (Ahern et al., 2008; Cabinet Office, 2011), De Haes et al. (2013) noted that more recent versions have shifted toward a strategic focus, integrating key governance elements. As a result, these governance frameworks differ in scope and focus, highlighting the need for a comprehensive approach to IT governance.

The COBIT framework offers a comprehensive approach to IT governance and management. De Haes and Van Grembergen (2009) validated COBIT as an effective IT governance framework based on expert-reviewed structures, processes, and relational mechanisms. COBIT also aligns well with Management Control Theory. According to De Haes et al. (2013), the control concept within the COBIT framework is rooted in management control and management control systems. This concept also broadly aligns with Simon's (1990; 2000) perspective on management controls. For example, COBIT 3 defines control as “the policies,

procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected'' (IT Governance Institute [ITGI], 2000, p.12). Building on the literature on management control and management control systems, the following core concepts of the COBIT framework correspond with key principles of MCT:

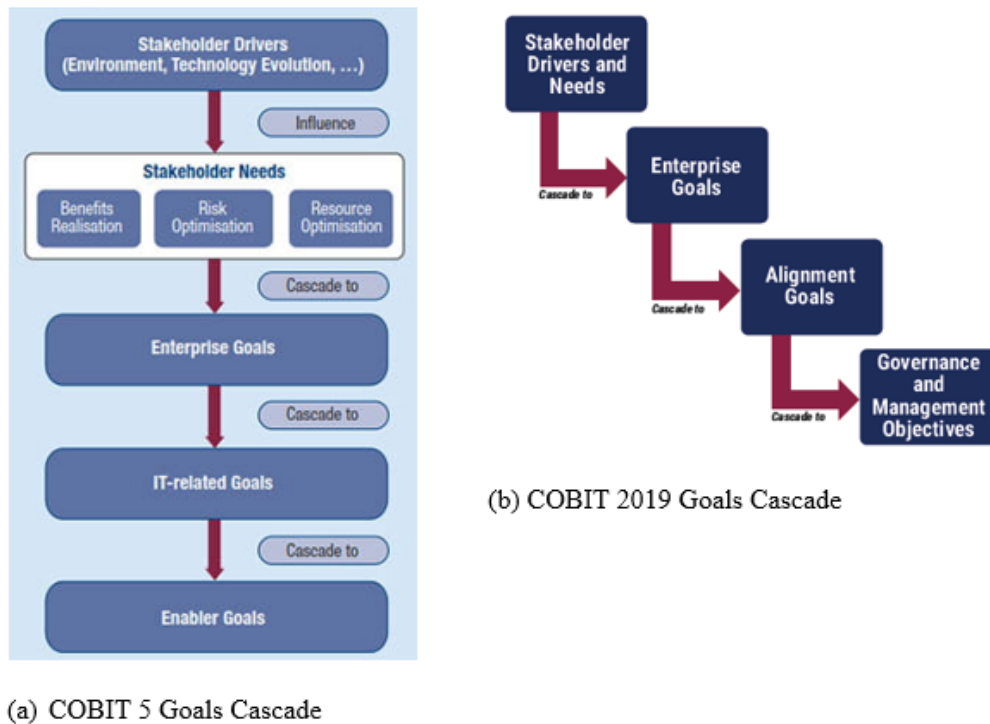
**Enterprise, IT-related, and Alignment Goals.** COBIT facilitates the alignment between a company's business goals and its use of IT. COBIT 5 specifies a cascade of goals that starts from a set of generic enterprise goals and proceeds to IT-related goals (De Haes et al., 2013a), shown in Figure 11, Panel a. ISACA (2012a) maintain these generic enterprise goals relate to a balanced stakeholder need, derive from balanced scorecard dimensions, and represent typical goals to which enterprise-specific goals are mapped. COBIT 5 assumes the specification of enterprise goals and their linkage to IT-related goals, and consequently to the IT processes within the framework, to facilitate alignment between business activities and IT. These relationships illustrate how IT-related goals contribute to achieving enterprise goals, which, in turn, influence IT-related goals. COBIT 2019 also showcased similar connections between its 13 alignment goals and 13 enterprise goals (ISACA, 2018a). A significant positive correlation exists between these alignment goals and enterprise goals (De Haes et al., 2020), as shown in Figure 11, Panel b, in that the level of achievement of alignment goals is linked to the degree of success of enterprise goals. Furthermore, the extent of achievement of each alignment goal is shaped by the level of success of a governance or management objective.

**Control Objectives.** The concept of control objectives is unique to COBIT. The COBIT 4.1 process model articulates control objectives as the definitive goal in establishing organizational structures, plans, policies, and procedures aimed at providing acceptable assurance for achieving business objectives, as well as preventing, detecting, and correcting

undesired events (ITGI, 2007). Control objectives imply establishing control that results in a required outcome (De Haes et al., 2013).

**Figure 11**

(a) COBIT 5 Goals and (b) COBIT 2019 Goals Cascades



**Note.** (a) From *COBIT 5 for Assurance* (p. 14), by ISACA, 2013b. Copyright 2013 by ISACA. Reprinted with permission. (b) From *COBIT 2019 Framework: Introduction and Methodology* (p. 28), by ISACA, 2018b, Copyright 2018 by ISACA. Reprinted with permission.

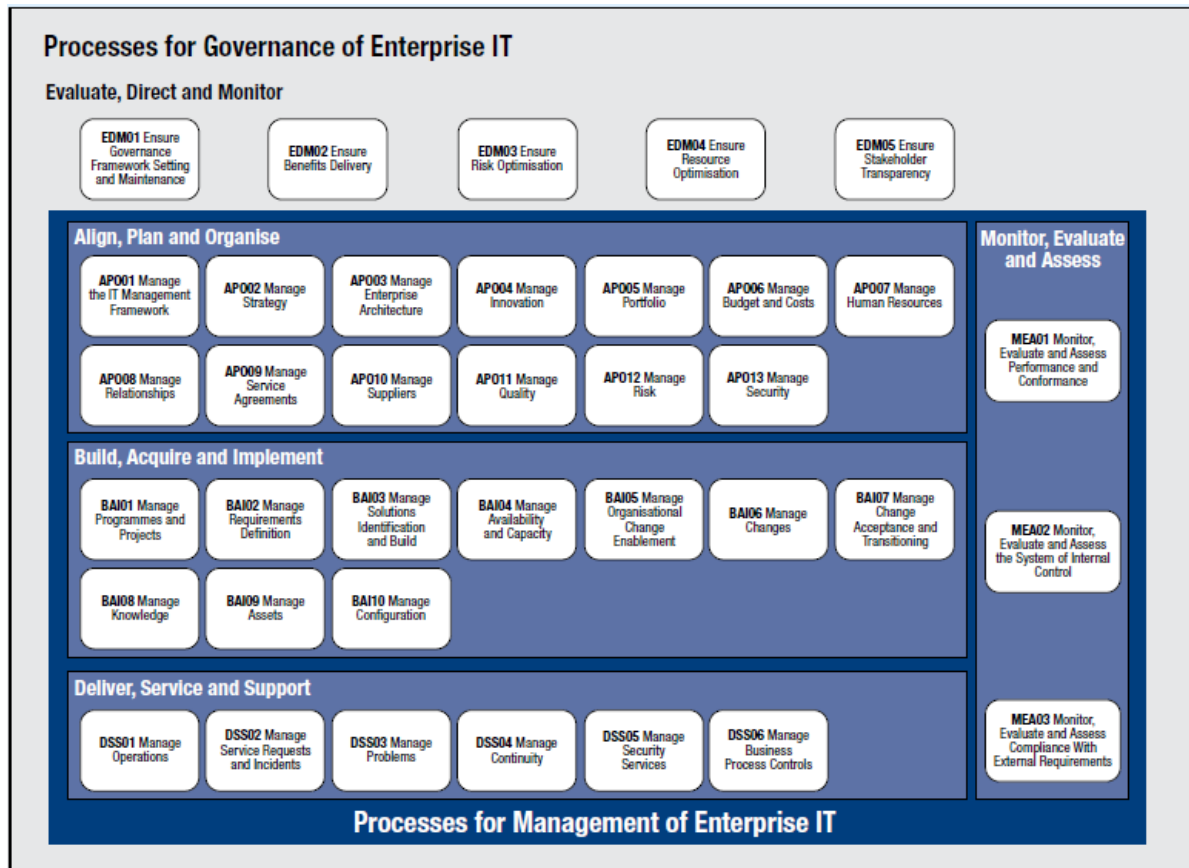
The COBIT 4.1 process model defines control objectives for 34 processes organized into four domains (ITGI, 2007), specifically, "Plan and Organize" (p. 29); "Acquire and implement" (p.73); "Deliver and Support" (p. 101), and "Monitor and Evaluate" (p.153). The COBIT 5 Process Reference Model, shown in Figure 12, succeeded the COBIT 4.1 process model and introduced 37 governance and management processes (ISACA, 2012b) categorized under high-level controlling objectives (Sihotang et al., 2019): "Evaluate, Direct and Organize



(EDM)”; “Align, Plan and Organize (APO)”; “Build, Acquire and Implement (BAI)”; “Deliver, Service and Support” and “Monitor, Evaluate and Assess (MEA)” (p.2).

**Figure 12**

*COBIT Reference Model*



*Note.* From *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT* (p. 14), by ISACA, 2013b. Copyright 2013 by ISACA. Reprinted with permission.

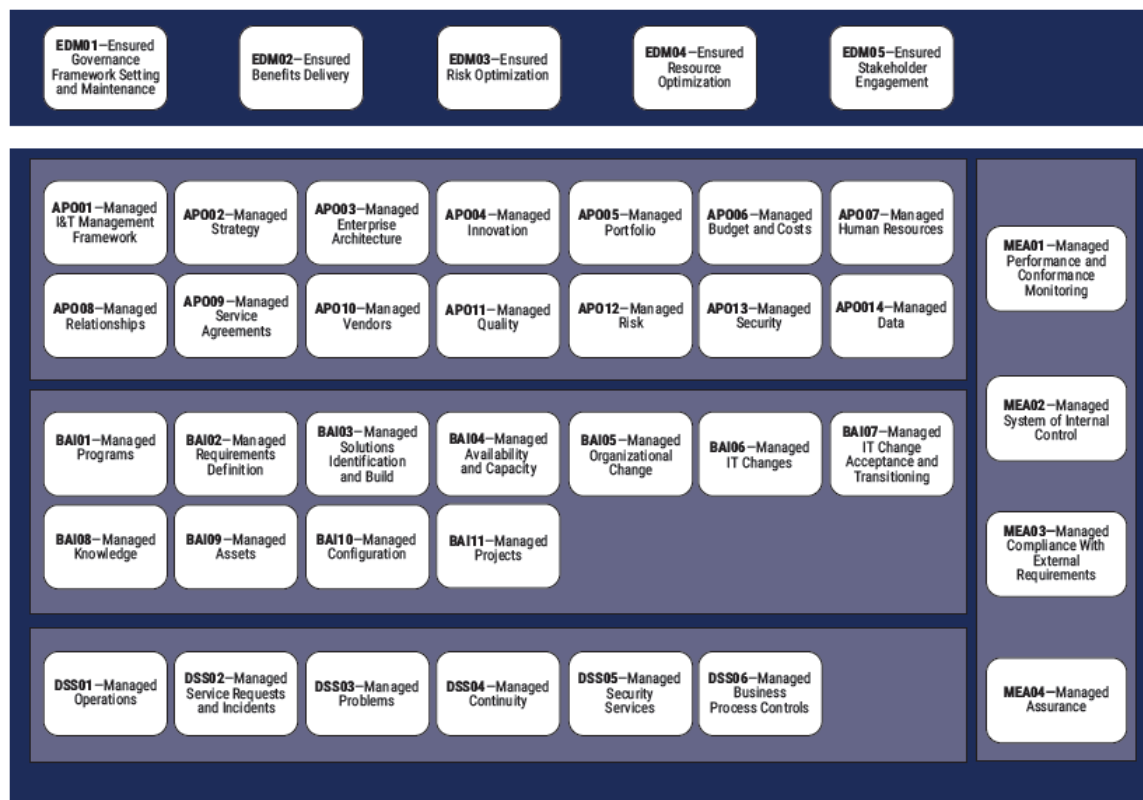
Control objectives are also presented as statements of purpose or intended outcomes designed to manage inherent risks. For example, “Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information” or “Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions” (Cybersecurity Audit Program, n. d.). They outline the behaviors, processes, technologies, and

documentation necessary to address these risks. Achieving a control objective requires controls in the form of organizational structures, policies, guidelines, procedures, or practices. For example “Integrity checking mechanisms are used to verify software, firmware and information integrity” (Cybersecurity Audit Program, n. d.). Controls may be administrative, technical, or legal in nature, while control activities can include system configurations, forms, reports, documentation, approval matrices, segregation of duties, and other related measures.

**Governance and Management Objectives.** COBIT 2019 Core Model defines 40 governance and management objectives, as shown in Figure 13, that must be achieved for information and technology (I&T) in support of enterprise goals (ISACA, 2018a).

**Figure 13**

*COBIT 2019 Core Model*



*Note.* From *COBIT 2019 Framework: Introduction and Methodology* (p. 21), by ISACA, 2018b. Copyright 2018 by ISACA. Reprinted with permission.

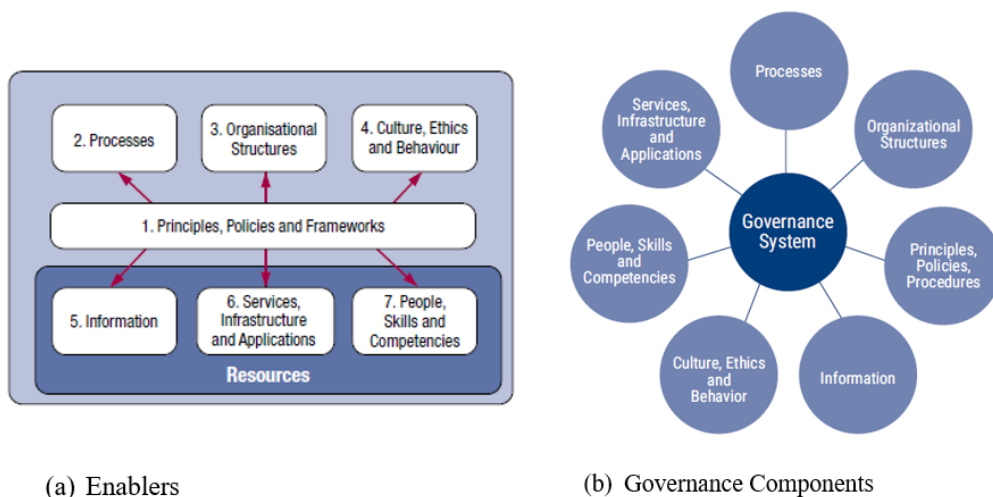
In this model, a governance or management objective corresponds to a process, meaning an objective is linked with a process and vice versa. Similar to the groupings in the COBIT 5 Process Reference Model, the COBIT 2019 Core Model categorizes governance objectives within the EDM domain, while management objectives fall under the APO, BAI, DSS, and MEA domains. Unlike the COBIT 5 Process Reference Model, the COBIT 2019 Core Model introduces ‘Managed Data,’ ‘Managed Projects,’ and ‘Managed Assurance’ as new governance and management objectives (De Haes et al., 2020). Also, COBIT 2019 states that each governance or management objective is supported by various governance components—previously referred to as “enablers” in COBIT 5—that work together to facilitate the achievement of that objective.

**Enablers and Governance Components.** COBIT 5 incorporates both formal and informal mechanisms into its framework, recognizing them as enablers. De Haes et al. (2013) identified organizational structures, processes, ethics, culture, and behavior as enablers that contribute individually and collectively to the achievement of corporate IT governance and management. COBIT 5 identified enablers, as shown in Figure 14, Panel a, that facilitate the achievement of IT-related goals (ISACA, 2012b): “principles, policies and frameworks,” “processes,” “organizational structures,” “culture, ethics and behavior,” “information,” “services, infrastructure and applications,” and “people, skills and competencies” (p. 15). These enablers support risk management and the creation of business value from IT usage (De Haes et al., 2013). Enablers are synonymous with governance components in COBIT 2019. ISACA (2018) identified these components as “organizational structures, processes, policies and procedures, information items, culture and behavior, skills and competencies, and services, infrastructure, and applications” (p. 12), as shown in Figure 14, Panel b, which work together to meet governance and management objectives.

The process component in particular, is generally seen as highly effective, though it is also the most challenging for organizations to implement (Huygh et al., 2018). Processes are crucial for ensuring compliance with external legislation and regulations. Huygh et al. (n. d.) explored how compliance requirements influence IT governance implementation and identified key governance and management processes needed at different compliance levels. He observed that meeting compliance requirements demanded more mature IT governance and management. He also emphasized that security and assurance processes are especially critical under stricter regulations and that organizations must demonstrate adherence through clear, documented, and controlled processes.

**Figure 14**

(a) *COBIT 5 Enablers* and (b) *COBIT 2019 Governance Components*



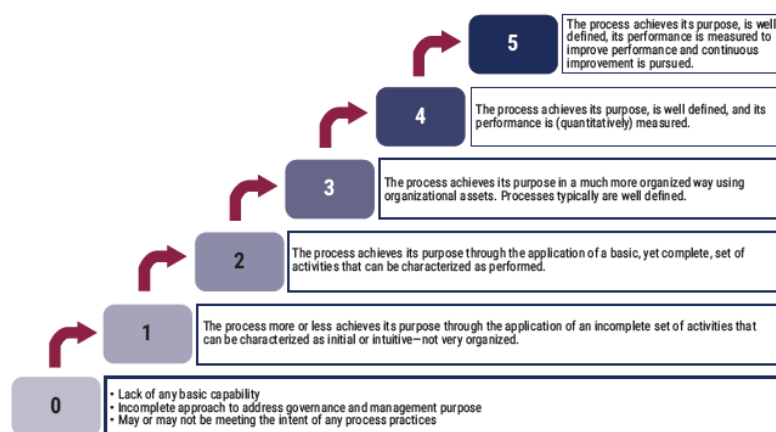
**Note.** (a) From *COBIT 5 for Assurance* (p. 27), by ISACA, 2013b. Copyright 2013 by ISACA. Reprinted with permission. (b) From *COBIT 2019 Framework: Introduction and Methodology* (p. 22), by ISACA, 2018b, Copyright 2018 by ISACA. Reprinted with permission.

Also, the process component encompasses various government or management practices, each comprising one or more activities to execute the process (De Haes et al., 2020). The degree to which these activities are performed determines a process's ability to apply good

practices and achieve its goals. According to ISACA (2018), the COBIT 2019 Core Model provides a capability measurement, similar to the COBIT 5 Process Reference Model, for any given process, as shown in Figure 15. This framework is based on Capability Maturity Model Integration (CMMI) and offers capability levels ranging from 0 to 5, which help determine the extent of process implementation and performance. The COBIT 2019 Core Model outlines specific activities that are at least necessary to attain a particular level of process capability. Each activity within the process practices is assigned a level of capability. A process reaches a specific capability level once all activities designated for that level (and for lower levels of capability) are successfully completed (De Haes et al., 2020).

**Figure 15**

*Capability Levels for Processes*



*Note.* From *COBIT 2019 Framework: Introduction and Methodology* (p. 39), by ISACA, 2018b. Copyright 2018 by ISACA. Reprinted with permission.

**Performance Outcome.** A robust measurement process must be implemented to ensure that stakeholder needs are met effectively. To facilitate Simons' (1990, 2000) feedback system—formal diagnostic control systems that monitor organizational outcomes and correct variances from expected performance standards—COBIT builds on the balanced scorecard concept (ISACA, 2012b). COBIT relies on the balanced scorecard concepts developed by

Kaplan and Norton (1996) and adapted to the IT field by Van Grembergen et al. (2003) and Hu and Huang (2006). COBIT 5 organizes enterprise and IT-related goals according to the balanced scorecard dimensions—financial, internal processes, customer, and learning and growth—along with their associated performance metrics (De Haes et al., 2013; ISACA, 2012b). These metrics are applied at the IT process level. For example, Figure 16 presents the metrics of enterprise and IT-related goals, as well as those of the Manage Risk process. Building also on the balanced scorecard concept, the COBIT 2019 Core Model provides metrics to evaluate outcomes for each enterprise and alignment goal (ISACA, 2018a). Additionally, the model includes metrics for process practices related to each governance or management objective. These metrics serve as outcome measures for each process practice, support the measurement of their achievement, and allow for the assessment of their contribution toward a specific objective (De Haes et al., 2020). Figure 17 presents the metrics of enterprise and alignment goals, as well as those of the Managed Data objective. By consolidating all these measures at the enterprise goals, alignment goals, and practice levels, a comprehensive and balanced scorecard is developed across the enterprise (De Haes et al., 2020). Therefore, the balanced scorecard serves as a comprehensive tool for evaluating whether stakeholder needs are being met and corporate goals are being achieved.

Pharmaceutical companies like GSK have adopted the COBIT framework to strengthen IT governance. Following the creation of its global support organization, GSK used COBIT 4.1 to evaluate governance processes, ensuring alignment with strategic and corporate goals (Williamson, 2014). The application support department tailored COBIT by selecting relevant processes and mapping them to IT governance focus areas, identifying key risks, control objectives, and implementation strategies. Framing the model in a familiar business context made it accessible to users with limited COBIT knowledge. This approach enabled GSK to

detect vulnerabilities, assess controls effectively, and enhance program performance through ongoing monitoring.

**Figure 16**

*Metrics for (a) Enterprise Goals, (b) IT-related Goals, and (c) Managed Risk*

BSC Dimension	Enterprise Goal	Metric
Financial	1. Stakeholder value of business investments	<ul style="list-style-type: none"> <li>Percent of investments where value delivered meets stakeholder expectations</li> <li>Percent of products and services where expected benefits are realised</li> <li>Percent of investments where claimed benefits are met or exceeded</li> </ul>
	2. Portfolio of competitive products and services	<ul style="list-style-type: none"> <li>Percent of products and services that meet or exceed targets in revenues and/or market share</li> <li>Ratio of products and services per life cycle phase</li> <li>Percent of products and services that meet or exceed customer satisfaction targets</li> <li>Percent of products and services that provide competitive advantage</li> </ul>
	3. Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> <li>Percent of critical business objectives and services covered by risk assessment</li> <li>Ratio of significant incidents that were not identified in risk assessments vs. total incidents</li> <li>Frequency of update of risk profile</li> </ul>

(a) Enterprise Goals and Metrics

BSC Dimension	IT-related Goal	Metric
Financial	01 Alignment of IT and business strategy	<ul style="list-style-type: none"> <li>Percent of enterprise strategic goals and requirements supported by IT strategic goals</li> <li>Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services</li> <li>Percent of IT value drivers mapped to business value drivers</li> </ul>
	02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> <li>Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss</li> <li>Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment</li> <li>Number of non-compliance issues relating to contractual agreements with IT service providers</li> <li>Coverage of compliance assessments</li> </ul>

(b) IT-related Goals and Metrics

AP012 Manage Risk		Area: Management Domain: Align, Plan and Organise
<b>Process Description</b> Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.		
<b>Process Purpose Statement</b> Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.		
<b>The process supports the achievement of a set of primary IT-related goals:</b>		
IT-related Goal	Related Metrics	
02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> <li>Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss</li> <li>Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment</li> <li>Number of non-compliance issues relating to contractual agreements with IT service providers</li> <li>Coverage of compliance assessments</li> </ul>	
04 Managed IT-related business risk	<ul style="list-style-type: none"> <li>Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment</li> <li>Number of significant IT-related incidents that were not identified in risk assessment</li> <li>Percent of enterprise risk assessments including IT-related risk</li> <li>Frequency of update of risk profile</li> </ul>	

(c) Manage Risk Process and Related Metrics

**Note.** Metrics cascade from enterprise goals all the way to processes. (a, b, c) From *COBIT*

*5: Enabling Processes* (pp. 16, 17, 107), by ISACA, 2012b. Copyright 2013 by ISACA.

Reprinted with permission.



**Figure 17**

*Metrics for (a) Enterprise Goals, (b) Alignment Goals, and (c) Managed Data*

Reference	BSC Dimension	Enterprise Goal	Example Metrics
EG01	Financial	Portfolio of competitive products and services	<ul style="list-style-type: none"> <li>Percent of products and services that meet or exceed targets in revenues and/or market share</li> <li>Percent of products and services that meet or exceed customer satisfaction targets</li> <li>Percent of products and services that provide competitive advantage</li> <li>Time-to-market for new products and services</li> </ul>
EG02	Financial	Managed business risk	<ul style="list-style-type: none"> <li>Percent of critical business objectives and services covered by risk assessment</li> <li>Ratio of significant incidents that were not identified in risk assessments vs. total incidents</li> <li>Appropriate frequency of update of risk profile</li> </ul>

(a) Enterprise Goals and Metrics

Reference	IT BSC Dimension	Alignment Goal	Metrics
AG01	Financial	I&T compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> <li>Cost of IT noncompliance, including settlements and fines, and the impact of reputational loss</li> <li>Number of IT-related noncompliance issues reported to the board or causing public comment or embarrassment</li> <li>Number of noncompliance issues relating to contractual agreements with IT service providers</li> </ul>
AG02	Financial	Managed I&T-related risk	<ul style="list-style-type: none"> <li>Appropriate frequency of update of risk profile</li> <li>Percent of enterprise risk assessments including I&amp;T-related risk</li> <li>Number of significant I&amp;T-related incidents that were not identified in a risk assessment</li> </ul>

(b) Alignment Goals and Metrics

Domain: Align, Plan and Organize Management Objective: AP014 – Managed Data		Focus Area: COBIT Core Model
<b>Description</b>		
Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.		
<b>Purpose</b>		
Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.		
<b>The management objective supports the achievement of a set of primary enterprise and alignment goals:</b>		
<b>Enterprise Goals</b>	➔	<b>Alignment Goals</b>
<ul style="list-style-type: none"> <li>EG04 Quality of financial information</li> <li>EG07 Quality of management information</li> </ul>		AG10 Quality of I&T management information
<b>Example Metrics for Enterprise Goals</b>		<b>Example Metrics for Alignment Goals</b>
EG04 a. Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information b. Cost of noncompliance with finance-related regulations		AG10 a. Level of user satisfaction with quality, timeliness and availability of I&T-related management information, taking into account available resources b. Ratio and extent of erroneous business decisions in which erroneous or unavailable I&T-related information was a key factor c. Percentage of information meeting quality criteria
EG07 a. Degree of board and executive management satisfaction with decision-making information b. Number of incidents caused by incorrect business decisions based on inaccurate information c. Time to provide information supporting effective business decisions d. Timeliness of management information		

(c) Manage Data Objective and Related Metrics

**Note.** Metrics cascade from enterprise goals to objectives (a, b) From *COBIT 2019*

*Framework: Introduction and Methodology* (pp. 29, 30), by ISACA, 2018b. Copyright

2018 by ISACA. Reprinted with permission; (c) From *COBIT 2019 Framework:*

*Governance and Management Objectives* (p. 143), by ISACA, 2018a, Copyright 2018 by

ISACA. Reprinted with permission



Designing and implementing an I&T governance solution for manufacturing was one of the use cases developed by ISACA (2018c) through the COBIT 2019 governance system design process. As such, drug manufacturing organizations can similarly leverage the updated COBIT framework to strengthen their IT governance practices.

## **2.4 Data Life Cycle, Management, and Governance**

Data management and governance are essential for organizational competitiveness and sustainability. According to Pearce (2017), the advantages of these practices extend to strategy, sales, marketing, finance, audit, compliance, business intelligence, analytics, reporting, and cybersecurity. Furthermore, the significance of data management and governance cannot be overstated when it comes to protecting sensitive data in a drug manufacturing context.

### **2.4.1 Manufacturing Product Life Cycle and Big Data**

The product life cycle encompasses the entire process of a product, from creation to disposal. Chhetri et al. (2017) identified the stages of the product life cycle within the context of Industry 4.0, which include design, prototyping, ordering, industrial processing, sales, and maintenance. They also emphasized the enabling technologies that support these stages, such as advanced robotics, smart sensors, cyber-physical systems, additive manufacturing, the Internet of Things, cloud computing, machine learning (ML), big data analytics, and augmented reality. Tao et al. (2018) presented a more detailed manufacturing product life cycle. They asserted that each stage of the manufacturing product life cycle involves unique activities, which engage relevant departments and personnel and generate substantial amounts of data. Table 1 offers an overview of the data assets commonly utilized in manufacturing. These data assets progress through the data life cycle, and protecting them is essential to operational integrity and competitive advantage.

**Concept Generation.** The development of new product concepts or improvements is informed by customer preferences, market insights, investment strategies, and other sources.

**Table 1***Data Assets of the Manufacturing Product Life Cycle*

<b>Manufacturing product life cycle stages</b>	<b>Activity</b>	<b>Data required</b>	<b>Data generated</b>
Concept Generation	<ul style="list-style-type: none"> <li>Formulate the concept for new products or product enhancements</li> </ul>	<ul style="list-style-type: none"> <li>Customer preferences</li> <li>Market insights</li> <li>Investment strategies</li> </ul>	<ul style="list-style-type: none"> <li>Customer feedback</li> <li>Customer satisfaction survey results</li> <li>Product sales volume</li> <li>Investment planning</li> </ul>
Product Design	<ul style="list-style-type: none"> <li>Design the product's functionality, appearance, and structure</li> </ul>	<ul style="list-style-type: none"> <li>Descriptions of product functions</li> <li>Design parameters</li> <li>Appearance</li> <li>Configurations</li> <li>Test results</li> <li>Faults from similar products</li> </ul>	<ul style="list-style-type: none"> <li>Product blueprints</li> <li>Prototypes</li> </ul>
Raw Material Procurement	<ul style="list-style-type: none"> <li>Develop suitable procurement plans</li> </ul>	<ul style="list-style-type: none"> <li>Quotes</li> <li>Substitutes</li> <li>Material availability</li> <li>Potential suppliers</li> </ul>	<ul style="list-style-type: none"> <li>Type, quantity, and quality of raw materials,</li> <li>Supplier data (pricing, inventory levels, and distance)</li> </ul>
Manufacturing	<ul style="list-style-type: none"> <li>Create product by processing or assembling raw materials or components</li> </ul>	<ul style="list-style-type: none"> <li>Design specifications</li> </ul>	<ul style="list-style-type: none"> <li>Production parameters</li> <li>Attributes, performance data, and process conditions of production factors</li> </ul>
Transportation	<ul style="list-style-type: none"> <li>Transport product</li> </ul>	<ul style="list-style-type: none"> <li>Market demand</li> <li>Orders</li> </ul>	<ul style="list-style-type: none"> <li>Inventory levels</li> <li>Location data</li> <li>Order fulfillment status</li> </ul>
Sales	<ul style="list-style-type: none"> <li>Launch and market product</li> </ul>	<ul style="list-style-type: none"> <li>Supplier data</li> <li>Inventory data</li> <li>Customer data</li> <li>Order data</li> </ul>	<ul style="list-style-type: none"> <li>Customer preferences</li> <li>Insights from preference group</li> <li>Regional order distribution</li> </ul>
Utilization	<ul style="list-style-type: none"> <li>Operate or use product</li> </ul>	<ul style="list-style-type: none"> <li>User manual</li> <li>Product usage guidelines</li> </ul>	<ul style="list-style-type: none"> <li>Product status</li> <li>User behavior</li> <li>Operational conditions and environmental data</li> </ul>
After-sales Service	<ul style="list-style-type: none"> <li>Maintain, service, and repair product</li> </ul>	<ul style="list-style-type: none"> <li>Product data</li> </ul>	<ul style="list-style-type: none"> <li>Product failure</li> <li>Causes of failures</li> <li>Component quality analysis</li> <li>Maintenance records</li> <li>Product status</li> </ul>
Recycle/Disposal	<ul style="list-style-type: none"> <li>Recycle or dispose product</li> </ul>	<ul style="list-style-type: none"> <li>Cost of recycling</li> <li>Disassembly plans</li> <li>Value</li> <li>Reusable state</li> <li>Component lifespan</li> </ul>	<ul style="list-style-type: none"> <li>Value of reusable components</li> <li>Recycling or disposable type, timing, method, location details</li> </ul>

**Note.** Based on the content in “Data-driven Smart Manufacturing,” by F. Tao et al., 2018,

*Journal of Manufacturing Systems*, 48, pp. 157-169.

(<https://doi.org/10.1016/j.jmsy.2018.01.006>)

Various types of data are analyzed in this phase, including customer demands in various forms such as comments, complaints, and online videos, along with market information like customer satisfaction survey results, product sales volume, investment planning, and more.

**Product Design.** The product development team works together to finish product design tasks by sharing and exchanging ideas and information. This information includes descriptions of product function, appearance, design parameters, configurations, test data, and historical data on faults from similar products.

**Raw Material Procurement.** A suitable procurement plan is created for purchasers by evaluating quotes, alternatives, availability, and potential suppliers of materials or components. The data evaluated includes manufacturer details such as the type, quantity, and quality of raw materials, as well as supplier information like pricing, inventory levels, and distance.

**Manufacturing.** Products are made by processing or assembling raw materials and components according to design specifications, which are subsequently tested for quality. The production process is consistently monitored through real-time collection and recording of parameters, attributes, performance, and the conditions of production factors.

**Transportation.** Once production is finished, products are moved to the sales area according to market demand and orders. Meanwhile, customers receive delivery services after a product sale. Logistics arrangements are improved by leveraging inventory, location, and order data to ensure the timely and accurate transportation of products.

**Sales.** Product launch and marketing activities rely on supplier data, inventory data, customer data, and order data. Throughout the sales process, insights from customer preferences, preference groups, order location distribution, and other information enhance product design, production, logistics, and sales progress.

**Utilization.** Under normal conditions, customers use the product according to the user manual. During the utilization phase, a significant amount of data, including product status, operational environment, and user behavior, is generated during the usage phase.

**After-sales Service.** This phase involves maintaining, servicing, and repairing the product. Product data is collected and used to develop and communicate suitable maintenance and service solutions to manufacturers. Data related to product failures, causes, component quality, maintenance records, and status is logged and managed to forecast product longevity and prevent other potential failures.

**Recycle/Disposal.** Optimizing the benefits of product recycling involves considering factors such as the cost of recycling and disassembly, the value, the state of reusability, and the remaining lifespan of components. Each component's value is evaluated using product status data and historical maintenance data to determine the optimal timing, method, location, and type of recycling or disposal.

## 2.4.2 Data Life Cycle

The availability of data in various formats ensures its accessibility and usability within a system. However, data is only useful when it is transformed into clear information that users can easily understand. Before specific information can be derived from data, it typically goes through several stages known as the data life cycle.

The definition of the data life cycle and its phases varies among different authors and organizations. Nonetheless, certain characteristics distinguish each defined phase from the others. Eryurek et al. (2021) sought to define the data life cycle based on the processes affecting a data object. They described the data life cycle as “the order of stages a piece of data goes through from its initial generation or capture to its eventual archival or deletion at the end of its useful life” (Eryurek et al., 2021, p. 85). They maintain, however, that not all data passes through every phase of the data life cycle—data creation, processing, storage, usage, archiving,

and destruction. Furthermore, they assert that these phases represent logical dependencies rather than actual data flows. On the contrary, Rahul and Banyal (2020) contend that the data life cycle defines the flow of data within an organization. From their perspective, the data life cycle encompasses the complete data process within the system. They proposed a life cycle for big data that includes the creation, storage, usability, sharing, archiving, and destruction phases. Nonetheless, Tao et al. (2018) outlined a typical life cycle for manufacturing data, suggesting the use of manufacturing data to enable smart manufacturing initiatives from the following stages of the data life cycle:

**Data Collection.** Data is gathered from multiple sources, including products, equipment, human operators, networks, and information systems. Data collection is facilitated by IoT technology through smart sensors and radio frequency identification (RFID), allowing for real-time monitoring of product health and equipment. Additionally, the mobile Internet enables the collection of user data via smart terminals. Furthermore, web crawling retrieves public data based on predefined conditions, while manufacturing information systems utilize database technologies to provide management data.

**Data Storage.** The vast amount of unstructured, semi-structured, and structured data from manufacturing processes is securely stored and effectively integrated using object-based storage architecture, cloud computing, and cloud services. The object-based storage architecture allows for flexible integration of unstructured and semi-structured data. Cloud computing offers storage solutions that are not only flexible but also cost-effective and energy-efficient. Cloud services ensure that the distribution and heterogeneity are shielded, resulting in scalable and shareable storage.

**Data Processing.** Data processing transforms raw data into understandable information, which is essential for manufacturers' decision-making processes. Key operations involved in data processing include preprocessing, data reduction, and analysis aimed at

extracting knowledge from large data sets. Preprocessing removes redundant, inconsistent, and misleading data, as well as missing values and duplicates. Data reduction organizes large datasets into meaningful and structured forms through feature selection or case selection. Cleaned and simplified data is then analyzed using techniques such as large-scale computing, ML, and forecasting models. Advanced data mining methods like classification, clustering, association rules, prediction, deviation analysis, regression, and more enhance the effectiveness of the analysis.

**Data Visualization.** Visualization enhances the accessibility, user-friendliness, and clarity of processed data, making it easier for end users to interpret. It effectively conveys information through graphical means, facilitating user comprehension. Common techniques include diagrams, graphs, charts, and virtual reality. Real-time data is available online through smart terminals.

**Data Transmission.** Data continuously flows between cyber-physical systems, information systems, and human operators. Communication and interaction among these distributed manufacturing systems and resources happen through data transmission. Advancements in communication networks, IoT, and the Internet have enhanced the technological foundation for real-time, reliable, and secure data transmission, facilitating effective integration of distributed manufacturing resources across various locations. This enables efficient integration of manufacturing resources spread across different areas.

**Data Applications.** Data-driven approaches and integration in manufacturing processes improve operational efficiency, enhance customer understanding, and promote agile responses to market changes. First, the design phases benefit from data analytics, which effectively translates customer insights into product features. Second, real-time production monitoring helps adapt to changes, thereby improving product quality control. Third, leveraging data-driven decision-making optimizes manufacturing processes, while early

detection of defects ensures timely adjustments. Fourth, predictive analytics in product utilization enables preventive maintenance and fault prediction, which guarantees seamless operations.

However, the manufacturing data life cycle lacks some critical stages. Table 2 presents a comparison of the manufacturing data life cycle stages from Tao et al. (2018) with those of and Eryurek et al. (2021) and Rahul and Banyal (2020). Including the usage, archiving, and destruction phases in a Holistic Manufacturing Data Life Cycle is essential because these stages ensure that data is used effectively, appropriately stored for future reference or regulatory compliance, and disposed of properly when no longer needed.

**Table 2**

*Comparison of Data Life Cycle Stages across Different Models*

<b>Data life cycle (Eryurek et al., 2021)</b>	<b>Big data life cycle (Rahul &amp; Banyal, 2020)</b>	<b>Manufacturing data life cycle (Tao et al., 2018)</b>	<b>Holistic manufacturing data life cycle</b>
Creation	Creation		Creation
		Collection	Collection
Processing		Processing	Processing
Storage	Storage	Storage	Storage
Usage	Usability		Usage
		Visualization	Visualization
		Transmission	Transmission
Archiving	Archiving		Archiving
		Applications	Applications
Destruction	Destruction		Destruction

**Note.** The holistic manufacturing data life cycle was synthesized by the author based on the data life cycle proposed by Eryurek et al. (2021), the big data life cycle by Rahul and Banyal (2020), and the manufacturing data life cycle by Tao et al. (2018).

### **2.4.3 Data Management**

The view of data as an invaluable corporate asset has become increasingly common among business and IT leaders. However, the implementation of various data integration projects has raised significant data management issues, such as migrating data from legacy systems to ERP solutions (Clemmons & Simon, 2001), data warehousing projects (Watson et al., 2004), and business intelligence efforts (Matney & Larson, 2004). The unsuccessful

implementation of ERP solutions in pharmaceutical companies underscores the importance of effective data management. Susilowati et al. (2021) reported a failed ERP implementation at FoxMeyer Drugs. FoxMeyer Drugs, once the fourth largest U.S. pharmaceutical distributor with \$5 billion in annual sales, faced bankruptcy following a failed ERP implementation (Scott, 1999; Scott & Vassey, 2002). Data conversion errors led to inaccurate customer sales histories and costly order mistakes, with \$16 million spent fixing errors in just six weeks (Scott, 2003). The system's inability to handle transaction volumes further compounded the issues, many of which remained unresolved (Scott, 1999). Beyond failed data integration projects, the ongoing impact of regulatory requirements such as the European Union General Data Protection Regulation (GDPR), Sarbanes-Oxley Act (SOX), and the Health Information Protection and Portability Act (HIPAA) exerts pressure on businesses to understand how data is used, where it is stored, controlled, secured, retained, and archived (Abraham et al., 2019). Organizations are compelled to navigate their regulatory compliance challenges. These challenges highlight the critical need for robust data management strategies that ensure data accuracy, integrity, and compliance.

Data management is crucial for businesses, regardless of their size or purpose. It plays a significant role in many organizations as advancements in information technology allow them to capture structured, semi-structured, and unstructured data (Tao et al., 2018). DAMA International (2017) defines data management as “the development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect, and enhance the value of data and information assets throughout their life cycles” (p. 18). However, an organization-wide mandate is necessary to fully benefit from data management. The objectives of enterprise data management include measuring data quality, ensuring the accuracy of reference data, and promoting a consistent understanding of various business terms across the organization (Pearce, 2017). Enterprise data management empowers organizations to leverage their data



assets with the support of suitable tools and processes. Strengtholt (2020) argues that achieving a data-driven approach, which entails maximizing the value derived from data, is challenging without integrating data management disciplines throughout the enterprise. Among the aspects of data management outlined by DAMA International (2017), Strengtholt (2020) believes that some elements are particularly relevant for effectively managing a modern data architecture at scale: data governance; data life cycle management; data architecture; data modeling and design; reference and master data management; data integration and interoperability; metadata management; data quality management; database management, data warehousing, business intelligence, and advanced analytics management; data storage and operations; and data security management.

Enterprise data management can also benefit from the COBIT models. The process component of the Managed Data objective includes ten key management practices, each consisting of practical activities for implementing the process (ISACA, 2018a):

Define and communicate the organization's data management strategy and roles and responsibilities...Define and maintain a consistent business glossary...Establish the processes and infrastructure for metadata management...Define a data quality strategy... Establish data profiling methodologies, processes and tools...Ensure a data quality assessment approach...Define the data cleansing approach...Manage the life cycle of data assets...Support data archiving and retention...Manage data backup and restore arrangements. (p. 143-147)

Several studies demonstrate the practical application of COBIT 2019's Managed Data objective across diverse organizational contexts. Hidayat et al. (2023) examined its use within an IT security environment, highlighting its IT governance maturity. Similarly, Atrinawati et al. (2021) applied the Managed Data objective in a higher education governance setting, using maturity models to identify data management gaps and inform strategic planning. These studies

underscore the Managed Data objective role in establishing measurable, structured data governance practices, insights that are particularly relevant for pharmaceutical contexts where data integrity and compliance are paramount.

Managing the data life cycle also enables the achievement of enterprise data management. DAMA International's revised edition of DAMA-DMBOK2 emphasizes that “data management is life cycle management” (Significant changes to DAMA-DMBOK2 revised edition, n. d.). Similarly, Prasad (2024) emphasized the need for comprehensive oversight of the data life cycle, from creation to disposal, regardless of whether data is stored on-site or off-site. Pearce (2024) further outlined the data management activities that should occur at each stage of the data life cycle. These data management activities strengthen security throughout the various data life cycle phases. Implementing them in the holistic manufacturing data life cycle requires specific steps for the collection, processing, archiving, and application phases.

First, in the collection phase, data management activities involve using secure communication protocols, encrypting data at its point of origin, and applying real-time monitoring alongside anomaly detection. Secure communication protocols like VPNs and TLS/SSL safeguard data transmitted through IoT devices and networks, preventing interception or tampering (Nguyen et al., 2015). Encrypting data at the source ensures that even if unauthorized access occurs, the data remains unreadable without the appropriate decryption keys (Stamp, 2011). Additionally, real-time monitoring of data collection allows for prompt detection of unauthorized access or security breaches as they happen (Saez et al., 2018).

In the processing phase, key activities include encrypting data, securely preprocessing it, and ensuring user authentication with access control. Encryption safeguards sensitive data both during and after processing (Schneier, 2015). Secure data preprocessing, which involves data cleaning and organization, minimizes the risk of errors and manipulation (Han et al.,

2022). Access control and authentication measures, including role-based access control (RBAC) and multi-factor authentication (MFA), guarantee that only authorized users can access or modify data during this stage (Stamp, 2011).

In the visualization phase, data management involves controlling user access based on their roles. Role-based visualization customizes data views according to each user's position, ensuring they access information relevant to their responsibilities while minimizing exposure to sensitive data (Mahmoodpour et al., 2018). This approach enhances security and improves the user experience by presenting only essential information.

Ensuring data encryption and legal compliance is crucial during the archiving phase. Encryption protects data during transmission and storage, and complying with data protection regulations guarantees that legal and regulatory requirements for proper archiving are met (Zhao & Gao, 2024). Maintaining compliance helps prevent potential legal issues and fosters digital trust.

Finally, authenticating users and controlling access are vital in the application phase. Implementing two-factor authentication (2FA) heightens security by reducing the risk of unauthorized access (Stamp, 2011). Robust access control mechanisms, such as RBAC, limit access to sensitive data based on job roles, ensuring only authorized personnel can view and modify data within the applications (Stamp, 2011).

The Secure Data Management for Manufacturing is illustrated in Table 3 and discussed below:

**Data Creation.** Categorize data based on its importance and sensitivity. Perform quality checks and validations to ensure its accuracy and integrity. Also, the collection and use of data should adhere to ethical and legal standards through secure consent processes.

**Data Storage.** Implement data encryption, access controls, and user authentication.

Data retention policies should be established based on business needs and regulatory requirements. Also, employ strategies for data backup and recovery to ensure data accessibility.

**Table 3**

*Secure Data Management for Manufacturing*

Stage	Secure data management activities
<b>Creation</b>	<ul style="list-style-type: none"> <li>Classify data according to its importance and sensitivity.</li> <li>Conduct quality checks and validation to verify accuracy and integrity.</li> <li>Ensure adherence to consent, ethical, and legal requirements.</li> </ul>
<b>Collection</b>	<ul style="list-style-type: none"> <li>Establish secure data collection protocols to ensure that data is obtained solely from authorized sources.</li> <li>Encrypt data collected via smart terminals and IoT sensors to protect it from unauthorized access.</li> <li>Validate and monitor data sources to prevent malicious or inaccurate data entry</li> </ul>
<b>Processing</b>	<ul style="list-style-type: none"> <li>Encrypt data both before and after processing to ensure confidentiality.</li> <li>Establish access controls to restrict who can process or modify data.</li> <li>Use secure preprocessing methods to remove inconsistent or redundant data and ensure only authorized personnel can access processing functions.</li> </ul>
<b>Storage</b>	<ul style="list-style-type: none"> <li>Implement encryption, access control, and user authentication measures.</li> <li>Establish retention policies aligned with business needs and regulatory requirements.</li> <li>Employ backup and recovery strategies to ensure data availability</li> </ul>
<b>Usage</b>	<ul style="list-style-type: none"> <li>Define access policies according to roles and responsibilities.</li> <li>Establish for data processing to maintain consistency and reliability.</li> <li>Monitor and audit data usage to ensure adherence to policies and regulations.</li> </ul>
<b>Visualization</b>	<ul style="list-style-type: none"> <li>Apply access controls to prevent unauthorized access to sensitive visual data.</li> </ul>
<b>Transmission</b>	<ul style="list-style-type: none"> <li>Encrypt data during transmission to ensure confidentiality.</li> <li>Establish standards for secure communication protocols and network configurations.</li> <li>Conduct integrity checks to verify that data remains unchanged during transmission</li> </ul>
<b>Sharing</b>	<ul style="list-style-type: none"> <li>Establish agreements for sharing data with external parties.</li> <li>Use anonymization or masking to safeguard sensitive data.</li> <li>Continuously monitor and review data access and sharing practices.</li> </ul>
<b>Applications</b>	<ul style="list-style-type: none"> <li>Control access to data-driven applications.</li> </ul>
<b>Archiving</b>	<ul style="list-style-type: none"> <li>Encrypt archived data.</li> <li>Store archived data in accordance with legal and regulatory requirements.</li> </ul>
<b>Destruction</b>	<ul style="list-style-type: none"> <li>Develop protocols for securely deleting data to ensure complete removal.</li> <li>Establish guidelines for data retention and secure archiving prior to deletion.</li> <li>Maintain audit trails to verify compliance and uphold data privacy</li> </ul>

**Note.** The Secure Data Management was synthesized by the author based on the data

management activities outlined by Pearce (2024) and applied to the holistic manufacturing data life cycle.

**Data Usage.** Establish data access policies based on roles and responsibilities. Data processing standards should also be defined to maintain consistency and reliability. Regularly

monitor and audit data usage to ensure compliance with established policies and regulatory requirements.

**Data Transmission.** Establish standards for secure communication protocols and network configurations. Also, data should be encrypted during transmission to ensure confidentiality. In addition, conduct data integrity checks to verify that information remains unaltered throughout transmission.

**Data Sharing.** Establish data-sharing agreements with external entities. Also, implement data masking or anonymization to safeguard sensitive data. In addition, implement ongoing monitoring and auditing of data access and sharing.

**Data Destruction.** Establish protocols for secure data deletion to guarantee the permanent removal of data. Also, create guidelines for how long data should be retained before secure archiving or deletion. Additionally, maintain thorough audit trails to verify compliance and protect data privacy.

#### **2.4.4 Data Governance**

Recognizing data as corporate assets with compliance requirements suggests that some form of data governance would enhance data management. Data governance is central to data asset management. Its importance has increased due to recent regulations, such as GDPR and NDPR, which affect various industries. Additionally, the data landscape has evolved significantly over time, requiring diverse approaches to data governance. This evolution is driven by factors such as the growing volume of data, the exponential rise in the number of people accessing data, advancements in data collection methods, the collection of diverse and sensitive data types, expanded data use cases, the emergence of new regulations and laws concerning data handling, and rising ethical concerns surrounding data usage (Eryurek et al., 2021). Pearce (2017) defined data governance as the means of “establishing, monitoring and sometimes enforcing policies, procedures, standards and guidelines that are related to the

overall management of enterprise data, with the goal of sustainably ensuring data availability, usability and security” (p. 1). He notes that “data governance activities provide direction and structure to data stewardship and enterprise data management activities” (p. 1). Pearce (2024) also contends that data governance should oversee data management activities, while Abraham et al. (2019, p. 8) offer a six-part definition of data governance:

A cross-functional framework for managing data as a strategic enterprise asset. In doing so, data governance specifies decision rights and accountabilities for an organization’s decision-making about its data. Furthermore, data governance formalizes data policies, standards, and procedures and monitors compliance.

According to the definitions above, data governance refers to the high-level stewardship of data by executives and the planning and control of data management. Eryurek et al. (2021) defined it as “a data management function to ensure the quality, integrity, security, and usability of the data collected by an organization”. Pearce (2024) stressed that adapting data governance activities to each phase of the data life cycle is essential for ensuring quality, maintaining security, protecting privacy, and achieving compliance for critical and sensitive data. Essentially, data governance aims to foster trust in data. Its value lies in its capacity to enhance stakeholders' trust across various aspects of data, including its collection, analysis, utilization, and publication (Eryurek et al., 2021). Accordingly, data governance focuses on maximizing the value of data assets within an organization (Carretero et al., 2017). Additionally, data governance seeks to ensure data accessibility, availability, and indexing for searching among all relevant stakeholders, generally encompassing the entire organizational knowledge-worker population (Eryurek et al., 2021). Therefore, well-governed data can generate measurable organizational value, particularly when data governance is approached as a continuous, evolving program focused on ongoing improvement (Eryurek et al., 2021).

**Data Governance Framework.** Implementing a data governance framework allows for more effective and successful management of data. According to Eryurek et al. (2021), frameworks effectively provide a holistic view and visualize plans. Prasad (2024) highlights that a data governance framework offers a strategy for effectively managing data throughout its life cycle. Like any structure, a well-designed data governance framework requires a solid foundation that delineates clear roles and responsibilities. Eryurek et al. (2021) note that data governance frameworks involve the intricate interplay of many roles and responsibilities, emphasizing each role's contribution to the seamless operation of the data governance machine. Therefore, adopting a data governance framework fosters collaboration at various levels across organizations for enterprise-wide data management. Furthermore, a data governance framework establishes rules for the collection, utilization, and storage of data (Prasad, 2024).

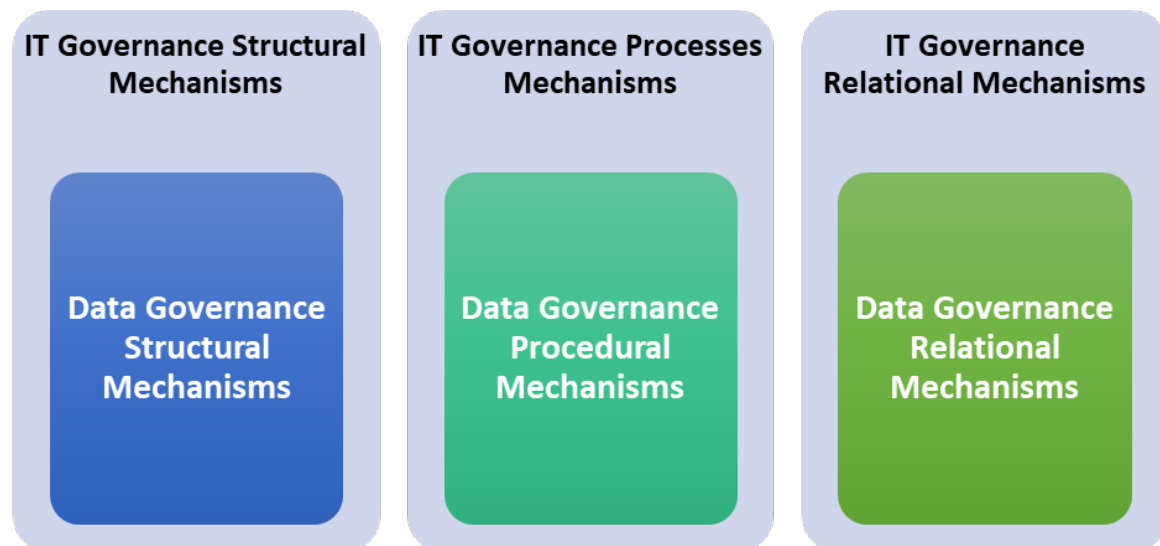
**Data Governance Mechanisms.** Data governance mechanisms empower organizations to maintain control over their data. These mechanisms, illustrated in Figure 18, support the strategic planning and management of various data activities (Mosely et al., 2009; Abraham et al., 2019): formal structures that connect business, IT functions, and data management; established decision-making and monitoring processes and procedures; and practices that encourage active participation and collaboration among stakeholders.

**Structural Mechanisms.** The structural mechanisms of data governance are similar to those of IT governance. These mechanisms establish governance bodies, lines of authority, and accountabilities (Borgman et al., 2016). They involve the assignment of decision-making authority and roles. Defining the assignment of decision-making authority determines which organizational unit is empowered to make data governance decisions (Otto, 2011b). This authority can be positioned hierarchically, indicating the level within the organization where it is located (Otto, 2011c); functionally, specifying which department holds this authority (Mosely et al., 2009); or along a continuum, identifying whether decisions are made by a central

unit, decentralized units, or both (Barker, 2016). Key governance roles include the executive sponsor, data governance leader, data governance council, data governance office, data owner, data producer, data consumer, and data steward (Abraham et al., 2019).

**Figure 18**

*Data Governance Mechanisms*



**Note.** Based on the content in “Data Governance: A Conceptual Framework, Structured Review, and Research Agenda,” by R. Abraham et al., 2019, *International Journal of Information Management*, 49, pp. 424-438.

(<https://doi.org/10.1016/j.ijinfomgt.2019.07.008>)

**Procedural Mechanisms.** Data governance procedural mechanisms reflect those found in IT governance frameworks. These mechanisms aim to ensure the effective use, proper sharing, accurate recording, and secure storage of data (Borgman et al., 2016). Data governance procedural mechanisms include data strategy, processes, policies, standards, procedures, contractual agreements, performance measurement, compliance monitoring, and issue management (Abraham et al., 2019). The data strategy outlines a high-level action plan based on strategic business objectives (Cheng et al., 2017). Data policies provide overarching guidelines and rules for creating, acquiring, storing, securing, using, and ensuring the quality



of data (Alhassan et al., 2019). Data standards guarantee consistency in how data and related activities are represented and conducted across an enterprise (Kim & Cho, 2017). Data procedures refer to “the documented methods, techniques, and steps followed to accomplish a specific activity or task” (Mosely et al., 2009, p. 48). Procedures vary significantly among different businesses. Data processes are standardized, repeatable, and documented methods to govern data (Al-Ruithe et al., 2018b). Contractual agreements facilitate the provision and sharing of data among participating internal departments and external organizations (Abraham et al., 2019). Compliance monitoring is conducted to track and ensure that regulatory requirements and the organization's policies, standards, procedures, and service level agreements (SLA) are followed and adhered to (Al-Ruithe et al., 2018a). Issue management involves identifying, handling, and resolving data-related issues (Mosely et al., 2009). Performance measurement evaluates the effectiveness of data governance by assessing the degree to which goals have been achieved (Al-Ruithe et al., 2018a; Carretero et al., 2017).

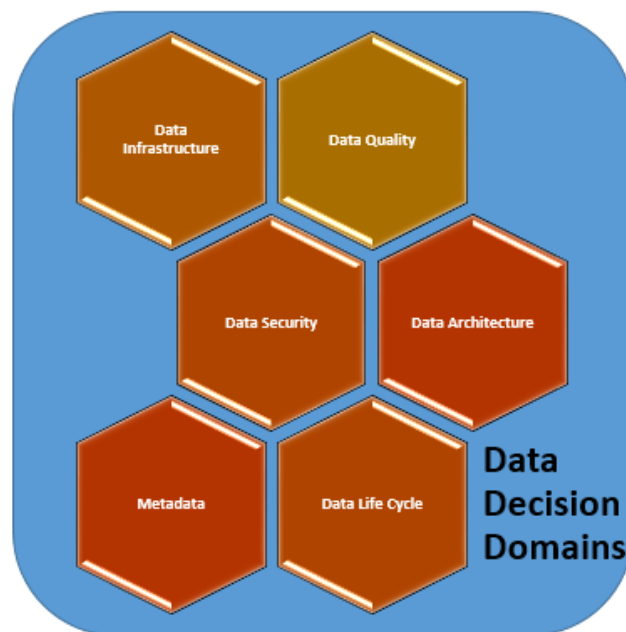
***Relational Mechanisms.*** The relational mechanisms of data governance exhibit parallels with those found in IT governance. These relational governance mechanisms facilitate collaboration among stakeholders (Borgman et al., 2016) and include elements such as communication, training, and coordination for decision-making (Abraham et al., 2019). Training ensures that stakeholders possess the necessary knowledge and skills to effectively support the implementation of data governance initiatives (Tallon et al., 2013). This communication aims to raise continuous awareness of the data governance program (Begg & Caira, 2012). The coordination of decision-making pertains to methods of cross-functional alignment (Abraham et al., 2019). Hagmann (2013) and Kooper et al. (2011) describe the vertical or hierarchical approach marked by a pyramidal structure where decision-making authority, steering, and control are concentrated at the upper tier (Hagmann, 2013). In contrast,

the horizontal or cooperative approach fosters collaborative behaviors to clarify differences and resolve issues (Wende & Otto, 2007).

**Data Decision Domains.** Governance mechanisms are closely tied to key data decision domains. Abraham et al. (2019) classified the primary data decision domains into data life cycle, metadata, data quality, data architecture, data storage and infrastructure, and data security, as shown in Figure 19, summarized in Table 4, and discussed below.

**Figure 19**

*Data Decision Domains*



**Note.** Based on the content in “Data Governance: A Conceptual Framework, Structured Review, and Research Agenda,” by R. Abraham et al., 2019, *International Journal of Information Management*, 49, pp. 424-438.

(<https://doi.org/10.1016/j.ijinfomgt.2019.07.008>)

**Data Life Cycle.** The data life cycle refers to the approach to data creation, collection, processing, storage, usage, visualization, archiving, applications, and destruction. Data governance centered on the data life cycle involves identifying the business processes that

utilize data (Carretero et al., 2017) and analyzing the data flow to identify potential duplication in data storage (Ballard et al., 2014). It also encompasses establishing data retention requirements based on business needs, accountability, and regulatory obligations (Cousins, 2016). Furthermore, data governance necessitates that organizations specify when data may be deleted (Mosely et al., 2009).

**Metadata.** Metadata refers to data that helps in understanding other data. It is utilized to classify data provenance (Lee et al., 2017; Were & Moturi, 2017), sensitivity (Cousins, 2016), and retention periods (Weller, 2008). Metadata-driven data governance encompasses outlining a metadata strategy (Grimstad & Myrseth, 2010), establishing shared metadata standards (De Abreu Faria et al., 2013), and defining processes for building a metadata repository (Rasouli et al., 2016c). It also defines the roles of data modelers and enterprise data architects responsible for managing metadata (Khatri & Brown, 2010).

**Data Quality.** Data quality refers to whether data is suitable for its intended purpose. It encompasses the capability of data to meet the requirements for use within a specific context (De Abreu Faria et al., 2013). Quality-driven data governance involves developing a data quality strategy (Thomas, 2006a), defining roles and responsibilities (Malik, 2013), and establishing processes for managing data quality. Other tasks include monitoring data quality, which consists of defining data quality metrics (Brous et al., 2016a) and continuously measuring data quality levels (Mosely et al., 2009; Weber et al., 2009). Additional responsibilities include addressing data quality issues (Mosely et al., 2009; Rifaie et al., 2009).

**Data Architecture.** Data architecture serves as a blueprint for managing data. It involves defining enterprise data objects (Dyché & Levy, 2006; Thomas, 2006b) and developing an enterprise data model at conceptual, logical, and physical levels (Mosely et al., 2009). Data governance, guided by data architecture, includes identifying enterprise data requirements (Ballard et al., 2014) and defining architectural policies, standards, and guidelines

(Mosely et al., 2009). It also outlines the responsibilities of data architects concerning the enterprise data model (Mosely et al., 2009).

**Data Infrastructure.** Data infrastructure and storage consist of various components that enable data sharing, consumption, and storage. They focus on IT artifacts that facilitate effective data management across an enterprise (Tallon et al., 2014). Therefore, organizations must consider software and hardware requirements, including functionality, complexity, reliability, capacity, maintainability, scalability, and cost (Al-Ruithe et al., 2018a). Data governance related to data storage and infrastructure involves evaluating the application and storage landscape (Dreibelbis et al., 2008), as well as planning software applications and storage capacity to support the data life cycle, quality, and security (Tallon, 2013). Other governance mechanisms establish policies, standards, processes, and procedures for storing and distributing data (Tallon et al., 2014), control storage costs (Tallon et al., 2014), and educate stakeholders on the proper use of storage (Tallon, 2013).

**Data Security.** Data security controls safeguard data during both storage and transmission. Data security involves protecting digital assets from unauthorized access, alteration, or loss throughout their life cycle (Chapple et al., 2018). Effective data security strategies integrate technical controls, organizational policies, and user awareness to safeguard both personal and business-critical information (ISACA, 2018b).

Data governance literature places data security as a cross-cutting theme across decision domains. Each domain intersects with data security: metadata may reveal data sensitivity; infrastructure manages secure storage; the data life cycle dictates how securely data is created, used, and destroyed; data quality affects the reliability and integrity of secure information; and data architecture determines how securely data is structured, integrated, and made accessible across systems. Therefore, data security does not operate in isolation but instead both influences and is influenced by decisions made across all domains. Compared to other domains,

data security is the domain that ensures the safe functioning of all others. Without adequate security, high-quality data can be corrupted, sensitive metadata exposed, and architectural structures compromised. While data quality guarantees usability, and the data life cycle manages data movement, data security provides protection, fosters trust, and ensures compliance throughout these processes. It also directly supports regulatory compliance (e.g., GxP, GDPR) and business continuity. Therefore, research into data security offers the most direct contribution to protecting organizational value compared to other domains.

**Table 4**

*Data Decision Domains and Governance Mechanisms*

Domain	Definition / Focus	Governance Mechanisms
<b>Data Life Cycle</b>	Management of data from creation to destruction	<ul style="list-style-type: none"> <li>• Identify business processes using data</li> <li>• Analyze data flows to avoid duplication</li> <li>• Set data retention and deletion rules</li> </ul>
<b>Metadata</b>	Data that provides context or information about other data	<ul style="list-style-type: none"> <li>• Classify data provenance, sensitivity, and retention</li> <li>• Develop metadata strategy - Define standards and repositories</li> <li>• Assign roles to data modelers and architects</li> </ul>
<b>Data Quality</b>	Suitability of data for intended use	<ul style="list-style-type: none"> <li>• Develop data quality strategy</li> <li>• Define roles/responsibilities</li> <li>• Monitor and address quality issues</li> <li>• Set and measure data quality metrics</li> </ul>
<b>Data Architecture</b>	Blueprint for organizing and managing data	<ul style="list-style-type: none"> <li>• Define enterprise data models (conceptual, logical, physical)</li> <li>• Set architectural policies, standards, and guidelines</li> <li>• Assign responsibilities to data architects</li> </ul>
<b>Data Infrastructure</b>	Technical foundation for data storage, sharing, and processing	<ul style="list-style-type: none"> <li>• Evaluate application/storage landscape</li> <li>• Plan software and hardware needs (scalability, cost, etc.)</li> <li>• Define policies and train users</li> </ul>
<b>Data Security</b>	Protection of data from unauthorized access, alteration, or loss across its life cycle	<ul style="list-style-type: none"> <li>• Implement technical and organizational controls</li> <li>• Promote user awareness</li> <li>• Support cross-domain security (e.g., secure metadata, architecture, quality)</li> <li>• Ensure compliance and continuity in high-risk contexts</li> </ul>

**Note.** Based on the content in “Data Governance: A Conceptual Framework, Structured Review, and Research Agenda,” by R. Abraham et al., 2019, *International Journal of Information Management*, 49, pp. 424-438. (<https://doi.org/10.1016/j.ijinfomgt.2019.07.008>).

While other domains focus on usability, organization, or efficiency, data security research addresses the resilience and trustworthiness of data systems. It allows organizations to anticipate risks, develop context-specific controls, and adapt governance models to emerging threats. In contexts like Nigerian pharmaceutical manufacturing, where regulatory systems are maturing and infrastructure may be limited, research into data security addresses a crucial gap by providing empirical evidence to inform practice and policy.

**Organizational Scope of Data Governance.** The scope of data governance can be either inter-organizational or intra-organizational. According to Abraham et al. (2019), the intra-organizational scope refers to the governance of data within a single organization. It involves the governance of data at both the firm and project levels (Tiwana et al., 2014). Firm-level data governance spans the entire enterprise and aligns the demands and interests of various stakeholder groups, such as business and IT departments (Otto, 2011b). Data governance at the project level focuses on managing the quality and integrity of data specific to individual projects (Mosely et al., 2009). The inter-organizational scope covers the governance of data between enterprises and their ecosystems (Tiwana et al., 2014). Companies are increasingly partnering with external collaborators like public sector organizations, industry peers, and suppliers to develop new information (Winter & Davidson, 2018). While these partnerships allow businesses to seize environmental opportunities, they also pose risks such as loss of control over data, exposure to unsecured information, and low-quality informational products (Al-Ruithe et al., 2018a).

**Data Governance Consequences.** Adopting data governance practices can have positive effects on an organization. According to Abraham et al. (2019), these benefits manifest as intermediate performance effects and enhanced risk management. Intermediate performance outcomes arise in several ways. First, data governance increases the level of data usage, contributing to marketing performance through higher customer spending and sales. Second,

data governance enhances data quality by improving availability, completeness, accuracy, coherence, and timeliness and reducing errors caused by data inconsistencies. Third, data governance positively affects a firm's dynamic and operational capacities by enhancing existing operational modes, which leads to renewed competitive strategies in the marketplace. Additionally, the consequences of data governance aid in managing data-related risks. Data governance mitigates these risks by enabling the creation of risk-reducing policies and controls to monitor compliance. Furthermore, Pearce (2024) identified the consequences of data governance that occur at each stage of the data life cycle from a security standpoint, as discussed below:

**Data Creation.** Establish precise data classification, enforce compliance with data standards, and ensure compliance with data protection regulations.

**Data Storage.** Adhere to policies and regulations. Implement measures to prevent data loss and system failures. Ensure data security by blocking unauthorized access and breaches.

**Data Usage.** Maintain proper access and controls. Encourage transparency and accountability in data usage. Ensure accurate and secure data processing.

**Data Transmission.** Protect data while it is in transit. Implement measures for data integrity to minimize the risk of tampering. Ensure data security during transmission to prevent unauthorized access.

**Data Sharing.** Establish and enforce policies, roles, and responsibilities for data sharing. Ensure data privacy protection when sharing with external parties. Comply with regulations and security measures during the data sharing process.

**Data Destruction.** Maintain accessible audit trails for inspection. Ensure proper disposal of data to prevent leaks or breaches. Comply with regulations governing data retention.

Secure data management practices are established by integrating Pearce's (2024) data management activities and governance outcomes with the comprehensive manufacturing data life cycle, as shown in Table 5.

**Table 5**

*Secure Data Management and Governance in Manufacturing*

Stage	Secure data management activities	Data governance consequences
<b>Creation</b>	<ul style="list-style-type: none"> <li>Classify data according to its importance and sensitivity.</li> <li>Conduct quality checks and validation to verify data accuracy and integrity.</li> <li>Ensure adherence to consent, ethical, and legal requirements.</li> </ul>	<ul style="list-style-type: none"> <li>Implement accurate data classification.</li> <li>Ensure compliance with data standards.</li> <li>Maintain conformity with data protection regulations.</li> </ul>
<b>Collection</b>	<ul style="list-style-type: none"> <li>Establish secure data collection protocols to ensure that data is obtained solely from authorized sources.</li> <li>Encrypt data collected via smart terminals and IoT sensors to protect it from unauthorized access.</li> <li>Validate and monitor data sources to prevent malicious or inaccurate data entry</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced data integrity by preventing unauthorized data collection.</li> <li>Secure, real-time data collection</li> <li>Ensure trustworthiness of data sources through source validation</li> </ul>
<b>Processing</b>	<ul style="list-style-type: none"> <li>Encrypt data both before and after processing to ensure confidentiality.</li> <li>Establish access controls to restrict who can process or modify data.</li> <li>Use secure preprocessing methods to remove inconsistent or redundant data and ensure only authorized personnel can access processing functions.</li> </ul>	<ul style="list-style-type: none"> <li>Ensure secure data processing.</li> <li>Maintain access restrictions to safeguard sensitive data.</li> <li>Promote data accuracy and security during preprocessing.</li> </ul>
<b>Storage</b>	<ul style="list-style-type: none"> <li>Implement encryption, access control, and user authentication measures.</li> <li>Establish retention policies aligned with business needs and regulatory requirements.</li> <li>Employ backup and recovery strategies to ensure data availability</li> </ul>	<ul style="list-style-type: none"> <li>Safeguard data by preventing unauthorized access and breaches.</li> <li>Comply with policies and regulations.</li> <li>Implement measures to prevent system failures and data loss.</li> </ul>
<b>Usage</b>	<ul style="list-style-type: none"> <li>Define access policies according to roles and responsibilities.</li> <li>Establish for data processing to maintain consistency and reliability.</li> <li>Monitor and audit data usage to ensure adherence to policies and regulations.</li> </ul>	<ul style="list-style-type: none"> <li>Maintain adequate access and controls.</li> <li>Ensure accurate and secure data processing.</li> <li>Promote accountability and transparency in data utilization.</li> </ul>
<b>Visualization</b>	<ul style="list-style-type: none"> <li>Apply access controls to prevent unauthorized access to sensitive visual data.</li> </ul>	<ul style="list-style-type: none"> <li>Reduced risk of data leaks by securing access to sensitive visual data.</li> </ul>
<b>Archiving</b>	<ul style="list-style-type: none"> <li>Encrypt archived data.</li> <li>Store archived data in accordance with legal and regulatory requirements.</li> </ul>	<ul style="list-style-type: none"> <li>Archived data remains secure.</li> <li>Compliance with retention schedules to mitigate legal risks.</li> </ul>
<b>Transmission</b>	<ul style="list-style-type: none"> <li>Encrypt data during transmission to ensure confidentiality.</li> <li>Establish standards for secure communication protocols and network configurations.</li> </ul>	<ul style="list-style-type: none"> <li>Secure data during transmission to prevent unauthorized access.</li> <li>Safeguard data while it is in transit.</li> </ul>



Stage	Secure data management activities	Data governance consequences
Sharing	<ul style="list-style-type: none"> <li>• Conduct integrity checks to verify that data remains unchanged during transmission.</li> </ul>	<ul style="list-style-type: none"> <li>• Implement data integrity to minimize the risk of tampering.</li> </ul>
	<ul style="list-style-type: none"> <li>• Establish agreements for sharing data with external parties.</li> <li>• Use anonymization or masking to safeguard sensitive data.</li> <li>• Continuously monitor and review data access and sharing practices.</li> </ul>	<ul style="list-style-type: none"> <li>• Establish and enforce regulations, roles, and obligations for sharing data.</li> <li>• Ensure the protection of data privacy when sharing with external parties.</li> <li>• Adhere to regulations and security measures when sharing data.</li> </ul>
Applications	<ul style="list-style-type: none"> <li>• Control access to data-driven applications.</li> </ul>	<ul style="list-style-type: none"> <li>• Enhanced application security by preventing unauthorized access.</li> </ul>
Destruction	<ul style="list-style-type: none"> <li>• Develop protocols for securely deleting data to ensure complete removal.</li> <li>• Establish guidelines for data retention and secure archiving prior to deletion.</li> <li>• Maintain audit trails to verify compliance and uphold data privacy</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure appropriate disposal of data to prevent leaks or breaches.</li> <li>• Adhere to regulations governing data retention.</li> <li>• Maintain accessible audit trails for inspection.</li> </ul>

**Note.** The Secure Data Management and Governance was synthesized by the author based on the data management activities outlined by Pearce (2024) and applied to the holistic manufacturing data life cycle.

Securing all data is impossible and costly for most businesses. However, enterprise data management and data governance provide an additional layer of defense for modern enterprises' most valuable assets with minimal extra effort. Ultimately, enterprise data management and data governance reduce risks to manufacturing data.

## 2.5 Data Security

Data security is currently a concern for both industry and academia due to the widespread adoption of IT systems. The growing saturation of computing in all aspects of an enterprise expands the sources of data loss, corruption, and various other data-related risks. Until we make data resistant to these risks, we cannot regard an IT-driven society as secure.

### 2.5.1 Layers of Security and Data Security

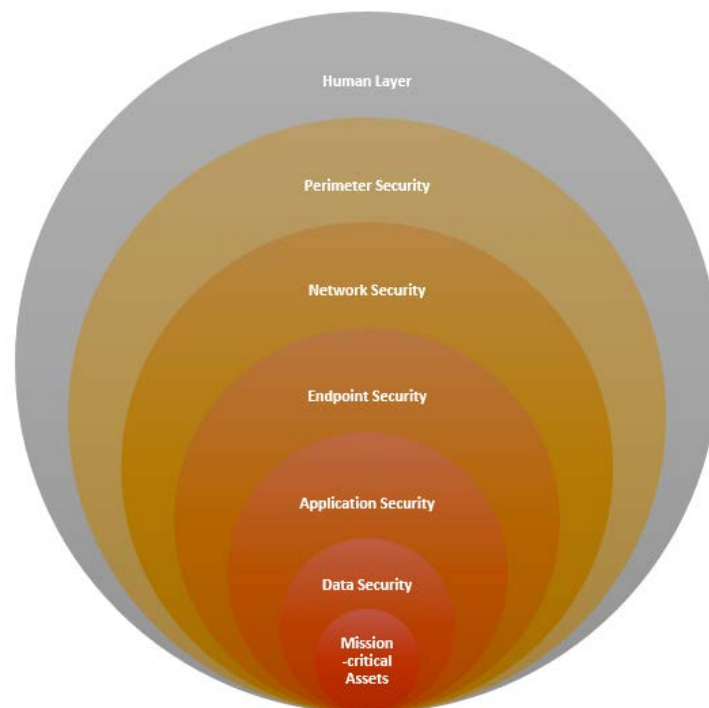
In today's digital era, where cyber threats are prominent, organizations must bolster their defenses to protect sensitive data, infrastructure, and assets. Safeguarding organizational resources from cyber threats necessitates a multifaceted approach that involves various layers

of security. From human factors to mission-critical assets, each layer plays a crucial role in managing risks and safeguarding sensitive information. We examine the layers of security identified by Elijah et al. (2021), as illustrated in Figure 20—human, perimeter, network, endpoint, application, and data security—highlighting their importance in protecting mission-critical assets.

**Human Layer.** The human layer of an organization consists of its employees. Consequently, organizations will encounter significant challenges due to human error and malicious insider threats. The human layer of security necessitates a comprehensive understanding of the human factor and involves implementing policies, controls, and reporting that ensure the protection of critical assets against human threats (Elijah et al., 2021).

**Figure 20**

*Layers of Security*



**Note.** Based on the content in “A Survey on Industry 4.0 for the Oil and Gas Industry: Upstream Sector,” by O. Elijah et al., 2019, *IEEE Access*, 9, pp. 144438-144468. (<https://ieeexplore.ieee.org/iel7/6287639/6514899/09579415.pdf>).

**Perimeter Security Layer.** Perimeter security serves as the first line of defense against external threats. This security layer ensures both physical and digital safety for the entire business (Elijah et al., 2021). The primary goal of perimeter security is to protect the boundaries of an organization's network from external attacks and unauthorized access. It involves managing the flow of network traffic, both incoming and outgoing, in accordance with the organization's established security policies, thereby strengthening the digital border.

**Network Security Layer.** The network layer is crucial for managing and protecting communication between applications and devices within an organization's network. Network security involves safeguarding the internal network infrastructure and communication channels from unauthorized access (Elijah et al., 2021). While network security includes both hardware and software protection, it is mainly focused on defending an organization's network infrastructure.

**Endpoint Security Layer.** Desktops, laptops, smartphones, tablets, and other mobile devices serve as gateways to the network. Securing these endpoints is crucial because they act as access points to that network. The endpoint security layer aims to protect individual devices from malware, phishing attacks, and other security threats (Elijah et al., 2021).

**Application Security Layer.** The application security layer focuses on keeping software and devices safe from threats. According to Elijah et al. (2021), application security safeguards critical assets by protecting and securing applications. It entails fortifying software applications against vulnerabilities and exploits that could compromise data confidentiality and integrity.

**Data Security Layer.** The data security layer is dedicated to safeguarding data both within and outside the network. According to Elijah et al. (2021), data security focuses on protecting the storage and transfer of data. It encompasses protocols and measures designed to protect sensitive information from unauthorized access, alteration, disclosure, or destruction,

both at rest and in transit. However, its effectiveness is tightly interconnected with all other layers: human error or insider threats at the human layer, weak perimeter or network protections, or poorly secured endpoints and applications can all undermine the integrity of data security efforts.

**Mission Critical Assets.** This layer emphasizes the protection of assets vital for an organization's operation and longevity. Mission-critical assets include essential hardware, core systems, proprietary software, applications, intellectual property, sensitive customer information, financial data, and trade secrets. Safeguarding these assets is crucial for ensuring business continuity and resilience against cyber threats. According to Elijah et al. (2021), mission-critical data requires the highest level of protection. Therefore, securing mission-critical assets mandates a comprehensive security strategy that addresses vulnerabilities across all security layers.

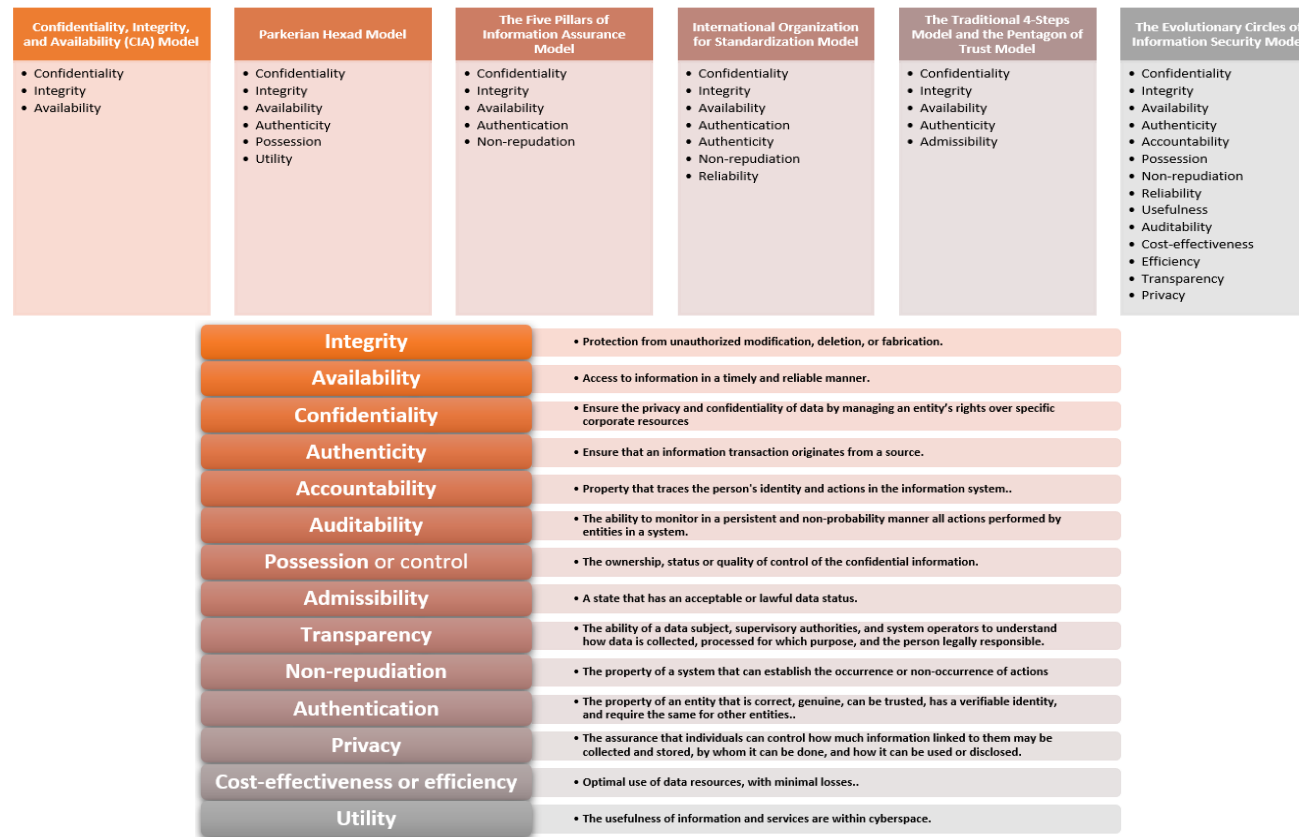
While all layers of cybersecurity are essential to a defense-in-depth strategy, focusing research specifically on the data security layer is especially important because data is the primary target of most cyberattacks. Other layers, such as perimeter, network, or endpoint security, act as protective barriers, but they are only effective insofar as they protect access to data. Research in data security offers direct insights into how data is stored, accessed, transmitted, and protected throughout its life cycle. It also makes the consequences of breaches clearer, such as data loss, IP theft, or regulatory violations. As attackers increasingly bypass traditional defenses, understanding protective measures and vulnerabilities at the data layer becomes crucial for securing organizational assets, especially in high-stakes industries like pharmaceuticals.

### **2.5.2 Data Security Models**

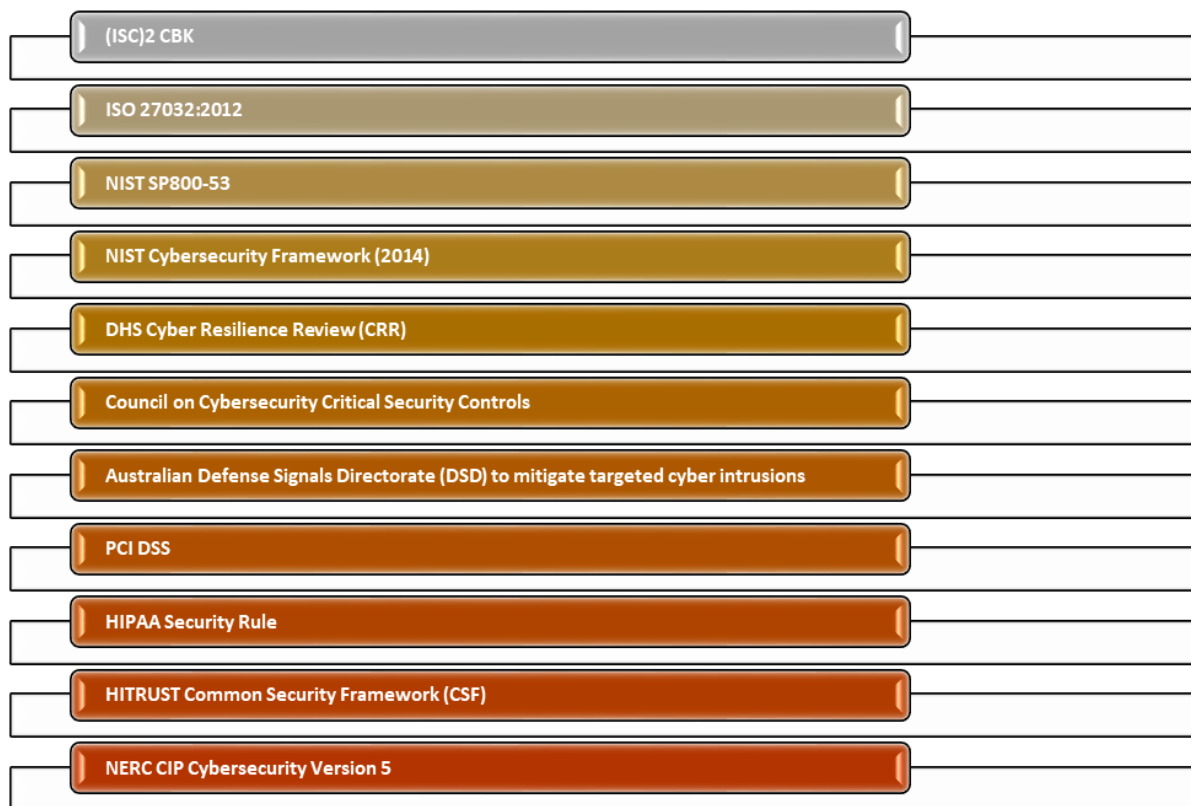
A data security model can incorporate various concepts. Researchers have defined data security through a variety of different concepts. For instance, Avizienis et al. (2004) described

it in terms of privacy, confidentiality, integrity, and availability, while Carretero et al. (2017) expanded this to include access control, authenticity, reliability, and privacy. These conceptual distinctions are critical in understanding how security principles are implemented, especially in environments dealing with sensitive information. Numerous models have been developed over the years to address information security concerns. Moghaddasi et al. (2016) identified key models and associated concepts in a study aimed at enhancing information quality, providing a structured lens through which data protection can be evaluated. As illustrated in Figure 21 these models and their core elements underpin the modern understanding of data and information security. They also form the theoretical backbone of major cybersecurity frameworks, such as those presented in Figure 22 (Sabillon et al., 2016). The following section reviews several foundational and emerging information security models, their relevance, and effectiveness in the pharmaceutical domain:

**Confidentiality, Integrity, and Availability Model.** Clark and Wilson introduced the Confidentiality, Integrity, and Availability (CIA) Triad Model in 1987. According to Chapple et al. (2018), confidentiality, integrity, and availability are vital components of information security. In this model, integrity refers to protection against the improper destruction or alteration of information. Data integrity involves preventing unauthorized and improper modifications of data. It implies safeguarding data from unauthorized changes, deletion, or fabrication (Bertino & Sandhu, 2005; Sun et al., 2014). Availability ensures timely and reliable access to information. Data availability pertains to the ability to avoid and recover from software errors, hardware failures, and malicious denial of access to data. It measures the extent to which user data can be utilized or recovered and the techniques used to verify the data (Bertino & Sandhu, 2005; Sun et al., 2014). Confidentiality involves maintaining authorized restrictions on access to information while allowing its legal disclosure only (Moghaddasi et al., 2016). Data confidentiality guarantees that only authorized individuals can access the data.

**Figure 21***Data Security Models and Concepts*

**Note.** Based on the conceptual discussion in “Reasons in support of data security and data security management as two independent concepts: a new model,” by H. Moghaddasi et al., 2019, *The Open Medical Informatics Journal*, 10, pp. 4-10. (<https://doi.org/10.2174/1874431101610010004>).

**Figure 22***Major Cybersecurity Frameworks*

**Note.** Based on the content in “National Cyber Security Strategies: Global Trends in Cyberspace,” by R. Sabillon et al., 2016, *International Journal of Computer Science and Software Engineering*, 5 (5), pp. 67-81. (<https://www.proquest.com/scholarly-journals/national-cyber-security-strategies-global-trends/docview/1868264400/se-2?accountid=188730>).

Additionally, data confidentiality protects privacy by regulating an entity’s rights over particular corporate resources (Sun et al., 2014). Treacy and McCaffery (2016) regard confidentiality, integrity, and availability as fundamental concepts in data security.

The CIA Triad provides a foundational framework, emphasizing data confidentiality (protecting proprietary formulations), integrity (ensuring batch data is unaltered), and availability (maintaining access to systems for production continuity). It directly maps to

regulatory requirements, such as FDA 21 CFR Part 11 (US FDA, 2003). However, the CIA Triad is too high-level and abstract and lacks guidance on implementation in environments with complex regulatory or operational needs. Moreover, it does not account for non-technical dimensions like human behavior or organizational processes, which are critical in GMP settings.

**Parkerian Hexad Model.** In 1998, Donn B. Parker introduced three additional non-overlapping data attributes to complement the CIA triad. These new attributes in the Parkerian Hexad model are referred to as possession, authenticity, and utility (Turab & Kharma, 2019). According to Parker's definition, the concept is based on the potential loss that a government, business, or individual may suffer if the components of the Parkerian Hexad are compromised at any stage of information security (Dhawan, 2014). In this model, confidentiality refers to the boundaries of individuals and the types of information that can be retrieved, integrity means being accurate or consistent with the expected status of the information, availability indicates timely access to information, possession signifies control or ownership of information, authenticity denotes proper labeling or attribution of information, and utility implies the usefulness of the information (Moghaddasi et al., 2016).

Building on the CIA Triad, the addition of possession/control, authenticity, and utility makes the Parkerian Hexad Model highly relevant to pharmaceutical environments, where IP theft and authenticity of production data are vital concerns. Its broader scope allows for a more refined assessment of information value, especially in contexts involving clinical trials or formulation records, where data must not only be accurate and secure but also genuine, possessed by the rightful entity, and usable for its intended purpose. A notable weakness in the Parkerian Hexad Model is the increased complexity it brings without clear implementation pathways. Moreover, possession/control and utility can be hard to define and enforce in automated manufacturing pipelines.



**The Five Pillars of Information Assurance Model.** The Five Pillars of the Information Assurance Model evolved from the CIA triad. This model expanded the CIA triad to include the attributes of non-repudiation and authentication, which are not attributes of information or systems; rather, they describe the methods or procedures designed to protect confidentiality and ensure the integrity and authenticity of information (Dardick, 2010). Launched by the U.S. Department of Defense in 2002, the Five Pillars of Information Assurance Model was formalized in the National Information Assurance Glossary (Committee on National Security Systems, 2010). This publication specified information assurance as the measures taken to defend and protect information and information systems by ensuring their integrity, confidentiality, availability, non-repudiation, and authentication. Moghaddasi et al. (2016) described these five pillars of information assurance. The confidentiality attribute ensures that information is not disclosed to unauthorized individuals, organizations, or systems. Availability means timely and reliable access to data by users. Non-repudiation provides assurance that the findings of analyses are true, relevant, and cannot be denied. It ensures that the sender has transmitted the data to the receiver and that the recipient's identity is verified, making it impossible to deny the authenticity of the processed information. Therefore, the veracity of the processed information cannot be recanted. Authentication is the process of verifying an entity's (user, process, or device) identity or other claimed or suspected attributes or data sources and their integrity (Cherdantseva & Hilton, 2014).

The Five Pillars of Information Assurance Model addresses compliance and traceability requirements, and is especially useful for audit trails and validating system access during inspections. It reinforces non-repudiation, important in batch sign-offs and electronic record management. However, its conceptual overlap with other models makes the Five Pillars of Information Assurance less distinct. Also, this model may overemphasize digital system assurance at the expense of physical and process security.

**International Organization for Standardization Model.** In 2004, ISO introduced a data security model. Initially, this model outlined seven principles for information and communication technology (ICT) security: confidentiality, availability, integrity, authenticity, accountability, non-repudiation, and reliability (ISO, 2004). According to Von Solms and Van Niekerk (2013), the ICT security concept defined by ISO also refers to data security. Moghaddasi et al. (2016) elaborate further on these principles, commonly known as the "7 ISO principles." Confidentiality involves preventing unauthorized access or disclosure by unauthorized entities, individuals, or processes. Integrity pertains to the correctness and completeness of data. Availability means that data is accessible and usable upon request by an authorized entity. Non-repudiation entails the ability to verify the occurrence of an action and its originating entities. Reliability denotes consistency in expected behaviors and outcomes. Authenticity is the property of being what an entity claims to be. Accountability involves tracing an individual's identity and actions within the information system. However, it is noteworthy that accountability was neither included in the ISO/IEC 27000:2018 standard (ISO, 2018) nor explicitly listed as a standalone principle in ISO/IEC 27001:2022 (ISO, 2022a). Nevertheless, elements of accountability were embedded within various clauses.

The International Organization for Standardization (ISO/IEC 27001) Model offers structured, certifiable guidelines that align with global compliance standards, such as EU Annex 11 (European Commission, 2011) and WHO TRS 937 (WHO, 2006). In addition, it is tailored for risk-based thinking and continuous improvement, essential for pharmaceutical manufacturing. However, its implementation is resource-intensive and may require cultural shifts. Also, its heavy focus on documentation and audits may slow operational agility in fast-paced manufacturing environments.

**The Traditional 4-Steps Model and the Pentagon of Trust Model.** In 2005, Piscitello

put forward the "Pentagon of Trust" model. This model combines the admissibility attribute with the traditional 4-step model comprising confidentiality, integrity, authenticity, and availability (Moghaddasi et al., 2016). Admissibility pertains to the condition where the status of the data is deemed licit or acceptable.

The Pentagon of Trust Model is particularly relevant for electronic records and signatures under frameworks like FDA 21 CFR Part 11(US FDA, 2003) and EU Annex 11(European Commission, 2011). The admissibility concept of this model aligns closely with regulatory compliance in pharmaceutical operations. In a GMP-regulated environment, data must not only be accurate and secure but also be provably legitimate, a requirement in audits and legal scrutiny. In regulatory inspections, the ability to prove that data is both secure and admissible is crucial, especially in validation reports, batch release documents, and clinical data submissions. However, the model, while conceptually robust, is less prescriptive in terms of practical implementation, offering limited guidance on how to technically ensure admissibility.

**The Evolutionary Circles of Information Security Model.** In 2012, Cherdantseva and Hilton introduced privacy, cost-effectiveness, efficiency, transparency, and auditability as new data security concepts in response to essential commercial requirements. Their model encompasses 14 attributes that address data security across five evolving domains: integrity, confidentiality, availability, reliability, cost-effectiveness, non-repudiation, possession, privacy, authenticity, usefulness, efficiency, accountability, auditability, and transparency (Moghaddasi et al., 2016). According to the creators of this model, data security has evolved from a basic concept managed solely by technical staff to a sophisticated framework overseen by high-level management.

The Evolutionary Circles of Information Security Model focuses on the dynamic nature of security threats, particularly relevant in environments where new technologies (e.g., AI in

drug discovery, smart sensors) are rapidly adopted. It encourages a layered and adaptive security approach. However, this model is conceptually abstract, with limited prescriptive value. Also, it may be challenging to align with rigid validation protocols required by regulatory agencies.

Table 6 illustrates the models' relevance, practical implications, and effectiveness in the pharmaceutical domain. In pharmaceutical manufacturing, ISO/IEC 27001 offers the most holistic and regulatory-aligned approach, though it comes with high implementation costs. The CIA Triad and Five Pillars Model provide a strong foundational baseline but lack operational specificity. Models like the Parkerian Hexad and Pentagon of Trust fill important conceptual gaps, especially around authenticity and trust, while the Evolutionary Circles Model supports a forward-looking strategy. Although no single model fully addresses the multifaceted challenges of pharmaceutical data security, a blended approach that leverages the strengths of multiple frameworks may offer the most robust security posture for this sector.

**Table 6**

*Relevance and Impact of Data Security Models in Pharma*

Model	Strengths	Weaknesses	Best Use Case
CIA Triad	Simple, foundational, regulatory-aligned	Too basic for nuanced threats	Baseline security evaluation
Parkerian Hexad	Broader conceptual coverage (authenticity, utility, possession)	Ambiguous implementation pathways for possession/control and utility	Advanced risk profiling and IP protection
Five Pillars of Information Assurance	Strong focus on accountability, access control, and auditability	Conceptual overlap with other models; limited emphasis on physical/process security; includes procedural methods (not attributes), reducing conceptual clarity	Signature control, data lineage (traceability), audit readiness
ISO/IEC 27001	Globally recognized, risk-based, GxP-aligned	Resource-intensive, rigid documentation requirements	Comprehensive compliance strategy and information security strategy
Pentagon of Trust	Focus on ethical admissibility	Not operationally prescriptive, lacks technical detail	Governance, third-party assurance
Evolutionary Circles	Adaptive, strategic, layered, maturity-driven	Not prescriptive, lacks implementation guidance, abstract	Long-term strategic information security planning

### 2.5.3 Data Security Management and Governance

Data must be adequately managed and governed to address data security challenges effectively, as discussed in sections 2.4.3 and 2.4.4. As Moghaddasi et al. (2016) notes, data security as a condition or state that results from such effective management. Nonetheless, Strengtholt (2020) highlighted the importance of data security management in successfully operating and scaling contemporary organizational environments. According to the Data Management Association, data security management is divided into planning and control activities (Mosely et al., 2009). The planning phase involves formulating data security standards, while the control phase includes defining security controls and conducting data security audits. However, Mosely et al. (2009) assert that an effective data security management function establishes robust governance mechanisms that are sufficiently easy for all stakeholders to comply with in day-to-day operations. Data governance driven by data security requires developing comprehensive policies, standards, and procedures. (Morabito, 2015). Additionally, it entails developing data security controls (Ballard et al., 2014; Tallon et al., 2014), conducting thorough risk assessments (Ballard et al., 2014; De Abreu Faria et al., 2013; Khatri & Brown, 2010), and clearly defining data security roles (Mosely et al., 2009; Khatri & Brown, 2010). Furthermore, auditing practices are necessary to ensure that the procedures and practices align with security policies, standards, and guidelines (Palczewska et al., 2013).

**Risk Assessment.** Risk is ever-present and constantly evolving. This reality is especially true when business operating environments, both external and internal, change dramatically, such as through changes in management or control settings or threat landscape. Additionally, malicious hackers are always seeking loopholes in data security systems, and simply accepting these risks exposes an enterprise to excessive liabilities. Therefore, businesses must identify, analyze, and manage data security risks. Jiao (2020) describes risk assessment

of this nature as the process of identifying, analyzing, and evaluating risk factors associated with business data.

A data risk assessment involves identifying all types of data, reviewing locations that store and manage sensitive information, including IP and PII, as well as identifying those who access it and any changes to data access controls. It may also include examining files, databases, shared drives, and collaboration tools to determine if they contain critical information regarding customers, clients, employees, business-sensitive data, or projects. A data risk assessment provides visibility into all potential threat vectors that could lead to security breaches or privacy violations. Furthermore, risk assessments help identify and address gaps that can worsen in the event of a cyber risk due to the lack of key controls (Khan, 2016). However, managing risk necessitates a commitment to identifying and analyzing new risk factors, along with acquiring or developing new controls to tackle ongoing threats to data security (Jiao, 2020). According to Jiao (2020), establishing and implementing an internal control system for data protection and reducing internal risks is the appropriate course of action.

**Data Security Policy and Standards.** An organization, along with its regulators and stakeholders, has specific needs regarding data access, confidentiality, and protection. A data security policy establishes a structured framework and guidelines to align organizational practices with operational requirements. According to Mosely et al. (2009), formulating a data security policy relies on identifying data security requirements and fostering collaboration among data stewards, IT security administrators, legal departments, as well as internal and external audit teams. However, it is common for IT security policies and data security policies to be merged into a combined security policy. Mosely et al. (2009) recommend separating the data security policy from the IT security policy because the former is more granular and data-driven than the latter. Furthermore, Chapple et al. (2018) emphasized that an organization can develop a practical and enforceable data security policy tailored to its needs, which prescribes

the application of specific security controls to protect data. While the Managed Data objective of the COBIT Core Model provides policies for data management, quality assessment, cleansing, and privacy (ISACA, 2018a), additional policies addressing technical aspects such as data classification, access control, encryption, retention, disposal, backup, recovery, and supplier relationships (ISO, 2022b) are essential for a comprehensive and robust policy framework.

**Control Objectives and Controls for Data Security.** Control objectives are essential for mitigating data security risks. Organizations must also implement effective controls to meet the requirements of relevant legislation (Mosely et al., 2009). ISACA provided control objectives for data security as part of an IS audit/assurance program for cybersecurity (Cybersecurity Audit Program, n. d.). According to ISACA's control objectives, “information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information”. The audit program also identified the necessary controls to achieve the data security control objective: protection of data-in-transit; data-at-rest; protection against data leaks; maintenance of adequate capacity for availability; management of assets throughout their removal, transfers, and disposition; separation of development, testing environment, and production environments; maintaining software, firmware, and information integrity (Cybersecurity Audit Program, n. d.).

Data security controls can take various forms. Van Stone and Halpert (2018) emphasized several common data protection controls and considerations related to data security planning, which include data classification, data loss prevention, encryption, user awareness, access management, antimalware, firewalls, and logging and monitoring. These common data protection controls are addressed by the following COBIT 5 data security governance practices, which are also illustrated in Figure 23.

**Define System and Data Ownership.** Define and uphold the responsibilities linked to information (data) ownership and information systems. Owners should make informed decisions about classifying and protecting information and systems based on that classification. System owners must also consider the criticality and sensitivity of the data when making decisions about classifying and protecting information and systems according to that classification.

**Figure 23**

*COBIT 5 Data Security Governance Practices*



**Note.** Based on the content in “Mistakes Happen: Mitigating Unintentional Data Loss,” by

M. Van Stone, & B. Halpert, 2018, *ISACA Journal*, pp. 23-29.

([https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/mistakes-](https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/mistakes-happenmitigating-unintentional-data-loss)

[happenmitigating-unintentional-data-loss](https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/mistakes-happenmitigating-unintentional-data-loss)).

**Manage Contract Personnel.** Contract personnel and consultants supporting the enterprise with IT skills must be aware of and comply with organizational policies and agreed-upon contractual requirements. Managing contract personnel also includes verifying that all



contractors receive the necessary training and understand data protection policies. Contract personnel should work under terms that align with the organization's security, confidentiality, and compliance standards.

**Identify and Classify Information Sources.** Identify, validate, and categorize various sources of internal and external information necessary to effectively operate business processes and IT services. Proper classification helps streamline access and manage security protocols efficiently.

**Organize and Contextualize Information into Knowledge.** Arrange information according to classification criteria. Identify and establish meaningful connections among the information elements and facilitate their use. Determine ownership and define and implement access levels for knowledge.

**Protect against Malware.** Implement and maintain enterprise-wide prevention, detection, and remediation measures, with particular emphasis on applying updated security patches and ensuring robust virus protection. Ensure timely updates and continuous monitoring to strengthen defenses against worms, viruses, spam, spyware, and other forms of malware. This control safeguards information systems and technology from worms, viruses, spam, spyware, and other malware.

**Manage Network and Connectivity Security.** Implement comprehensive security measures and management procedures to protect information across all connectivity methods, ensuring secure access to business resources. This control includes secure protocols, firewalls, and encryption where necessary to prevent unauthorized access.

**Manage Endpoint Security.** Ensure that endpoints, including servers, desktops, network devices, software, laptops, and other mobile devices, meet or exceed the security requirements for storing, processing, or transmitting information. Enforce regular security

updates and access controls across all endpoints. Effective endpoint security reduces the risk of unauthorized access and data breaches.

**Manage User Identity and Logical Access.** Ensure that information is accessible to all users according to their business needs and collaborate with the business units that oversee their access rights for business processes. This control protects data confidentiality by applying role-based access control to protect data confidentiality. Access privileges should be regularly reviewed and updated as roles evolve within the organization.

**Manage Sensitive Documents and Output Devices.** Implement appropriate physical protection measures, accounting practices, and inventory management for sensitive IT assets such as security tokens, negotiable instruments, special-purpose printers, or special forms. Additionally, ensure restricted access and logging for all handling of sensitive assets. This control reduces the risk of data leaks and unauthorized use of sensitive resources.

**Monitor Security-related Events within the Infrastructure.** Implement intrusion detection systems to monitor the infrastructure for unauthorized access attempts, ensuring that all events are included in the broader incident and event monitoring management framework. Using intrusion detection systems enables real-time alerts for suspicious activities. An integrated monitoring approach helps identify potential security threats proactively and supports faster response times.

**Manage Roles, Responsibilities, Levels of Authority, and Access Privileges.** Manage the business roles, responsibilities, segregation of duties, and authority levels needed to support the objectives of the business process. Authorize access to all information assets linked to business information processes, including those held by IT, business, and third parties. This control ensures that the organization understands where data is located and who is processing it on its behalf.

**Maintain Traceability of Data Events and Accountabilities.** Ensure that business information can be traced back to the original business event and the responsible parties. This control allows for tracking information throughout its life cycle and associated processes. It also guarantees that the information feeding the business is reliable and has been processed according to its intended purpose.

**Secure Information Assets.** Secure enterprise information assets, including electronic information (such as user applications, portable media devices, storage devices, and methods that generate new assets in any form), physical information (like source documents and output reports), and information during transit using approved methods. This control benefits the company by ensuring comprehensive information protection.

These governance practices aim to combat intentional and unintentional threats, both internal and external, to data protection. They also establish defense-in-depth strategies to ensure data security. Now we discuss data security controls specific to cyber defence.

**Data Security Controls for Cyber Defense.** Effective data security demands a framework that not only aligns with industry standards but also drives real, actionable protection. The Center for Internet Security (CIS) Critical Security Controls (CSCs) provide such a framework, translating security principles into concrete steps and making it a powerful choice for data security. Although CIS controls align with the leading compliance frameworks from the Payment Card Industry (PCI), NIST, HIPAA, ISO, and COBIT (Maennel et al., 2018), they offer a distinct advantage for organizations prioritizing data security. Groš (2021) highlights that the primary difference between CIS CSCs and other frameworks like the PCI Data Security Standard, ISO 27001, and NIST Special Publication 800-53r5 is that CSCs require actual implementation rather than leaving adoption as optional based on a risk assessment.

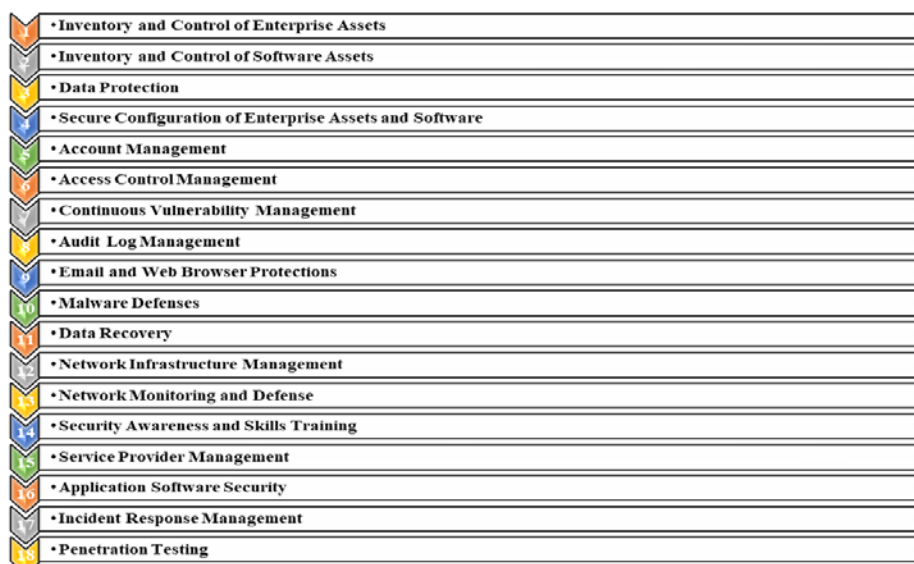
CIS CSCs primarily focus on cyber defense. Frangie et al. (2018) describe CIS controls as a collection of priority actions that protect critical systems and data within an organization from the most common cyber threats. CIS controls offer a concise set of high-priority and high-effectiveness defensive measures that provide a "to-do first" starting point for any organization looking to bolster its cybersecurity defense (CIS Critical Security Controls [CSC] Version 8, n. d.). These controls represent essential first steps in safeguarding an organization's integrity, mission, and reputation. Kobezak et al. (2018) maintain that the CSC framework provides an organization with key areas to focus its efforts. The purpose of these controls is to assist organizations in concentrating on the most critical cybersecurity measures for their protection (CIS CSC Version 8, n.d.). According to Venkatesh (2018), these measures aim to help organizations promptly establish the starting point for defense, allocate limited resources for actions that deliver immediate and high-value benefits, and direct attention and resources toward other risks specific to the organization or its mission. They consist of a set of recommended measures that provide precise and achievable means of countering the most pervasive attacks (Venkatesh, 2018). Originally outlined with 20 critical security controls (Sabillon et al., 2016, p.76), the framework was revised to eighteen controls, as depicted in Figure 25 and outlined below (CIS CSC Version 8, n. d.):

Inventory and Control of Enterprise Assets...Inventory and Control of Software Assets... Data Protection...Secure Configuration of Enterprise Assets and Software...Account Management...Access Control Management...Continuous Vulnerability Management...Audit Log Management...Email and Web Browser Protections...Malware Defenses...Data Recovery...Network Infrastructure Management...Network Monitoring and Defense...Security Awareness and Skills Training...Service Provider Management...Application Software Security...Incident Response Management...Penetration Testing.

To scale the framework across organizations of various sizes, CIS introduced implementation groups (IGs). There are three IGs that organizations can utilize depending on their cybersecurity capabilities. According to Groš (2021), micro-enterprises fall into IG1, small and medium-sized enterprises fit into IG2, and large enterprises are aligned with IG3. Additional criteria that organizations may use to identify their IG include data sensitivity, service criticality, the level of skills, and the resources available to address cybersecurity. The IGs accumulate in such a way that IG2 includes all the sub-controls defined in IG1, and IG3 includes all the sub-controls defined in IG2. Therefore, the recommended approach for implementing CIS Controls starts from the lower implementation group sub-controls and progresses to the higher ones (CIS CSC Version 8, n. d.). Essentially, the concept is that the smallest enterprises implement only IG1, while the largest enterprises implement all three implementation groups.

**Figure 24**

*Centre for Internet Security Critical Security Controls*



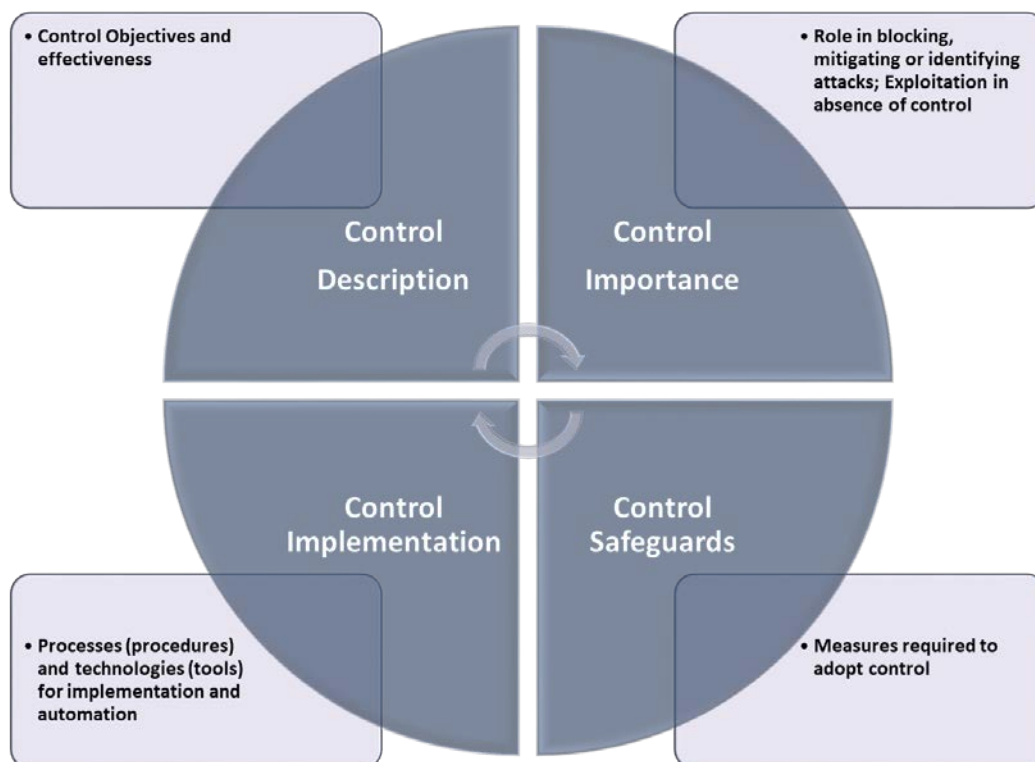
**Note.** Based on content from *CIS Critical Security Controls Version 8* (n. d.), Center for

Internet Security. [https://learn.cisecurity.org/e/799323/1-799323-2020-07-22-](https://learn.cisecurity.org/e/799323/1-799323-2020-07-22-28vhr/34gng/353120386?h=PFal4bZFIsWyxUZLtapobIQYuJN4rdKfpl2c7F7301o)

[28vhr/34gng/353120386?h=PFal4bZFIsWyxUZLtapobIQYuJN4rdKfpl2c7F7301o](https://learn.cisecurity.org/e/799323/1-799323-2020-07-22-28vhr/34gng/353120386?h=PFal4bZFIsWyxUZLtapobIQYuJN4rdKfpl2c7F7301o)

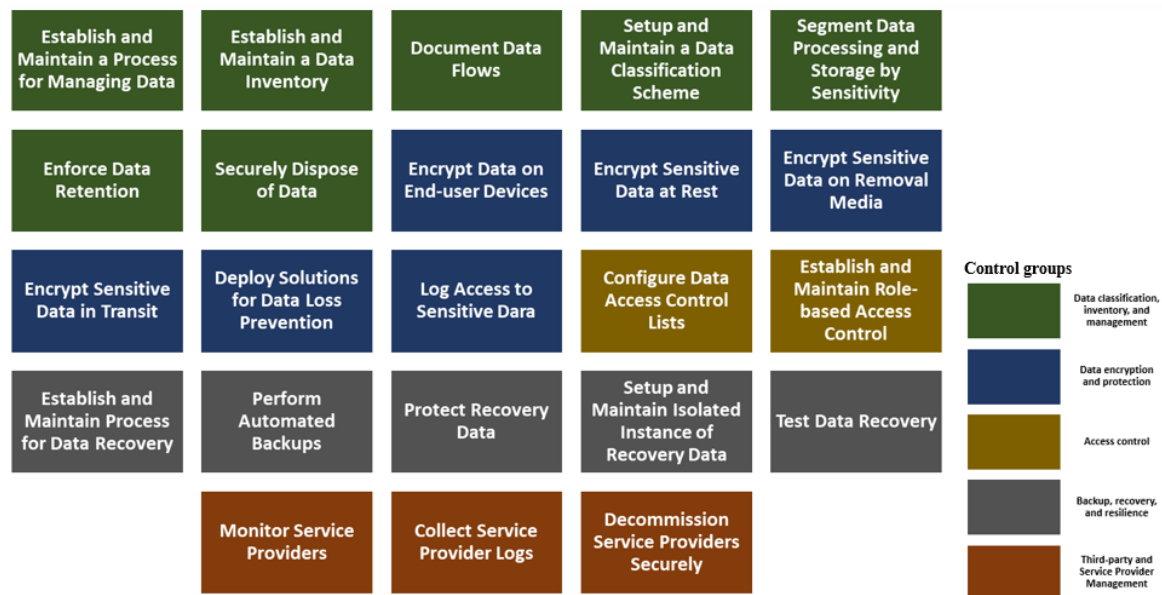
Some pharmaceutical organizations have embraced CIS CSCs as a cybersecurity framework. CordenPharma is a global contract development and manufacturing organization (CDMO) with cGMP-compliant facilities worldwide (Global API, excipient, drug product, & packaging CDMO, n. d.). It provides end-to-end services from drug development to manufacturing under contract for other companies in the pharmaceutical industry (About us, n.d.). CordenPharma needed a more standardized security program to address the diverse security requirements of its 20 to 30 clients (CordenPharma adopts CIS Controls as their framework, n.d.). CordenPharma adopted CIS Controls as a framework because it effectively served the needs of its customers. Using the CIS Control spreadsheet, they assessed which systems met various controls and identified where they failed to meet a requirement (CordenPharma adopts CIS Controls as their framework, n.d.). They also verified solutions according to the CIS control descriptions and implemented them accordingly. Consequently, CIS Controls effectively addressed CordenPharma's needs, which impressed their clients.

CIS Controls v8 has been enhanced to remain at the forefront of today's systems and software. The shift to cloud computing, mobility, outsourcing, virtualization, remote work, and evolving attacker tactics prompted this update and bolsters an organization's security as it transitions to all-cloud and hybrid environments. Figure 26 illustrates that the presentation of each of the 18 controls in CIS Controls v8 features an outline with a brief description of the control's objective and its effectiveness as a defensive measure; an explanation of the importance of this control in blocking, mitigating, or identifying attacks, along with details on how attackers actively exploit the absence of this control; a more technical overview of both processes (procedures) and technologies (tools) that facilitate the implementation and automation of this control; and specific measures (safeguards) that organizations must undertake to adopt the control.

**Figure 25***Structure of a Critical Security Control*

**Note.** Based on content from *CIS Critical Security Controls Version 8* (n. d.), Center for Internet Security. <https://learn.cisecurity.org/e/799323/1-799323-2020-07-22-28vhr/34gng/353120386?h=PFal4bZFIsWyxUZLtapobIQYuJN4rdKfpl2c7F7301o>

The controls regarding data assets, as outlined in CIS CSC Version 8 (n. d.), include the safeguards of Control 3, “Data Protection,” and Control 11, “Data Recovery”, along with CIS safeguards CSC 6.8, “Define and Maintain Role-Based Access Control”, CSC 8.12, “Collect Service Provider Logs”, CSC 15.6, “Monitor Service Providers”, and CSC 15.7, “Securely Decommission Service Providers”. These CSCs, incorporated in the Data Security Control Framework (DSCF), as shown in Figure 27, address data security controls for cyber defense and are discussed below:

**Figure 26***Data Security Controls Framework for Cyber Defence*

**Note.** The Data Security Controls Framework for Cyber Defence was synthesized by the author based on content from *CIS Critical Security Controls Version 8* (n. d.), Center for Internet Security. <https://learn.cisecurity.org/e/799323/1-799323-2020-07-22-28vhr/34gng/353120386?h=PFal4bZFIWyxUZLtapobIQYuJN4rdKfpl2c7F7301o>

**Establish and Maintain a Process for Managing Data.** Develop and maintain a comprehensive data management process that covers data ownership, sensitivity, handling, disposal requirements, and retention limits in accordance with the organization's sensitivity and retention standards. Review and update relevant documentation annually or whenever significant organizational changes occur that may affect this safeguard.

**Establish and Maintain a Data Inventory.** Develop and maintain a comprehensive data inventory in accordance with the enterprise data management process. This measure should include, at a minimum, an inventory of sensitive data. Ensure the data inventory is continuously updated to reflect any new data types or sources introduced to the organization. Review the inventory annually, with a particular emphasis on ensuring the completeness and



accuracy of sensitive data records.

**Document Data Flows.** Document data flows, including those from service providers, according to the enterprise data management process. Review and update documentation annually or whenever significant organizational changes occur that could impact this safeguard. Identify key points in the data flow where data moves between secure and less secure environments, so that specific security controls are applied at those transitions. Monitor data across internal systems and external service providers to maintain a comprehensive view of data movement. Use flow diagrams to visualize data pathways, supporting compliance, security assessments, and incident response.

**Setup and Maintain a Data Classification Scheme.** Implement and maintain an enterprise-wide data classification system. Review and update the classification system annually or whenever significant changes within the enterprise could affect this protective measure. Ensure that the classification system includes criteria for data sensitivity, regulatory implications, and access requirements. Conduct training to ensure that all employees understand data classification and handle data appropriately. Regularly assess data classification levels to verify that data is categorized accurately and reflects its current usage and sensitivity.

**Segment Data Processing and Storage by Sensitivity.** Separate data processing and storage based on the sensitivity of the data involved. Refrain from processing sensitive data on enterprise assets intended for less sensitive information. In addition, implement network and system segmentation to establish barriers between different data sensitivity levels. Also, create procedures to ensure that only authorized personnel can access sensitive processing and storage environments. Regularly review and adjust segmentation measures to respond to any data sensitivity or regulatory requirements.

**Enforce Data Retention.** Retain data according to the enterprise data management

process. Data retention should encompass maximum and minimum timeframes. Establish retention schedules based on data sensitivity, regulatory requirements, and business needs, ensuring obsolete data is not kept beyond its usefulness. Automate retention policies whenever feasible to reduce manual oversight and human error risk. Periodically review data retention policies to reflect changes in regulatory standards or enterprise data usage patterns.

**Securely Dispose of Data.** Dispose of data securely following the enterprise data management process. Ensure that the disposal method and process align with the data's sensitivity. Use secure disposal methods, such as data wiping or physical destruction, to prevent data recovery on outdated devices. Keep disposal records to demonstrate compliance with data retention and disposal policies. Regularly review disposal procedures to adjust for new data storage technologies and disposal standards.

**Encrypt Data on End-user Devices.** Encrypt data on end-user devices that store sensitive information. Implement encryption protocols that adhere to industry standards for data protection to prevent unauthorized access in the case of device loss or theft. Regularly update encryption software and protocols to fix security vulnerabilities. Educate users about the importance of encryption practices and ensure that encryption is activated and cannot be bypassed on all relevant devices.

**Encrypt Sensitive Data at Rest.** Encrypt sensitive data at rest in applications, databases, and servers. Use storage-layer encryption (server-side encryption) as a minimum requirement and application-layer encryption (client-side encryption), where access to data storage devices does not allow plain-text access to the data. Use secure transmission protocols like TLS to protect data as it moves across internal and external networks. Regularly rotate and securely manage encryption keys to maintain data confidentiality. Monitor data transmission activities to identify and respond to any unauthorized data transfers or protocol vulnerabilities.

**Encrypt Data on Removable Media.** Encrypt data on removable media. Implement a

policy that mandates encryption for all data stored on removable devices to prevent unauthorized access in the event of loss or theft. Ensure that encryption keys are securely stored and accessible only to authorized personnel. Regularly audit removable media usage and enforce compliance with encryption policies throughout the organization.

**Encrypt Sensitive Data in Transit.** Encrypt sensitive data while in transit. Use secure transmission protocols, such as TLS, to safeguard data as it travels across both internal and external networks. Regularly rotate and securely manage encryption keys to ensure data confidentiality. Monitor data transmission activities to detect and address any unauthorized transfers or weaknesses in protocols.

**Deploy Solutions for Data Loss Prevention.** Implement an automated system to identify all sensitive data that is processed, stored, or transmitted through enterprise assets, including those located on-site or with remote service providers. Configure data loss prevention solutions to monitor and alert on policy violations, thereby preventing unauthorized data transfers. Educate employees on the significance of data loss prevention policies and practices to strengthen data protection efforts. Regularly assess and optimize data loss prevention configurations to ensure they align with evolving data protection needs and business goals.

**Log Access to Sensitive Data.** Log access to sensitive data, including modifications and disposals. Review these logs regularly for signs of unauthorized access, data tampering, or improper disposal activities. Maintain access logs following retention policies and safeguard them against unauthorized alterations.

**Configure Data Access Control Lists.** Set up and manage data access control lists to ensure access permissions align with user need-to-know principles. Apply access permissions to applications, databases, and local and remote file systems. Establish procedures for requesting and granting access to sensitive information according to documented authorization workflows. Implement monitoring to detect and report any unauthorized attempts to access

sensitive data. Regularly audit access control lists to identify and eliminate unnecessary permissions to reduce exposure to unauthorized access.

**Establish and Maintain Role-based Access Control.** Define and maintain role-based access control by identifying and documenting the access rights needed for each role within the organization to effectively perform assigned tasks. Implement least privilege principles by restricting access rights to the minimum necessary for each role. Regularly conduct access reviews to identify and address any privilege creep over time. Conduct annual access control reviews of enterprise assets to ensure all privileges are authorized. Educate personnel on the importance of access control policies and procedures.

**Establish and Maintain Processes for Data Recovery.** Establish and maintain a data recovery process. This process should outline data prioritization, recovery activities, and backup security. Review and update documentation annually or when significant changes within the enterprise may impact this safeguard. Also, regularly test recovery processes to validate their effectiveness and ensure the organization's preparedness. Identify recovery time objectives for critical data to minimize disruption in the event of data loss.

**Perform Automated Backups.** Automate the backup of relevant enterprise assets. Perform weekly backups based on data sensitivity. Schedule backups during low-traffic times to minimize operational impact. Store backups in secure locations, ensuring both physical and network security for the backup systems. Regularly verify backup integrity to confirm that data can be successfully restored when necessary.

**Protect Recovery Data.** Safeguard recovery data with controls equivalent to the original data. Reference data separation and encryption according to requirements. Implement access restrictions to ensure that only authorized personnel can access recovery data. Regularly review protection measures for recovery data to align with evolving security standards. Protect backup storage locations using physical and network security controls to prevent unauthorized

access or loss.

**Setup and Maintain an Isolated Instance of Recovery Data.** Establish and maintain an isolated recovery data instance to safeguard recovery data from incidents that might affect primary data environments. Regularly test the isolated recovery instance to verify that it remains functional and uncorrupted. Limit access to the isolated instance, ensuring that only authorized personnel can carry out recovery operations.

**Test Data Recovery.** Test backup recovery at least quarterly for a sample of enterprise assets within scope. Conduct tests under simulated conditions to ensure that recovery times meet organizational needs. Document recovery test results and address any identified issues to enhance future recovery efforts. Provide regular training for recovery personnel to keep them familiar with recovery procedures.

**Monitor Service Providers.** Monitor service providers in line with the organization's service provider management policy. Regularly assess service provider performance and compliance with established security and data protection standards. Conduct audits and request periodic reports to ensure adherence to the agreed service SLAs and compliance requirements. Additionally, establish procedures for escalation if a service provider does not meet performance or security expectations.

**Collect Service Provider Logs.** Collect logs from service providers where supported. Aggregate these logs into a centralized log management solution for improved analysis and incident response. Regularly review service provider logs for any suspicious or unexpected activities to ensure compliance and security. Ensure that the collected logs are securely stored and access-controlled to maintain their integrity and confidentiality.

**Decommission Service Providers Securely.** Ensure service providers are decommissioned securely. Ensure that access related to a decommissioned provider is fully removed from systems to prevent unauthorized access. Retrieve any sensitive data stored with

the provider before termination, confirming proper deletion or transfer procedures. Document the decommissioning process for audit and compliance purposes.

**Data Security Auditing.** Auditing is an integral part of data governance. Auditing is a “methodical examination and review” (Merriam-Webster, n. d) and a valuable tool for effective risk management. Khan (2016) maintains that data security audits enhance an organization’s maturity level in combating the ever-growing threat of internal malicious data loss and cyber espionage by both employees and temporary workforces. He also asserts that every audit function should examine data protection and cybersecurity within their respective enterprise and collaborate with key departments to identify, reduce, and eliminate gaps as much as possible.

The foundation for data security auditing includes data security policy statements, standards documents, change requests, implementation guides, access monitoring logs, output reports, and other electronic or hard copy records. The purpose of auditing data security is to provide the data governance council and management with an objective, unbiased evaluation, along with sound, practical recommendations (Mosely et al., 2009). Like other audit engagements, data security auditing is a recurring control activity that involves analyzing, validating, advising, and recommending policies, standards, and practices related to data security management.

As Khan (2016) notes, the audit function should independently review the organization’s management of risks associated with data loss prevention through comprehensive enterprise-wide risk assessments and audits of data protection and cybersecurity. Therefore, data security auditors must be independent of the data they evaluate and should not be directly responsible for the activities under review. This separation guarantees an unbiased and objective assessment. Mosely et al. (2009) outline various activities involved in data security auditing: analyzing data security policies and standards in accordance

with best practices and requirements; assessing current implementation procedures and practices to ensure alignment with data security goals, policies, standards, guidelines, and expected outcomes; evaluating the adequacy of existing standards and procedures and their alignment with operational and technological needs; verifying the organization's compliance with regulatory requirements; checking the accuracy and reliability of security audit data; reviewing escalation procedures and reporting mechanisms in the event of a data security breach; auditing contracts, data sharing arrangements, and data security obligations of outsourced activities and external vendors to ensure they meet their commitments and that the organization fulfills its obligations concerning data from external sources; reporting to data stewards, senior management, and other stakeholders on the security posture and the maturity of practices within the organization; and recommending improvements in the design, operation, and compliance of data security.

In addition to reviewing organizational controls, data security audits may also include checks and tests of physical and technological aspects. ISACA's audit program (Cybersecurity Audit Program, n.d.) outlines procedures to assess the effectiveness of data security controls. These testing procedures detail how to evaluate control activities and gather supporting documentation. Testing activities may be part of internal or external audits of data security controls against inherent risks.

**Data Security Officer.** Data protection regulations, such as GDPR or NDPR, require that organizations designate a formal Data Protection Officer (DPO). According to NDPA, a major data controller is required to appoint a DPO (Adeoti, 2023). The DPO advises data controllers and processors on handling personal data, monitors compliance with NDPA, and serves as the primary point of contact for the NDPC concerning data processing issues (NDPA, 2023, § 32). According to the NDPR, both data controllers and processors are required to appoint a DPO (Adeoti, 2023; Babalola, 2022; Chika & Tochukwu, 2020). While the NDPR

does not contain specific provisions regarding the role of the DPO, its implementation framework outlines the DPO's responsibilities: advising the data controller on its obligations under the NDPR, monitoring compliance, and coordinating with the NITDA and DPCO on data protection matters (NDPR documentation). Furthermore, the NDPR does not address issues related to conflicts of interest. Babalola (2022) argues that this deficiency makes a DPO susceptible to undue influence and directives from their appointing bodies, compromising their ability to fulfill compliance responsibilities. He also points out that the implementation framework inconsistently conflicts with the NDPR regarding the types of data controllers required to appoint a DPO. This contradiction implies that not all controllers are mandated to designate a DPO. Additionally, DPOs may feel frustrated in trying to carry out their designated tasks due to the authority they hold within their organizations. Under the NDPR, a DPO does not need to operate with complete independence or report directly to the highest management level of the organization; however, they are responsible for ensuring compliance with the regulation (Babalola, 2022). Another significant challenge facing the evolving role of the DPO is the shortage of qualified professionals. Chika and Tochukwu (2020) assert that Nigeria lacks adequate active practitioners in this field. This shortage hampers the effective implementation and oversight of data protection practices, further limiting the impact of the DPO's evolving role in Nigeria.

Nonetheless, a DPO plays a critical role in data protection. The DPO's role is largely focused on protecting privacy and personal data. The Summary Chart of the Global Skills and Competency Framework identified personal data protection as a crucial skill in the digital era (SFIA 8 Summary Chart, n.d.) that a DPO should possess. However, protecting personal data, one aspect of privacy, cannot be effective without data security. Jiao (2020) claims that data privacy hinges on security. Ballard et al. (2014) argue that you cannot have privacy without security, but you can have security without privacy. They also maintain



that the implementation of data security controls is part of the protection phase of the privacy operational life cycle. Furthermore, Khatri and Brown (2010) opine that the data security officer could play a role or be responsible for access to the data, especially for specifying data access requirements. They also highlighted the risk analysis conducted by a data security officer that determines an organization's data requirements and safeguards for data confidentiality, integrity, and availability. Given the risks to data security and Ballard et al. (2014) claim that good security practices underpin effective privacy practices, the DPO role should evolve into a data security officer (DSO) role.

#### **2.5.4 Data Leakage and Prevention**

Manufacturers recognize the strategic value of manufacturing data, which is always at risk of leakage or loss. Concerns about data leakage are growing in both government and business sectors (Alneyadi et al., 2016). The manufacturing industry is particularly facing a data security concern related to data leakage due to the large volumes of data generated by factories. Data leakage is becoming more diverse, fueled by continuous factory data streams. Data leakage is an insider threat that affects many organizations and involves intentionally disclosing sensitive information (Alneyadi et al., 2016; Alhindi et al., 2021). Alneyadi et al. (2016) identified various channels through which data is leaked: email, social media, USB, printer, laptop, tablet, smartphone, fax, and CD. However, they overlooked the data-leaking channels in smart factories, such as IIoT devices, apps, and services. IoT devices are often susceptible to attacks due to inadequate built-in security features and a lack of regular updates or maintenance. For instance, Bayer experienced security breaches involving IoT devices used in production, which exposed industrial systems to potential remote access, disrupted automated workflows, and delayed drug manufacturing processes (Khan et al., 2025). Therefore, smart factories may leak sensitive manufacturing data from identified and unidentified sources, indicating a weak security posture. Data does not lose itself; rather, it

results from human actions. Whether due to negligence, compromised behavior, or malicious intent, individuals are often the cause of data being exposed or mishandled (Khan et al., 2025). One of the greatest threats to organizational data security is employee behavior. Verizon (n.d.) states that 82% of data breaches include a human element, while the Ponemon Institute (n.d.) indicates that 44% of insider incidents arise from compromised or malicious users. The actions of a single employee, whether intentional or inadvertent, can threaten an organization's data security, leading to serious consequences.

For instance, consider a situation where an employee is planning to leave the company and join a competitor. While working remotely, she has access to the company's IP stored in the cloud and feels entitled to take what she helped create, deciding to take it with her. From her home office, she downloads sensitive research files to her work laptop. She further violates security protocols by installing her personal Google Drive on the laptop and transferring all work-related files to her personal cloud storage. In this scenario, the employee's actions are not only malicious but also represent a significant breach of trust, potentially causing irreversible damage to the company's competitive edge.

Negligence can also result in data breaches, even in the absence of malicious intent. Consider another employee who, while not acting with ill intent, is careless with the sensitive data he handles. He works from various locations, using whichever tools are most convenient for completing his tasks without considering the security implications. This employee has access to PII and PHI, both of which require careful handling. Yet, his casual approach to data management leads to multiple security incidents. For instance, he accidentally sends an email containing a spreadsheet titled "PHI.xls" to the wrong recipient. Realizing his error, he forwards the document to his personal email account for safekeeping. His careless handling continues when he uploads the same file to the company's cloud storage, setting the sharing permissions to 'Public link,' thus potentially exposing the data to unauthorized parties. His

negligent behavior escalates as he copies the file to a USB drive or uploads it to commercial file-sharing platforms, increasing the risk of unintentional data leaks. He takes it a step further by pasting sensitive data into prompts on GenAI platforms without considering the risks these unsecured environments pose. Using risky GenAI sites to process company data, sharing sensitive information publicly from cloud services, and allowing anomalous data transfers are just a few of the ways this employee inadvertently jeopardizes the organization's data risk

These scenarios illustrate how both negligence and malicious intent in managing company data can lead to serious data breaches. Ultimately, the core issue lies not in the data itself but in how individuals handle it. Hughes-Lartey et al. (2021) emphasizes that cybercriminals exploit human factors, such as errors or risky behavior, as weak links in an organization's security framework. To mitigate these risks, organizations need clear visibility into user activities on their assets, which necessitates insider threat management to monitor user activities. User activity monitoring helps identify and prevent risky behavior while capturing visual evidence supporting security investigations (Spooner et al., 2018). However, to address the needs of modern information protection and safeguard sensitive data, insider threat management must be integrated with data loss prevention.

**Data Loss Prevention.** Data loss prevention (DLP) is a critical data security control against insider threats. DLP refers to a security system or strategy that prevents the unauthorized transfer of sensitive information by end-users outside the organization's network (Alhindi et al., 2021). Spooner et al. (2018) identified DLP as an important technical measure for an effective insider threat program. Organizations typically implement solutions to prevent data exfiltration and loss to minimize risks and comply with GDPR (AlKilani et al., 2019). These controls are particularly advantageous for insider threat programs in drug manufacturing companies, as they help safeguard sensitive formulas, IP, and proprietary research data.

**Data Loss Prevention Solutions.** Effective data security cannot be achieved without

data loss prevention solutions (DLPSs). Alneyadi et al. (2016) conducted a comparative analysis that identified Check Point, Triton, AirWatch, Fidelis XPS, Varonis IDU Classification Framework, and McAfee as leading commercial DLPSs. These solutions feature both preventive and detective capabilities, except Varonis IDU Classification Framework and AirWatch, which offer only detective or preventive functions. However, these solutions primarily benefit large organizations, as their acquisition and implementation costs are often prohibitive for many smaller organizations. Thombre (2020) also highlighted the significant cost and effort required for small to medium-sized organizations in deploying commercial DLPSs like Websense Forcepoint and Symantec. Conversely, the rapid growth of smart manufacturing has prompted an increased focus on open-source solutions (Waters et al., 2022). This trend led Koutsourelis and Katsikas (2014), Thombre (2020), and Ahmad et al. (2022) to introduce free or open-source DLPSs. Spooner et al. (2018) suggested OpenDLP and MyDLP as budget-friendly DLPS options for starting an insider threat program. Although adopting open-source DLPSs incurs no licensing costs and is therefore free to use, manufacturing organizations should ensure that these solutions can effectively safeguard data assets compared to commercial options before deployment. Spooner et al. (2018) recommended that the effectiveness of low-cost DLPSs be evaluated to determine their capability to address gaps in an insider threat program.

**Data Loss Prevention Solution Deployment.** The deployment of DLPSs varies based on the data that needs safeguarding. According to Alneyadi et al. (2016), DLP agents deployed on endpoints protect data in use, while data in transit is secured using DLP appliances. DLPSs that handle data in storage primarily aim to protect known data and restrict access by enforcing predefined security measures and encrypting entire file systems (Alneyadi et al., 2016). In addition to scanning, identifying, and safeguarding confidential data in repositories, these DLPSs also monitor and report security policy violations. Gaidarski and Kutinchev (2021)

modeled the structure, components, and deployment of the Cososys Endpoint Protector (EPP) DLP system. They utilized a Unified Modelling Language (UML) deployment diagram to illustrate the physical implementation of EPP software components and the general deployment of DLPSs: the Device Control module governs removable devices and peripheral ports; Content Aware Protection inspects content; and the eDiscovery software module scans data at rest. At endpoints, the deployed client software or agent manages the relevant data channels such as the wireless network, LAN network, USB ports, etc., or scans data at rest.

**Data Loss Prevention Methods.** Technological weaknesses can arise deliberately, accidentally, or from issues related to design, implementation, or tool limitations. Alneyadi et al. (2016) identified strengths and weaknesses of DLP systems based on their DLP methods: policy and access rights; virtualization and isolation; cryptographic approaches; and quantifying and limiting, which they categorized as preventive methods. They also highlighted data identification; data mining and text clustering; social and behavioral analysis; and quantifying and limiting, which they classified as additional preventive methods. Cheng et al. (2017) identified several content-based strategies used by DLPSs for scanning and identifying sensitive data at rest, in use, and in motion at different points. These strategies include data fingerprinting, lexical content analysis using rule-based methods and regular expressions, as well as statistical analysis. Cheng et al. (2017) argue that these methods can be bypassed by external or internal attackers using data obfuscation, confirming weaknesses in data identification that Alneyadi et al. (2016) noted could prevent DLPSs from accurately detecting sensitive data that has been significantly modified. AlKilani et al. (2019) demonstrated this technological vulnerability when they simulated a threat scenario that sought to evade the Symantec DLP deployed to protect confidential data that may leak through email and USB, i.e., data in motion and data in use. They employed basic techniques for data exfiltration in scenarios involving file structures, such as file fragmentation, encryption, binary manipulation,

and extension faking/merged streaming. Although they proposed solutions for undetectable scenarios, their experiment did not assess the DLPS's ability to scan confidential data at rest. Since the process of DLP begins with identifying sensitive data that needs protection (Pujeri et al., 2023), weaknesses in scanning sensitive data at rest could result in unrecognized data that is either not inventoried or unprotected. Moreover, scanning stored data allows enterprises to effectively identify the risks of data leakage within their internal organization (Cheng et al., 2017). Addressing this gap, Nwosu (2023a) analyzed the effectiveness of commercial and open-source DLPSs in identifying sensitive data at rest, following exfiltration techniques outlined by AlKilani et al. (2019). His study revealed that OpenDLP, an open-source DLP, consistently demonstrated a high success rate in detecting unmodified sensitive data, while the Endpoint Protector (EPP), a commercial DLPS, struggled to detect specific data types, such as unmodified phone numbers and bank account numbers. Scenario-specific results showcase the strengths and weaknesses of DLPSs in handling file fragmentation, encryption, binary manipulation, and extension faking/merge streaming.

**File Encryption.** File encryption transforms data into ciphertext to safeguard privacy from unauthorized access. File-level encryption employs encryption algorithms and unique keys to convert the original content of a file into ciphertext (Gasser & Aad, 2023). However, DLPSs often utilize predefined rules and pattern recognition to analyze file content and identify sensitive data types (Du et al., 2015). Encrypted data appears as random characters, making it difficult for DLPSs to recognize patterns associated with sensitive data. As a result, file-level encryption can bypass the data-at-rest scanning capabilities of OpenDLP and EPP (Nwosu, 2023a), similar to how encrypted files have eluded Symantec DLP's detection mechanisms for data in use and in motion (AlKilani et al., 2019). The ability of encryption to evade detection methods used by DLPSs demonstrates that these systems are vulnerable to data obfuscation.

**File Extension Faking and Merge Streaming.** Merging streams involves combining

multiple sources of data into a single, continuous flow. File compression can be utilized in merge streaming to enhance data transfer efficiency by minimizing the amount of data that needs to be stored or transmitted. However, compressing files obscures their content to prevent detection by security software (Archive collected data, Technique T1560, n.d.). When file extension faking—manipulating or altering a file's extension to disguise its true type (Mohanta & Saldanha, 2020)—is applied to compressed files, the detection mechanisms of security software, particularly those relying on file type recognition, are circumvented. Nwosu (2023a) demonstrated that OpenDLP's data-at-rest scanning functions were vulnerable to data obfuscation when file compression and extension faking were used together. He noted that commercial DLPSs, such as EPP and Symantec DLPSs, identified a file's original format even when its extension was changed and detected confidential files within a zipped file even if the zipped file's extension had been altered (AlKilani et al., 2019; Nwosu, 2023a).

**File Fragmentation.** File fragmentation means dividing individual files into smaller pieces and scattering them across a storage medium. Compressing and splitting files is often used to store or distribute large files more manageably, but it adds complexity that prevents some DLPSs from analyzing and identifying sensitive data within the file structure. For instance, OpenDLP could not detect sensitive data at rest when files were fragmented (Nwosu, 2023a). However, commercial DLPSs, such as EPP and Symantec DLP systems, detected sensitive data in fragmented or split files (AlKilani et al., 2019; Nwosu, 2023a).

**File Binary Manipulation.** Editing file binaries involves manipulating the underlying structure and binary content of files (Mohanta & Saldanha, 2020). File concatenation, which adds one file to another (Ballin et al., 2008), is a way to manipulate binary files. When one file is appended to another, the contents of both files change to evade the data detection mechanisms of DLP systems. For instance, Symantec's DLP system struggled to detect sensitive data when files were concatenated (AlKilani et al., 2019). However, OpenDLP and

EPP can analyze and identify sensitive content within a file, even if it has been appended (Nwosu, 2023a). Another method for manipulating binary files includes modifying file headers through magic number manipulation. When the magic numbers of files are altered, operating systems and security software may have trouble recognizing a file's format, type, or content, as well as how to process it (Mohanta & Saldanha, 2020). For example, when the magic numbers of files were deleted, DLP systems could not identify the actual content of the file, which hindered their ability to accurately detect sensitive data within files (AlKilani et al., 2019; Nwosu, 2023a). Thus, the scanning functions of DLP systems are vulnerable to certain forms of binary file manipulation, such as magic number alteration, while other types of binary file manipulations, like file concatenation, leave some DLP systems unaffected.

In addition to the solutions proposed by AlKilani et al. (2019), ML techniques have shown potential in enhancing the detection capabilities of DLP systems. ML models have been used for content analysis and sensitive data identification (Gugelmann et al., 2015). Also, convolutional and recurrent neural networks have been applied in a deep learning model to extract and categorize sensitive text and photo content with an impressive detection rate (Guha et al., 2021). Additionally, ML supports the use of N-gram analysis, data mining, and statistical content analysis in data loss prevention to classify corporate documents, recognize complex patterns, and identify modified documents, respectively (Alneyadi et al., 2016).

### **2.5.5 Data Security in Drug Manufacturing: Gaps in Empirical Literature**

Despite the increasing digitalization of pharmaceutical manufacturing, there remains a critical lack of empirical research that evaluates the alignment between current data management guidelines and data security principles; investigates how well the organizational practices of Nigerian pharmaceutical firms adhere to established data security best practices; and examines the protection of business-critical data, such as R&D information and drug formulas, beyond the narrow focus of personal data protection frameworks. While several



global and regional guidelines emphasize data protection (e.g., FDA, 2018; MHRA, 2015; PIC/S, 2021; WHO, 2016; 2021), relatively few empirical studies have critically assessed their implementation within the pharmaceutical sector. For instance, Leal et al. (2021) evaluated how Novartis applied data process mapping to identify vulnerabilities in manual data entry and storage, which led to improved procedural and technological controls. However, this case focused primarily on internal corporate mechanisms without examining the broader regulatory ecosystem or alignment with national policy frameworks.

In the Nigerian context, existing literature on data security primarily focuses on compliance with personal data protection regulations, such as the NDPR. For instance, Adeoti (2023), Akinwunmi (2024), and Babalola (2022) provide important analyses of Nigeria's data protection frameworks, particularly the NDPR and the 2023 Data Protection Act, with an emphasis on personal data rights and regulatory obligations. Similarly, Chika and Tochukwu (2020) examine general compliance practices, while Olukoya (2022) investigates legal and technical mechanisms for eliciting privacy and security requirements from regulatory texts. However, none of these sources address the protection of business-critical data, such as IP, proprietary R&D, or drug formulation data, which are central to the pharmaceutical sector. Other studies take a broader view of cybersecurity threats but lack pharmaceutical specificity. For example, Ikusika (2023) documented increasing cyberattacks on Nigerian firms but did not address vulnerabilities unique to pharmaceutical IP. Aguboshim and Ezeasomba (2022) acknowledged the gap between data security and IP protection but stopped short of offering a sector-specific framework. Similarly, while Imasuen (2021) and Waziri (2020) critique weak IP enforcement in Nigeria, they did not explore how this weakness interacts with pharmaceutical data protection challenges.

While recent global studies discussed the consequences of high-profile pharmaceutical data breaches, they overlooked core sector-specific vulnerabilities. Chopra (2021), for instance,

emphasizes legal disputes and insurance claims stemming from cyberattacks, with limited focus on preventive or operational measures. Similarly, Crosignani et al. (2023) analyze supply chain risks but neglect the unique demands of pharmaceutical manufacturing and the constraints faced in low-resource settings such as Nigeria.

Moreover, there is a notable absence of comparative studies examining whether actual data security practices in pharmaceutical companies align with regulatory standards. Without such analyses, it remains unclear whether data breaches stem from weak enforcement mechanisms, organizational shortcomings, or inherent limitations within existing guidelines. These gaps suggest that current academic and regulatory discourse may be overlooking the contextual realities and sector-specific risks facing pharmaceutical data systems in low- and middle-income countries.

This study contributes to bridging these gaps by offering an analysis of data management guidelines and actual practices within Nigeria's pharmaceutical manufacturing sector. It extends beyond personal data protection to empirically examine the handling of business-critical data, such as proprietary formulations and R&D information, while also assessing the contextual challenges that hinder the effective implementation of these guidelines and data security best practices. The findings would address sector-specific vulnerabilities and the infrastructural, regulatory, and operational realities of low- and middle-income contexts like Nigeria.

## **2.6 Nigeria's Pharmaceutical Industry**

Nigeria's pharmaceutical sector is a multi-billion-dollar industry with underutilized potential that could contribute more to the country's economy and enhance citizens' quality of life. In addition to having one of West Africa's fastest-growing and most promising pharmaceutical markets, Nigeria produces approximately 60% of the drugs in the West Africa sub-region, highlighting the immense sub-regional market (Isola & Mesagan,

2016). The pharmaceutical and healthcare industry is one of the most dynamic sectors in the country's economy, with a growth rate estimated at 7-9% (Eze, 2019). This industry is categorized under both the health sector and the industrial and manufacturing sectors, which are vital components of Nigeria's information infrastructure (Federal Republic of Nigeria, 2021).

### **2.6.1 Characteristics**

The Nigerian pharmaceutical industry can be described as highly regulated and fragmented, with limited capacity utilization. Although there is a low entry barrier, mergers and acquisitions are common. Additionally, industry growth is supported by various government policies.

**Industry Regulation.** Three health authorities regulate the Nigerian pharmaceutical industry, as shown in Figure 28: the Pharmacists Council of Nigeria, the Pharmaceutical Manufacturing Group of the Manufacturers Association of Nigeria, and NAFDAC (Obukohwo et al., 2018). The Pharmacists Council of Nigeria and NAFDAC operate under the Federal Ministry of Health, while PMG-MAN provides self-regulation that adds value for its members.

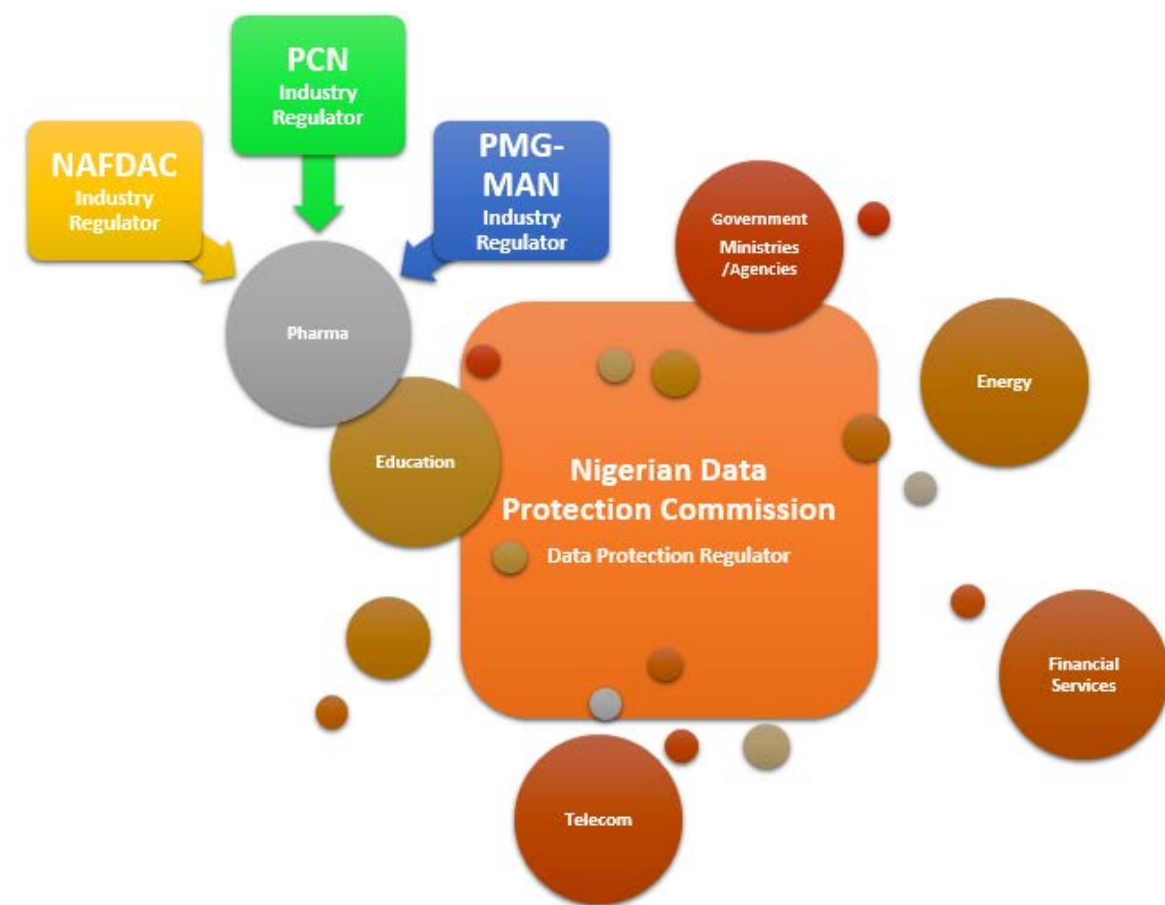
**Pharmacist Council of Nigeria.** The Pharmacists Council of Nigeria (PCN) is an agency of the federal government that primarily regulates the profession of pharmacists. According to Oseni (2019), the key oversight functions of PCN include standardizing premises and training pharmacists. PCN also develops a curriculum for degree programs and mandatory continuing education (Education and Training, n.d.). Additionally, it regulates all establishments where the pharmacy profession is practiced, including manufacturing facilities, retail points of sale, and drug warehouses (Pharmacy practice, n.d.).

**Pharmaceutical Manufacturing Group of Manufacturers Association of Nigeria.** The Pharmaceutical Manufacturing Group of the Manufacturers Association of Nigeria (PMG-MAN) is a part of the Manufacturers Association of Nigeria (MAN). PMG-MAN serves as the

umbrella organization for Nigerian manufacturers of medicinal and related products (Fadare et al., 2018). PMG-MAN focuses on enhancing Nigeria's pharmaceutical manufacturing standards (WHO, 2014) by supporting the production of high-quality finished medical goods and raw materials through GMP (About PMG-MAN, n. d.). Consequently, PMG-MAN facilitates access to safe and high-quality medicines for Nigerians. PMG-MAN also promotes and influences health and drug policy in several relevant areas, including regulatory, commerce, and other policy domains (About PMG-MAN, n. d.).

**Figure 27**

*Regulatory Framework of Nigeria's Pharmaceutical Industry and Data*



**National Agency for Food and Drug Administration and Control.** The primary regulatory authority for Nigeria's pharmaceutical industry is NAFDAC. Before NAFDAC was established, the Directorate of Food and Drug Administration and Control (FDAC), a division

of the Federal Ministry of Health, encountered significant limitations due to inadequate legislation aimed at curbing the production and distribution of counterfeit drugs, an almost non-existent product registration process, and other bureaucratic hurdles (Nwosu, 2023a). NAFDAC replaced the former FDAC, which was widely regarded as ineffective and a failed institution. Nwosu (2023a) attributed this failure to the broader deterioration of Nigeria's social and economic systems, emphasizing how corruption and inefficiency—manifestations of moral and cultural decline—compromised the performance of critical agencies like FDAC.

NAFDAC is the National Regulatory Authority (NRA) established under Nigeria's health and safety law to regulate and monitor the distribution of illicit and counterfeit food and drug products. Founded by Decree No. 15 in 1993 and later amended by Decree No. 19 in 1999, it is currently governed by the National Agency for Food and Drug Administration and Control Act, Cap N1 of the Laws of the Federation of Nigeria (LFN) 2004 (Olasupo et al., 2024). It officially became a parastatal under the Federal Ministry of Health on January 1, 1994 (Nwosu, 2023a). The law requires NAFDAC to regulate and control the importation, production, exportation, distribution, advertisement, sale, and use of food, drugs, medical devices, packaged water, cosmetics, detergents, and chemicals, collectively known as regulated products (Nwosu, 2023a; Oguejiofor et al., 2023). NAFDAC achieves this oversight by implementing its quality assurance system, promoting public awareness, and utilizing its inspectorate to enforce its initiatives (Nwosu, 2023a). Additionally, NAFDAC inspects and certifies plants worldwide regarding GMP before registering or renewing products from those factories (Drugs & medical devices, n. d.; Notes to industry, n. d.). NAFDAC applies established guidelines for setting up pharmaceutical plants in Nigeria within its regulatory framework. The agency is also mandated to establish regulations, standard specifications, and guidelines for manufacturing food, drugs, and related products, as well as to conduct inspections and ensure the registration of foods, drugs, and chemicals (Aibieyi & Eke, 2022).

NAFDAC's stringent regulations aim to safeguard public health by ensuring the safety and efficacy of healthcare products (Nwosu, 2023a; Oguejiofor et al., 2023). However, the laws that established NAFDAC are inadequate for the agency to fulfill its regulatory duties effectively. For instance, unlike other NRAs, NAFDAC did not establish specific standards or provide guidelines on data management or security for Nigeria's pharmaceutical industry. According to Nwosu (2023a), one of the significant issues facing many government organizations in Nigeria is the absence of strong enabling legislation and structural flaws. Government organizations derive their authority from the laws that establish them, and when these enabling laws are deficient, the organizations become ineffective, ultimately leading to their decline. Former President Obasanjo was dissatisfied with NAFDAC's performance, prompting him to disband the agency and inaugurate a new one under the leadership of Dora Akunyili (Aibieyi & Eke, 2022). Akunyili (2004) argues that among the major challenges, corruption poses a significant obstacle to effective regulatory and control mechanisms, undermining efforts to combat drug counterfeiting. Even with the amendments and significant reductions in the production and distribution of counterfeit goods and consumables that Akunyili's leadership brought (Igbokwe-Ibeto, 2015), several pitfalls in drug regulation persist. According to Aibieyi and Eke (2022), NAFDAC struggles with regulating importation, investigating production, and controlling the ongoing proliferation of counterfeit drugs, which Akunyili refers to as a form of terrorism against public health and an act of economic sabotage (Nwosu, 2023a). NAFDAC also faces security challenges. Aibieyi and Eke (2022) notes that drug counterfeiters, after unsuccessful negotiations, resorted to harassment, intimidation, physical attacks, and organized arson targeting NAFDAC staff and facilities across the country. In addition to the general lack of infrastructure in Nigeria's healthcare sector (Oguejiofor et al., 2023), Aibieyi and Eke (2022) highlights that the weakest point in the country's drug regulation lies in the implementation and enforcement.

However, the agency has made some groundbreaking advancements. NAFDAC primarily relied on manual procedures and paperwork, using outdated tools and operating with limited resources. These traditional methods were time-consuming, inefficient, lacked transparency, and were unreliable in handling regulatory duties' increasing complexity (Olasupo et al., 2024). Consequently, the agency decided to implement technological solutions by digitizing and automating its regulatory processes. Digitization enabled the agency to streamline several regulatory functions: online submission of applications for regulatory services, port clearance, electronic processing and approval of marketing authorizations, post-market surveillance, submission and review of Common Technical Document (CTD) dossiers for human drug registration, laboratory testing, clinical trial reviews, vigilance, and control (Olasupo et al., 2024). Additionally, digital technologies transformed NAFDAC's interactions with clients and stakeholders. The implementation of technological tools yielded positive impacts: improved efficiency by reducing human errors and preventing unnecessary delays; enhanced resource management; promoted regulatory efficiency; addressed counterfeit and substandard products; improved access to regulatory information; fostered transparency and accountability; and supported collaboration and capacity building (Olasupo et al., 2024).

Adopting and implementing digital innovation and automation in its regulatory processes marked a significant milestone for the agency, allowing it to perform its regulatory responsibilities and manage workloads more efficiently and effectively. Digitization also played a crucial role in the agency's Quality Management System (QMS), supporting ISO certification for certain regulatory processes (Olasupo et al., 2024). The transition to digital processes for various regulatory functions was also essential to the agency's achievement of international recognition as a WHO Global Benchmarked Maturity Level 3 (WHO-GBT ML3) NRA in Sub-Saharan Africa (NAFDAC, 2022). In addition, the agency's digitization strategies enabled it to qualify as a WHO-prequalified laboratory (WHO Global Benchmarking & Quality

Management Program, n.d.). The adoption of technological tools also significantly improved the agency's reputation among other NRAs worldwide.

This digital transformation enhances effectiveness, efficiency, and transparency, strengthening NAFDAC as a regulatory authority. While the digitalization of regulatory processes offers many benefits, it also presents several challenges. Olasupo et al. (2024) highlighted the issues that regulatory authorities encounter due to digitalization: resource constraints, technological infrastructure and connectivity, capacity building and knowledge gaps, interoperability and standardization, and concerns over data security and privacy. In particular, protecting sensitive regulatory data from cyber threats, unauthorized access, and breaches is a significant issue that demands robust data security measures. Moreover, strong regulatory oversight in Nigeria's pharmaceutical sector is essential for safeguarding both personal and drug manufacturing data. Ensuring the security of drug manufacturing data requires collaboration with relevant government agencies, including NITDA and NDPC. However, inadequate cooperation among government agencies makes the enforcement of regulations ineffective (Nwosu, 2023a).

**Data Protection Regulation.** In Nigeria, data protection is based on the constitutional right to privacy as established in Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended). The responsibility for data protection in Nigeria is divided among three government agencies: The National Information Technology Development Agency (NITDA), the Nigeria Data Protection Bureau (NDPB), and NDPC. NITDA, created under the National Information Technology Development Agency Act of 2007, was authorized to publish NDPR on January 28, 2019 (Chika & Tochukwu, 2020). The NDPR is modeled after the GDPR in some respects and draws inspiration from it. Chika and Tochukwu (2020) regard the NDPR as a deviation, as it modifies some clauses of the GDPR to fit Nigeria's economic context. Olukoya (2022) asserts that the NDPR mirrors the GDPR by outlining governing principles for



data processing, the necessity of consent for collecting and processing data, the rights of data subjects, conditions for international personal data transfers, penalties for non-compliance, and mechanisms for implementation, including an administrative redress panel, among other provisions. However, NDPR distinguishes itself by establishing enforcement agents called Data Protection Compliance Organizations (DPCOs), which are licensed by NITDA to help ensure adherence to the NDPR (Babalola, 2022). NDPR serves as the primary regulation for data protection, aimed at safeguarding the personal data of both Nigerians and non-Nigerian residents within the country. It imposes data protection responsibilities on organizations (Oguejiofor et al., 2023). In addition to NDPR, NITDA has released further guidelines and resources to assist organizations in achieving compliance: Frequently Asked Questions; Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020; Implementation Framework; Audit Template for NDPR Compliance; and the List of Licensed DPCOs (Akinwunmi, 2024; Regulations, n. d.). Babalola (2022) argues that the regulation encounters several issues: the mixing of American and European data privacy concepts with data protection; confusion between personal data and PII; exclusion of legitimate interest as a legal justification for data processing; an unclear distinction between the roles of data administrators and data processors; the lack of explicit enforcement guidelines concerning the extraterritorial scope of the regulation; the adoption of a licensing framework for DPCOs instead of the preferred 'accreditation,' raising concerns about legitimacy; acknowledgment of multiple data protection authorities; and uncertainty regarding NITDA's authority to oversee data protection. Although it was enforceable, the NDPR remained subordinate legislation, and no dedicated commission existed for data protection. NITDA had to broaden its responsibilities to include oversight of data protection.

In February 2022, the Nigerian government enacted an executive order aimed at providing interim support for oversight through the establishment of the NDPB (About, n.d.).

This order transferred data protection responsibilities, along with the existing regulations and guidelines from NITDA, to the NDPB. The NDPR remained an interim framework until the Nigeria Data Protection Act was passed. On June 12, 2023, the Nigeria Data Protection Act 2023 (NDPA) was enacted as the country's main legislation for data protection and has been effective since that date (Adeoti, 2023; Akinwunmi, 2024). NDPA outlines the obligations of the data processor, the steps organizations must take in the event of a data breach, the data controller's duty to notify affected data subjects, the requirement for the data controller to maintain records of data breach occurrences, and the obligation of the data controller to report these breaches (NDPA, 2023). Additionally, certain provisions of the act require clarification to help stakeholders fulfill their obligations and protect their rights. Adeoti (2023) noted that the use of vague and open-ended phrases makes it challenging for a data processor or controller to determine whether it is a controller or processor of major importance, complicating timely compliance with the Act. Nonetheless, the introduction of the NDPA led to the establishment of the NDPC to address the 2022 issue and oversee data protection in Nigeria. According to the NDPA, the NDPB was incorporated into the NDPC (Adeoti, 2023). Furthermore, the NDPR, along with the data protection regulations or circulars issued by NITDA or NDPB, remain relevant for data protection in Nigeria and are now considered regulations issued by the NDPC (NDPA, 2023, § 64). Thus, the NDPR functions alongside the NDPA. However, the NDPA takes precedence in cases with conflicting provisions in the NDPR (NDPA, 2023, § 63). The NDPC is currently the primary supervisory and regulatory body for data protection in Nigeria.

The NDPC is responsible for overseeing the implementation of the NDPA and matters related to data protection in Nigeria (FAQ-NDPC, n.d.). The NDPC is authorized to issue regulations, investigate suspected breaches of the NDPA, and impose fines for its violations (NDPA, 2023, § 6). The Commission is empowered to register data controllers and processors

of significant importance, accredit and license qualified individuals as DPCOs, address complaints regarding NDPA violations, and impose sanctions on those who breach its provisions (Adeoti, 2023). However, the NDPC faces some limitations. Notably, the commission cannot mandate reporting or investigate alleged data breaches involving non-personal data. Reporting obligations for data controllers are limited to breaches involving personal data. Nonetheless, a breach of valuable IP, such as drug formulas, research and development data, and other manufacturing data, threatens pharmaceutical companies' financial stability and may disrupt critical health, manufacturing, and industry infrastructure.

Furthermore, like some Nigerian government agencies, the lack of independence undermines the NDPC's ability to operate objectively and effectively. Adeoti (2023) expressed concerns about the commission's independence, highlighting that the composition of the governing council heavily relies on the executive branch of government, as the appointment and removal of council members are at the president's discretion. Political or external pressures can lead to compromised decision-making. This dependence erodes public trust and diminishes the NDPC's authority and credibility, as the agency may be perceived as serving political interests instead of the public interest.

Beyond the shortcomings of Nigeria's data privacy legislation, a major issue arises from the government's capacity to adhere to data protection regulations, as many agencies and parastatals have been known to violate the law. Regrettably, both government agencies and private companies have consistently failed to comply with these regulations through their actions, leading to significant embarrassment and challenges for individuals and corporations alike. Chika and Tochukwu (2020) contend that Nigeria does not have adequate regulations and policies to prevent improper data sharing and breaches. They further highlight the lack of enforcement efforts that lead to privacy violations in Nigeria. This situation underscores the

urgent need for stronger regulations and more effective enforcement mechanisms to safeguard sensitive data in Nigeria.

**Low Entry Barrier.** Nigeria's pharmaceutical industry has a low entry barrier. With as little as N1 million, a pharmaceutical company can be established to import medicines, provided that the registration requirements of NAFDAC and the Companies and Allied Matters Act are met (Ojo, 2014). Consequently, barriers to entry into the industry are relatively low (Obukohwo et al., 2018), especially in the area of import or distribution compared to other manufacturing segments.

**Highly Fragmented, Low-capacity Utilization.** Given its low entry barrier, Nigeria's pharmaceutical industry is highly fragmented. This sector is recognized for its complexity, as it involves many actors throughout the value chain—importers, manufacturers, distributors, national regulators, wholesalers, retailers, government ministries, non-governmental associations, and other stakeholders. Furthermore, the line between importers and manufacturers is not usually clear-cut since most manufacturers also import and act solely as marketers or distributors of branded medicinal products. Among these industry players, Obukohwo et al. (2018) identified twenty pharmaceutical companies listed on the Nigeria Stock Exchange between 2012 and 2016:

Afrab Chem. Limited, Archy Pharma Nigeria Ltd., Drug Field Pharmaceuticals Ltd, Ecomed Pharma Ltd., Emzor Pharmaceutical Industries Ltd, Evans Medical Plc, Fidson Healthcare Plc, Gemini Pharmaceuticals Nig. Ltd., GlaxoSmithKline Nigeria, Juhel Pharma., Enugu, May & Baker Nigeria Plc, Mopson Pharmaceutical Industries Ltd, Neimeth International Pharmaceuticals, Nigerian-German Chemicals Plc, PZ Cussons Plc, Ranbaxy Nig. Ltd., Lagos, SKG Pharma Plc., Lagos, Swipha Nigeria Ltd, Swiss Pharma Nig. Ltd, Lagos, and Vitabiotics Nigeria Ltd (pp. 138-139)

Nine of these listed companies export their products to various ECOWAS countries, specifically, “Drug Field Pharmaceuticals Ltd, Emzor Pharmaceutical Industries Ltd, Evans Medical Plc, Fidson Healthcare Plc, GlaxoSmithKline Nigeria, May & Baker Nigeria Plc, Mopson Pharmaceutical Industries Ltd, Neimeth International Pharmaceuticals and PZ Cussons Plc” (p. 132).

Furthermore, there are about 130 local drug manufacturers in Nigeria, representing roughly one-third of the total pharmaceutical manufacturing capacity in the West Africa sub-region (Adigwe, 2023). However, only a few local drug manufacturers operate at optimal capacity utilization. Industrial capacity utilization is below 30%, with approximately 70% of the pharmaceuticals consumed in Nigeria being imported (Adigwe, 2023).

**Mergers and Acquisitions.** Mergers and acquisitions characterize Nigeria's pharmaceutical industry and reflect its global standing. According to the WHO, Nigeria's health sector was ranked 187th out of 191 based on the manufacturing and storage capabilities for pharmaceuticals (Obukohwo et al., 2018). Consequently, only a limited number of Nigerian pharmaceutical companies can participate in international tenders for supplying essential medicines for major diseases like tuberculosis, malaria, and HIV/AIDS. Multinational brands clearly dominate the market due to their capitalization, global strategic partnerships, earning capacity, and established track records. While the global context presents a situation where the sector's growth rate outpaces the economy at 6.1% (Eze, 2019), growth opportunities are confined to certain key stakeholders within the industry. In the long term, marginal players will exit or be acquired by major players as it becomes increasingly challenging to remain competitive at a smaller scale.

**Government Interventions for Sustained Industry Growth.** One of the biggest obstacles to the growth of the Nigerian pharmaceutical industry is the saturation of lower-cost imported drugs in the marketplace. Local manufacturers struggle to compete effectively

with these imports, as they bear the costs of importing raw materials in addition to the high expenses of operating a local manufacturing facility. Furthermore, local manufacturers must pay value-added tax on imported raw materials, which is not applied to imported drugs (Ojo, 2014). To address these challenges, the Ministry of Finance implemented certain measures to help local manufacturing companies stay competitive. In this regard, the Ministry of Health banned the import of eighteen essential drugs in 2005 after evaluating the local manufacturing capacity for these drugs along with PMG-MAN (Ojo, 2014). According to Ogaji et al. (2014), the federal government included these essential medicines, which can be produced by the local manufacturing industry, on the import ban list to promote local production and enhance the sector's capacity utilization. Additionally, the Ministry of Health proposed plans to revise the tariffs on imported raw materials needed for drug production due to the 5% to 15% customs duty imposed by the ECOWAS Common External Tariffs (CET) (CardinalStone, 2017). In addition, the federal government made locally produced products more appealing by imposing a 20% import duty on finished pharmaceuticals (Fagbolu & Nnebue, 2019). The adjustments in tariffs and increases on imported raw materials and finished pharmaceuticals enable drug manufacturers to produce at a lower cost, enhance gross margins, stimulate growth, and sustain investment. Despite these governmental initiatives, many of Nigeria's pharmaceutical companies and healthcare providers struggle to compete adequately, except for a few internationally recognized brands (Eze, 2019).

### **2.6.2 Challenges and Trends**

Nigeria's pharmaceutical industry has faced numerous challenges and developments. Significant obstacles include poor infrastructure, weak regulatory systems, and disruptions, while trends such as WHO prequalification and advancements in science and technology have influenced industry performance. These challenges and trends contribute directly or indirectly to data security challenges and substandard and falsified medicinal products.

**Substandard and Falsified Medicinal Products.** WHO defines substandard medical products as “authorized medical products that fail to meet either their quality standards or specifications, or both” while falsified medical products “deliberately/fraudulently misrepresent their identity, composition or source” (Substandard and falsified medical products, 2018). Counterfeit medicinal products pose a significant challenge to Nigeria's pharmaceutical supply chains. A disconcerting aspect of the risk of drug counterfeiting is that the effects of drug use often go unnoticed unless they result in mass fatalities. In November 2008, 34 Nigerian children aged between 4 months and 3 years died, and over 50 were hospitalized for serious kidney damage following the administration of a dentition mixture containing paracetamol (Amadi & Amadi, 2014). According to Akinyadenu (2013), the outbreak resulted from the use of diethylene glycol (DEG) as a solvent for paracetamol instead of propylene glycol. The less toxic propylene glycol, which is commonly used in the pharmaceutical industry, may have been deliberately substituted with DEG. This event is analogous to a scenario created by Urciuoli et al. (2013). In one instance, Urciuoli et al. (2013) outlined the threat of employing malicious software to compromise a drug manufacturing company's industrial machinery. Specifically, hackers could use malware to gather information on the ingredients used to produce a specific drug and the quality checks conducted in the pharmaceutical supply chain's production, warehousing, and distribution facilities. After months of data gathering, malicious hackers collaborating with a terrorist group and corrupt pharmaceutical experts could target the supply chain by altering the ingredient mixture and producing a lethal drug. Assuming that thresholds and quality control mechanisms are stored electronically, hackers could alter the detection mechanisms used to alert inspectors. Deadly drugs could then be distributed within a few months, leading to a surge in fatalities that will persist until health authorities identify the source and remove all hazardous products from the market.

While acknowledging the significant progress made by the Ministry of Health through NAFDAC in tackling the issue of drug counterfeiting, it remains a serious threat to local drug manufacturers. Statistically, between 13 and 35 percent of global sales of fake and counterfeit medicines primarily come from India, Pakistan, and Nigeria (Aigbavboa & Mbohwa, 2020). Although the issue of substandard and falsified medicinal products can represent an illicit case of IP theft, it is fundamentally a public health crisis.

**Weak Regulatory Systems.** Nigeria's pharmaceutical industry may not be regulated as effectively as it should be. Giralt et al. (2017) observed that up to 90 percent of national Sub-Saharan African drug regulators are unable to effectively perform their core regulatory functions. In Nigeria's pharmaceutical sector, failures ranging from policy development to the implementation of existing laws, as discussed in previous sections, create opportunities for IP theft, drug counterfeiting, and personal financial gain. Moreover, the strictest standards and requirements imposed by NAFDAC are based on the processes involved in handling drugs from production to patient delivery (Aigbavboa & Mbohwa, 2020). It is therefore unsurprising that data security was not included in NAFDAC's approved strategic plans for Nigeria's pharmaceutical industry (NAFDAC Strategic Plan (2018–2023), n.d.).

Considering data protection, the scope of the NDPR applies only to transactions meant to ensure the privacy and processing of personal data of Nigerian citizens, which may suggest that NITDA had equated data privacy with data protection, as illustrated in Table 6. According to Brunswick (2019), "Data protection is the practice or process of safeguarding information from corruption and loss.... Data privacy (or information privacy) is related to organizations' processing rules and practices and regulates controllers and processors from using data in a wrongful manner" (p.14). Data protection involves safeguarding data from unauthorized access, while data privacy addresses what occurs with those who have authorized access. Furthermore, data protection typically emphasizes securing information and may include



security policies, secure communication protocols, and encryption. Data privacy can be regarded as a legal issue that focuses on how PII is collected, used, and stored. Therefore, data protection prioritizes security, whereas data privacy is mainly concerned with the regulation and usage of personal information.

**Table 7**

*Distinction between Data Protection and Data Privacy*

Aspect	Data Protection	Data Privacy
Definition	Practice or process of safeguarding information from corruption and loss (Brunswick, 2019).	Related to organizations' processing rules and practices; regulates controllers and processors from using data wrongfully (Brunswick, 2019).
Focus	Safeguarding data from unauthorized access.	Governing what happens with those who have authorized access.
Emphasis	Security measures such as policies, secure communication protocols, and encryption.	Legal and regulatory aspects of how PII is collected, used, and stored.
Primary Concern	Prioritizes the security of information.	Concerned with the regulation and usage of personal information.

Consequently, NITDA's NDPR and NAFDAC failed to adequately address data protection—or, more accurately, data security—in the pharmaceutical context. Likewise, the more recent NDPC's NDPA also failed to resolve this oversight. The absence of robust data security standards for drug manufacturing presents a significant challenge and contributes to the persistent problem of poor medicine quality in drug supply chains.

**Scientific and Technological Advancement.** Globally, pharmaceutical companies are increasingly pressured by scientific advancements in the life sciences to innovate technologically. In addition to challenges related to new drug development, the technological advancements of the past decade have compelled Nigerian pharmaceutical companies to adjust certain aspects of their business operations, such as drug distribution. As Ojo (2014) notes, local drug manufacturers in Nigeria distribute through central medical stores under federal or state health ministries, mega distributors, or private logistics and courier services. Some also rely on their distributor networks to reach wholesalers, retailers, and hospitals. Distribution occasionally extends to unregistered outlets, particularly outside formal supply chains.

However, pharmaceutical supply chains encounter several challenges that negatively affect their performance. A significant issue is the distribution of drugs, which is often cumbersome and involves various stakeholders across the value chain. According to Aigbavboa and Mbohwa (2020), pharmaceutical supply chains in Nigeria and many sub-Saharan African countries face struggles that lead to stock-outs and the unavailability of certain essential drugs in healthcare institutions. The bottlenecks surrounding drug distribution have led some Nigerian pharmaceutical organizations to implement ERP solutions. ERP systems are known to enhance supply chain performance (Forslund, 2010) by establishing electronic links and relationships with other players in the supply chain. Information systems and technologies such as ERP solutions offer various applications in supply chain management: material requirement planning, demand forecasting, inventory management, production planning and control, production order management, customer and supplier relationship management, and logistics planning (Urciuoli et al., 2013).

Pharmaceutical organizations that actively adopt and integrate modern technologies into their operations are better equipped to manage supply chain disruptions. While traditional supply chain risk management has emphasized physical security, the accelerated use of digital technologies and interconnected systems has introduced a new wave of cyber threats that are both increasingly prevalent and complex. According to Massacci and Pashchenko (2021) and Pashchenko et al. (2018), a large number of companies unknowingly rely on open-source libraries that contain known security flaws. Although open source is valued for its community-driven development, its widespread adoption has created significant security challenges. Given this vulnerability, the information layer of supply chains presents an attractive target for cybercriminals and malicious actors engaging in theft, sabotage, fraud, counterfeiting, or espionage. A breach within an organization's third-party ecosystem can expose sensitive data, potentially enabling the manipulation or reproduction of pharmaceutical products and

disrupting not only the organization but also the broader industry or economy (Urciuoli et al., 2013).

**Poor Infrastructure.** Reliable electrical power is a basic requirement for the appropriate handling of medications. In Nigeria's pharmaceutical sector, stable and sufficient electricity is crucial throughout the entire process, from production to delivery to consumers in the outbound value chain. However, electricity poses a significant challenge for local pharmaceutical companies. Nigeria, like many other countries in sub-Saharan Africa, continues to face issues with consistent and adequate energy supplies. With a national power capacity of 5,000 megawatts for its population of 180 million, Nigeria experiences a considerable shortfall that negatively impacts the energy-dependent pharmaceutical sector (Aigbavboa & Mbohwa, 2020). As a result, Nigerian drug manufacturers rely on both public and in-house generated energy sources. However, the energy supply from Nigeria's power holding company accounts for between 4 to 64 percent of the annual energy needs of drug manufacturers and is considered less expensive than alternative sources (Ogaji et al., 2014). This situation is particularly concerning in pharmaceutical supply chains, where a continuous and reliable electricity supply is essential for preserving the efficacy and storage of vaccines, antibiotics, and other temperature-sensitive products. The lack of a consistent energy source also negatively impacts the availability of information processing facilities and resources for local drug manufacturers.

**Supply Chain Disruptions.** Supply chains face disruptions from a variety of sources, factors, and risks that can affect the performance of their different components. Some of these risks involve disturbances that obstruct the movement of products and result in failures within the supply chain, while others stem from the actions of cybercriminals. Nigeria's pharmaceutical supply chain has been severely impacted by significant issues related to sectarianism, tribalism, religion, and an overall lack of effective governance. The security

threat posed by the Boko Haram insurgency in northeastern Nigeria has had a profoundly negative impact on the regional pharmaceutical supply chain, leading to the destruction of facilities and, in some cases, the loss of personnel (Aigbavboa & Mbohwa, 2020).

**World Health Organization Prequalification.** WHO prequalification is advantageous for pharmaceutical companies in the long run. The WHO prequalification medicines program enables the assessment of the quality, safety, and efficacy of medicines in close cooperation with experts from national regulatory authorities in various Member States (Ogaji et al., 2014). WHO prequalification contributes to improved manufacturing standards in low- and middle-income countries (LMIC) (FM'tHoen et al., 2014), such as Nigeria. Obtaining WHO prequalification enables local manufacturing companies to access international procurement opportunities from development partners that prohibit the procurement of products without WHO prequalification (Ogaji, 2014). Local manufacturers with a WHO prequalification certificate can participate in international tenders for pharmaceuticals. Moreover, WHO pre-qualification certification enhances access for local manufacturers to non-governmental organizations, as well as multilateral grants and funding. WHO pre-qualification may also create manufacturing opportunities for local producers, considering the industry's excess capacity, to attract international pharmaceutical companies seeking partnerships or arrangements to enter the Nigerian market. Consequently, WHO pre-qualification will help strengthen data security standards in Nigeria's pharmaceutical industry.

Some Nigerian drug manufacturers began the process of obtaining WHO cGMP and pre-qualification. Eleven pharmaceutical firms were initially involved in the WHO prequalification race, specifically, Afrab - Chem Limited, Chi Pharmaceuticals Limited, Daily Need Industries Limited, Drugfield Pharmaceuticals Limited, Emzor Pharmaceuticals Industries Limited, Evans Medical Plc, Juhel Nigeria Limited, Fidson Healthcare Plc, May and Baker Plc, Neimeth International Pharmaceuticals Plc, and Swiss Pharma Nigeria Limited,

(Ojo, 2014). Seven of the eleven companies were successful after an initial WHO audit. A second audit narrowed the list to five: Chi Pharmaceuticals Limited, Evans Medical Plc, Fidson Healthcare Plc, May & Baker Plc, and Swiss Pharma Nigeria Limited. These five firms successfully passed two subsequent verifications in the prequalification process. Unfortunately, there are currently no local drug companies in Nigeria listed on the WHO pre-qualified list (Adigwe, 2023).

## **2.7 Summary**

Chapter 2 provided a comprehensive review of data security in the pharmaceutical industry, integrating theoretical perspectives, regulatory standards, and practical challenges in drug manufacturing. The chapter was structured around the intersection of management theories, good manufacturing practices, data governance, and data security frameworks, showing how these elements jointly shaped secure and compliant pharmaceutical operations. The discussion opened with the theoretical and conceptual framework that anchored the study. MCT was adopted as a lens for understanding how organizations achieved strategic objectives through formal and informal control mechanisms. MCT emphasized diagnostic control systems, alignment of strategic goals with operational processes, and the use of structures, policies, and evaluation systems to ensure accountability. This perspective was combined with GMP, which served as internationally recognized standards ensuring that pharmaceutical products were consistently produced and controlled according to quality requirements. GMP, derived from PIC/S and WHO guidelines, underscored the importance of regulatory compliance, documentation, and risk management throughout the manufacturing process. By combining MCT and GMP, the chapter framed data security as not just a technical requirement but also a strategic control process essential for sustaining organizational integrity and public health. Building on this foundation, the chapter highlighted data governance and data integrity as critical components of GMP activities. Data governance referred to the systems and policies

that ensured data remained complete, consistent, and accurate across its life cycle. The chapter underscored the ALCOA+ principles—Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available—as the gold standard for data integrity in pharmaceutical operations. These principles were crucial in settings where automated systems generated heterogeneous datasets vulnerable to manipulation or error. Practical examples, including regulatory findings and industry case studies, illustrated how adherence to ALCOA+ prevented data breaches, maintained regulatory compliance, and protected patient safety.

The chapter then transitioned into a review of data classification and security considerations within pharmaceutical environments. It distinguished between traditional data (master, reference, transactional) and big data (generated by production equipment, IoT sensors, and operational systems). These data assets existed in three states—at rest, in motion, and in use—and faced threats such as unauthorized alteration, disclosure, and denial of use. The text provided concrete examples: IP theft, exposure of PII, and operational disruptions. Each threat was linked to significant business and regulatory risks, reinforcing the necessity of proactive security frameworks.

A significant portion of the chapter was dedicated to IT governance and management. It reviewed governance models—centralized, decentralized, and federal—while distinguishing IT governance (strategic direction, oversight) from IT management (day-to-day execution). EGIT was highlighted as a comprehensive framework, particularly through the COBIT model, which linked enterprise goals with IT-related objectives. COBIT's governance components were mapped to pharmaceutical contexts. Examples from industry leaders such as GSK demonstrated how these frameworks strengthened IT governance, mitigated risks, and aligned with management control principles.

The chapter then explored data life cycle management in manufacturing. From concept generation to recycling and disposal, each phase—design, procurement, production, transportation, sales, utilization, and after-sales service—generated critical datasets. These datasets had to be managed through creation, collection, processing, storage, usage, visualization, transmission, sharing, application, archiving, and destruction.

The chapter then examined data security governance and protective mechanisms. A multilayered strategy—spanning human, perimeter, network, endpoint, application, and data security—was recommended to defend mission-critical assets. Security models like the CIA Triad, Parkerian Hexad, and Five Pillars of Information Assurance were compared for their relevance in pharmaceutical settings. The role of CSCs was emphasized, noting their alignment with frameworks like NIST and ISO and their strength in mandating implementation rather than leaving controls optional. Moreover, DLP strategies, including technical solutions and procedural safeguards, were reviewed to address insider threats and prevent unauthorized exfiltration.

Finally, the chapter situated these global frameworks within Nigeria's pharmaceutical industry. It provided an overview of the regulatory environment, highlighting agencies such as NAFDAC, PCN, and PMG MAN and their roles in enforcing standards. Despite high regulatory aspirations, challenges persisted: fragmented markets, low capacity utilization, infrastructural deficiencies, and weak enforcement mechanisms. Substandard medicines and data breaches illustrated systemic vulnerabilities. Efforts toward WHO prequalification were presented as a critical step for Nigerian manufacturers to access global markets and align with international data security standards. Yet, the chapter noted that current regulations, such as NDPR and NDPA, inadequately addressed data security, creating gaps that exposed sensitive operational and patient data to significant risk.

In conclusion, Chapter 2 integrated theoretical insights and practical observations to demonstrate that effective data security in pharmaceuticals required more than isolated technical fixes. It required a holistic governance framework—anchored in MCT, enforced through GMP standards, operationalized via data governance and IT governance models, and contextualized within national regulatory landscapes. The synthesis of these elements highlighted a pressing need for stronger regulatory enforcement, enhanced industry best practices, and the adoption of advanced technological controls to safeguard data integrity and security. This comprehensive foundation set the stage for further analysis and solution development in subsequent chapters.



## **CHAPTER 3: RESEARCH METHODS AND DATA COLLECTION**

### **3.1 Introduction**

In recent years, there has been a notable increase in data breaches within the global pharmaceutical industry, despite the guidance provided by health authorities regarding effective data management. Studies indicate that the pharmaceutical sector incurs a higher total cost related to data breaches compared to less regulated industries. The widespread theft of data assets during the COVID-19 pandemic exposed the inadequacy of the existing safeguards. In particular, cybercrime in Nigeria is rapidly advancing, with a significant surge in sophisticated attacks targeting various sectors, including banking and pharmaceuticals. Millions of personal records and critical data have been compromised, placing the Nigerian pharmaceutical industry at severe risk due to stolen IP and patient information. The purpose of this study is to investigate data security gaps in the Nigerian pharmaceutical sector. Researchers have access to diverse research approaches. Nevertheless, research methods are generally classified into two main categories: quantitative and qualitative. These quantitative and qualitative paradigms are guided by philosophical underpinnings, and the specific nature of the research questions influences the perspective adopted for the study.

Chapter 3 underpins the entire research endeavor by outlining the research methods and data collection strategies. Rather than simply presenting isolated techniques, the chapter is laid out as a sequence of interrelated sections that build a clear picture of how the research was designed, executed, and justified. The chapter opens with an introduction (Section 3.1), which provides a roadmap for what follows. This introductory section orients the reader to the purpose of the chapter, highlighting that it explains the research approach, design, sampling, data collection, analysis, and ethical considerations. It sets the tone for a methodologically rigorous and transparent discussion. Following the introduction, the research approach and design (Section 3.2) lays the foundation for the entire research methodology. Within this section, the

research approach (Section 3.2.1) details the overarching qualitative strategy and philosophical stance, explaining why it was suitable for exploring the complex dynamics of data security. Next, the research design (Section 3.2.2) introduces the multiple case study design, explaining its capacity to capture context specific insights and justify the choice of case studies over other qualitative designs. Once the general approach and design are established, the chapter moves to the triangulation strategy (Section 3.3). This section explains why triangulation was central to the study, clarifying that multiple methods and sources were integrated to achieve credibility and richer insights. It shows how triangulation links different parts of the methodology into a coherent whole. After presenting the triangulation strategy, the triangulation methods for data collection (Section 3.4) outlines the specific techniques used to gather data. Document analysis is discussed first, showing how institutional and regulatory documents were examined to provide historical and contextual understanding. Interviews are then described, with a focus on how they complemented document analysis by generating firsthand data from key participants. Together, these subsections explain how different methods were combined in practice. The chapter then moves into the sampling design (Section 3.5), which describes how sources and participants were selected. The sampling strategy (Section 3.5.1) sets out the criteria and rationale for inclusion and exclusion, while the sample characteristics and size (Section 3.5.2) provides details of the sample itself. By placing these subsections here, the chapter ensures that readers understand both the logic behind sampling and the nature of the data pool before moving to data collection tools. The next major section, research tools (Section 3.6), explains the instruments developed for data gathering, with emphasis on the interview guide. This section is positioned after sampling because it builds directly on knowing who would be interviewed and how best to capture the required information. Ethical considerations are consolidated in the study procedure and ethical Assurances (Section 3.7). Ethical assurances (Section 3.7.1) describes how the study safeguarded participant rights, secured permissions,

and ensured scientific validity. Study procedures (Section 3.7.2) then outlines the step by step workflow, from literature review through to reporting, providing readers with a clear timeline and procedural context. Placing ethics and procedures together underscores how methodological steps were intertwined with ethical obligations. The chapter then transitions to data analysis methods (Section 3.8), which explains how collected data were examined and interpreted. Selected method (Section 3.8.1) details the chosen analytical approaches and why they fit the research questions. Excluded approaches (Section 3.8.2) demonstrates transparency by explaining why alternative methods were not adopted. Software for qualitative data analysis (Section 3.8.3) follows, describing how computer assisted qualitative data analysis software and tools like Microsoft Excel and Word were used to organize and code data. Grouping these subsections illustrates the layered nature of analysis, from theoretical decisions to practical tools. Building on the previous section, data collection and analysis (Section 3.9) gives a procedural breakdown of how the two main analytic techniques were applied. Qualitative content analysis (Section 3.9.1) describes the steps of decontextualization, recontextualization, categorization, and compilation as applied to documents. Thematic analysis (Section 3.9.2) explains how interview data were transcribed, coded, sorted, and thematically mapped. By placing this section after the methodological discussion, the chapter allows readers to see exactly how the chosen methods operated in practice. Finally, Chapter 3 closes with a summary, which revisits the key components of the research methods and data collection strategies. This concluding section reinforces how each preceding part—research approach, design, triangulation, sampling, tools, ethical safeguards, analytical techniques, and practical steps—fits into a coherent methodological framework. It signals a transition, preparing the reader to engage with the research findings presented in Chapter 4.

### **3.2 Research Approach and Design**

The research approach and design were tailored to explore complex data security issues within Nigeria's regulated pharmaceutical industry, requiring both rigor and adaptability to effectively capture and analyze data. The choice of research approach and design was driven by the study's objectives and research questions. By adopting a methodologically rigorous and context-sensitive design, this study provided a comprehensive understanding of data security issues in Nigeria's pharmaceutical industry.

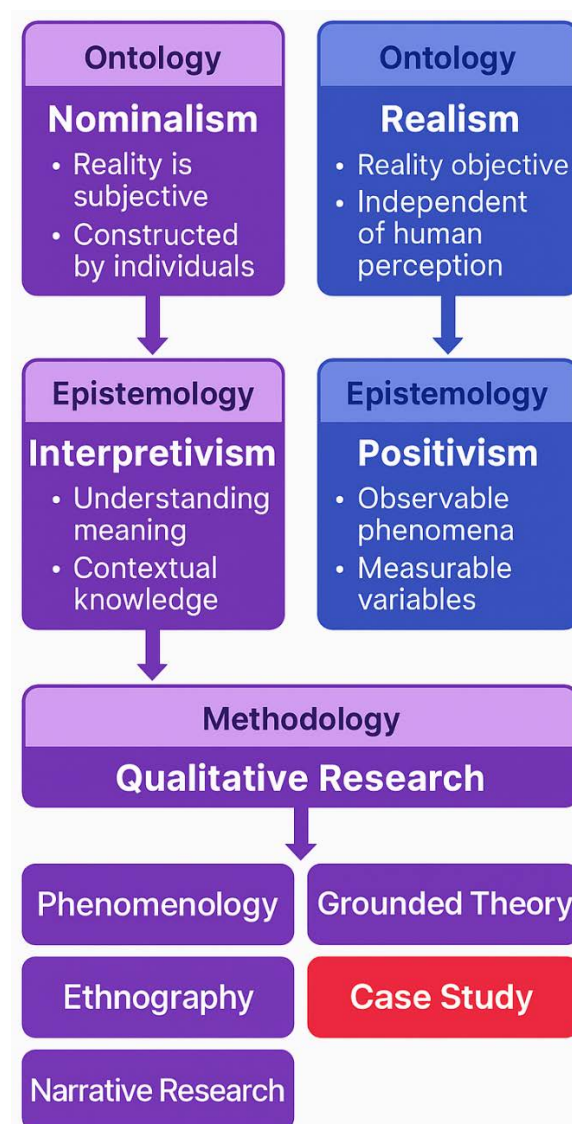
#### **3.2.1 Research Approach**

Given the research objectives and questions, an interpretivist stance guided by a nominalist ontological perspective was deemed the most appropriate research philosophy for the study, as shown in Figure 28. This choice aligned with the methodological implications identified by Easterby-Smith et al. (2015) regarding various ontologies and epistemologies. Interpretivism emphasizes how individuals assign meaning to their surroundings, particularly through sharing their experiences with others via language (Sprake & Palmer, 2022; Topping, 2015). This position forms the foundation of qualitative research that employs an interpretative and naturalistic methodology. This methodology highlights the absence of a single truth, meaning, or interpretation while acknowledging cultural and societal differences in which individuals reside (Sprake & Palmer, 2022; Topping, 2015). Since qualitative research aligns seamlessly with interpretative assumptions, qualitative methods were utilized. Moreover, as outlined in the problem statement and literature review, research on this topic remains relatively limited. Given the substantial gap in both empirical and conceptual literature, a qualitative research approach was deemed appropriate to enable in-depth exploration and generate context-specific insights. Since qualitative research emphasizes exploration and theory development, the study did not require a specific hypothesis or predetermined expectations regarding the results (Sprake & Palmer, 2022). Qualitative methods are

particularly suitable for addressing research questions about “experience, meaning, and perspective” (Hammarberg et al., 2016, p. 499). Additionally, the sensitivity of qualitative research to contextual factors makes its approaches effective in gathering specific information about the phenomenon.

**Figure 28**

*Research Philosophy and Approach*



**Note:** The research approach – case study- was determined by the author based on ontological, epistemological (Easterby-Smith et al., 2015), and methodological considerations (Gerrish & Lathlean, 2015; Creswell & Poth, 2018).

A quantitative research approach was not used because the study was not intended to measure the phenomenon empirically. Quantitative research employs positivist methodologies for explaining, predicting, and controlling phenomena. According to Guba and Lincoln (1994), a positivistic methodology is experimental, manipulative, and focused on verifying questions and hypotheses. This study did not hypothesize or attempt to obtain data to confirm, reject, or select hypotheses. The study neither tested hypotheses empirically nor investigated patterns and causal relationships.

Qualitative research approaches concentrate on exploring human experiences, aiming to capture detailed insights that extend beyond numbers and statistics. Gerrish and Lathlean (2015) identified the primary methods for qualitative research, namely grounded theory, ethnography, phenomenology, and narrative research. However, these approaches were unsuitable for the current study, given their limitations and the research questions.

Grounded theory was not regarded as a valid research approach because the study did not focus on the systematic development of a theory from the data. Additionally, it was not intended to alter or extend theories based on data collection and analysis. According to Holloway and Galvin (2015b) and Tarozzi (2020), grounded theory presupposes that no hypothesis or theoretical framework exists prior to data collection. Furthermore, Holloway and Galvin (2015b) argue that prior assumptions should be set aside to avoid adhering to a particular preconceived idea or direction. This position involves discarding theoretical thoughts to allow the emergence of the underlying analytic theory. However, this study proposed a theoretical framework that served as a valuable source of knowledge.

Ethnographic research in many organizations can be challenging due to access restrictions. Easterby-Smith et al. (2015) highlight limitations stemming from constraints imposed by organizations. Furthermore, building relationships and gaining entry often require time and commitment (Holloway & Galvin, 2015a). Easterby-Smith et al. (2015) also pointed

out the potential for researchers to influence their informants. Moreover, there is a risk that participants may simply say what they think researchers want to hear. While cultural immersion and the relationship between the researcher and informants can help mitigate this risk (Holloway & Galvin, 2015a), these measures often require a considerable amount of time for the study environment.

It is important to note that, despite the qualitative nature of this study, neither phenomenological nor narrative methods were considered. Phenomenological methods aim to describe and interpret human experience. According to Galvin and Holloway (2015), phenomenological research relies on descriptions and/or interpretations of daily human experiences as data sources. Phenomenology involves capturing individuals' internal perspectives from their viewpoints, which may not address the research questions.

On the other hand, narrative survey research depends on experiential stories. Storytelling can involve imagination or even distortion; thus, storytellers do not always convey the truth. What is revealed may include the elements of the story that the storytellers wish to present as central to their experience, even if not factually correct (Freshwater & Holloway, 2015). Polkinghorne (2007) supported this view, maintaining that 'storied texts serve as evidence for personal meaning, not for the factual occurrence of the events reported in the stories' (p. 479). Atkinson (1997) and Atkinson and Delamont (2006) noted that narrative research often fails to retell stories critically and analytically, lacks analytical rigor, and does not hold any special status compared to other research approaches. This perspective was echoed by Easterby-Smith et al. (2015), who emphasized that narrative methods offer little uniqueness to qualitative research. Atkinson and Delamont (2006) likewise argued that narratives are frequently employed in a non-reflective and contextualized manner. Thus, the validity of narrative methods relies not on research participants telling the truth, but on their perspectives, which may not always be valuable for objectively understanding the phenomenon.

In addition to phenomenology, ethnography, grounded theory, and narrative research, Creswell and Poth (2018) identify the case study as the fifth major qualitative research approach. The case study approach in qualitative research has evolved as a method for exploring real-life, contemporary issues within their contexts. As the earlier approaches were not well suited to our study's objectives, we considered the case study approach as a design for our research.

### **3.2.2 Case Studies**

Qualitative case studies serve as an intensive and context-focused research approach that enables in-depth exploration and rich description of a phenomenon. Yin (1994) and Stake (1995) describe qualitative case studies as intensive investigations that generate rich descriptions of a single phenomenon, event, or program. According to Creswell (2013, p. 97), case studies "explore a real-life, contemporary bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in-depth data collection involving multiple sources of information... and report a case description and case themes." Case studies involve empirically studying an existing phenomenon in its context using evidence from various sources (Robson, 2011). They provide effective means for studying a phenomenon within its context, significant for understanding (Clarke et al., 2015). Additionally, case studies offer a holistic yet flexible design, as the boundaries of the study shape data collection. Yin (2003) asserts that a qualitative case study may consist of either a single study or multiple studies. A single case study typically examines, usually over time, only one or a small number of units, such as a group of people or an organization (Easterby-Smith et al., 2015), thus facilitating in-depth analysis. Yin (2003) suggests using a single case study when the researcher intends to investigate a single entity or group. The critical distinction between a single case study and a multiple case study is that, in a multiple case study, the researcher analyzes several cases (Gustafsson, 2017). Another essential difference is that the researcher can evaluate the data



both within individual cases and across multiple cases (Yin, 2003). Thus, multiple case studies allow the researcher to explore both the similarities and differences among the cases.

Given the research questions, this study adopted a multiple-case study design. A multiple-case study involves analyzing several cases to identify patterns, differences, and insights across various contexts (Gustafsson, 2017). According to Urbinati et al. (2020), multiple-case study analysis effectively addresses "why" and "how" questions, making it particularly suitable for cross-case comparisons. Additionally, evidence from a multiple-case study is strong and credible; the more case studies included in a scientific article, the greater the confidence in its representativeness (Gustafsson, 2017). The emphasis on understanding the phenomenon, namely data security gaps, within the context of the regulated environment of Nigeria's pharmaceutical industry, and as it manifests in practice, justifies the use of multiple-case studies as the most appropriate research design for this study. Furthermore, Yin (2013) recommends that clear designs be established for all case studies prior to data gathering. Also, Houghton et al. (2013) emphasized the necessity of employing multiple methods in case studies to facilitate validation and completeness across various data sources. Case study research typically employs multiple data collection methods to gain an in-depth understanding of the phenomenon within its real-life context. Common methods include interviews, document analysis, direct observation, and archival records, which allow for research triangulation and a more comprehensive view of the case (Yin, 2018; Merriam & Tisdell, 2016). Therefore, this study adopted a multi-method approach, aligning with the exploratory and explanatory goals of case study research.

### **3.3 The Triangulation Strategy**

For this study, triangulation—‘the combination of methodologies in the study of the same phenomenon’ (Denzin, 1970, p. 291)—was applied to the research questions to elicit answers. According to Knafl and Gallo (1995), triangulation fosters the overall

quality of a study on the premise that it supports the achievement of a clearly stated purpose. This study leveraged triangulation to realize several benefits, including minimizing biases, confirming findings, enhancing comprehensiveness, and fostering a deeper understanding (Adami & Kiger, 2005; Casey & Murphy, 2009; Oppermann, 2000; Thurmond, 2001). First, triangulation helped to surmount biases in this study. Oppermann (2000) identified methodological/instrument, investigator, and data biases as potential issues that may be addressed through triangulation approaches. According to Patton (1990), triangulation helps guard against the accusation that the results of a study are merely an artifact of only one method, source, or bias from a single investigator. Triangulation allows for the corroboration of results across datasets by reviewing the information gathered using various methods, thereby minimizing the impact of potential biases that may exist in a single study (Bowen, 2009). Moreover, the triangulation of data provides “a confluence of evidence that breeds credibility” (Eisner, 1991, p. 110). Bowen (2009) further states that triangulation counters both researcher and respondent bias. Besides the aforementioned biases, additional biases identified in the present study were also reduced through triangulation.

Second, triangulation confirmed the findings from this study. According to Denzin (1989), the validity of a study is strengthened through triangulation, on confirmation of results from different sources. Such validity was supported by Knafl and Breitmayer (1991), who assert that reliance on triangulation in qualitative research for confirmatory purposes enhances confidence in the reliability of findings, where consistency is established through data collection from a variety of methods. Boyd (2001) also highlighted the enhanced validity of qualitative research through triangulation by confirming the findings of multiple data-collection techniques. According to Casey and Murphy (2009), confirmation involves comparing and assessing data from multiple sources to determine the extent of consistency or validation of findings. They demonstrated the use of triangulation for confirmation purposes in

a study that used across-method triangulation, with a quantitative phase following the qualitative phase in sequence. This design made it easier to analyze the qualitative data collected, which in turn informed a survey used to gather quantitative data. Likewise, the use of triangulation for confirmatory purposes increased confidence in the research data and improved the validity of the present study.

Third, triangulation provided a comprehensive picture of the data security gaps by facilitating data completeness. The completeness of the data implies the aggregation of multiple perspectives from various sources which depicts a comprehensive picture of a phenomenon. Jick (1979) proposed triangulation as a way to make the data complete given its support for the holistic and contextual portrayal of a phenomenon that can improve understanding. Also, Boyd (2001) refers to the contribution of triangulation to the comprehensiveness of a study where completeness is desired. Foss and Ellefsen (2002) also point to the potential of triangulation to generate richer and more authentic data. In addition, Halcomb and Andrew (2005) emphasized triangulation's ability to generate complete and relevant data. What is more, triangulation provides the opportunity to discover a holistic view of the studied phenomenon when comprehensiveness is sought (Adami & Kiger, 2005). Employing triangulation for comprehensiveness resulted in a holistic view as well as a deep and extensive understanding of data security gaps.

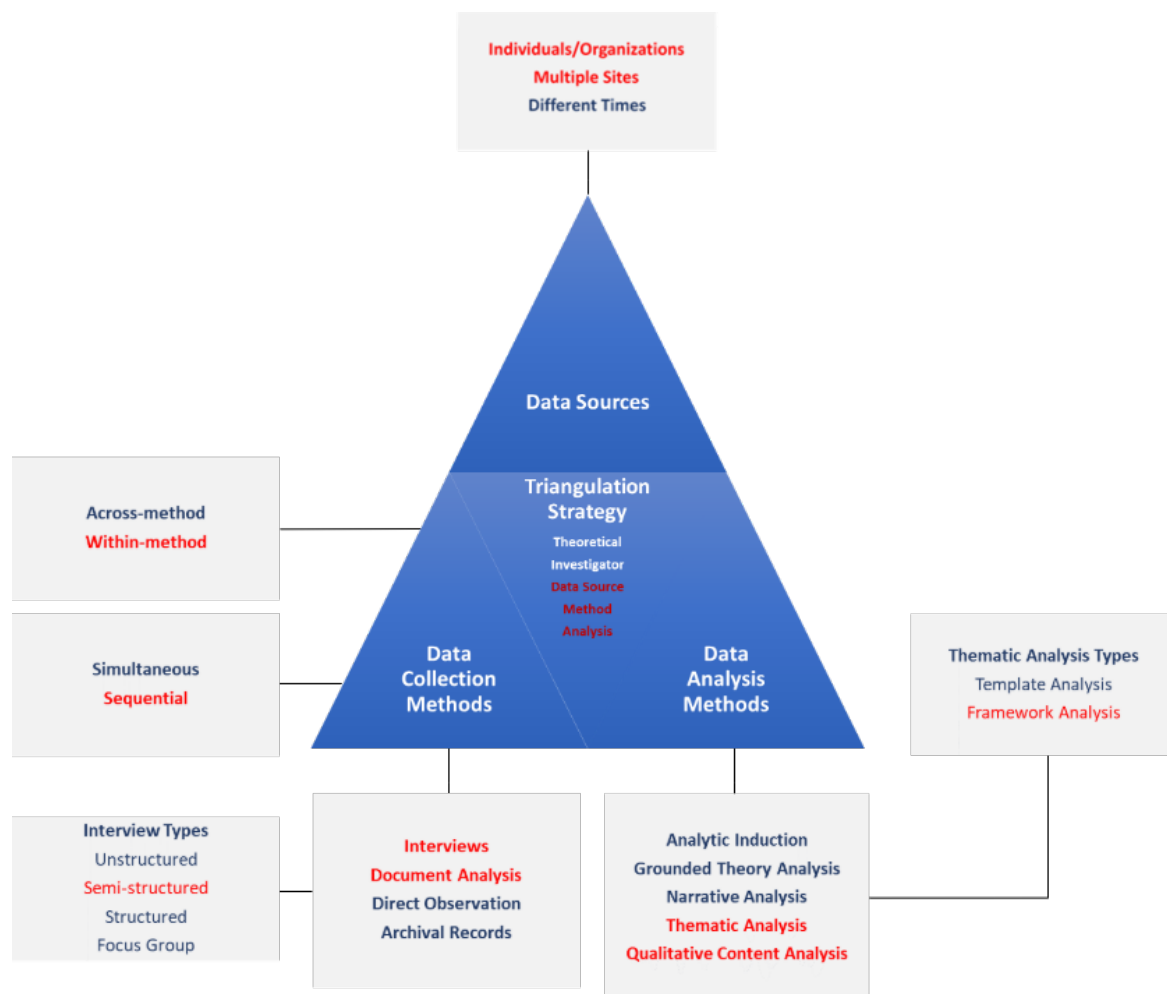
Fourth, triangulation facilitates an enhanced understanding of a phenomenon. Jick (1979) points out the usage of triangulation to further explain a research problem and create new methods. Triangulation approaches allowed for the interpretation of data with a reasonable level of assurance, which enhanced understanding of data security gaps.

Figure 29 illustrates the triangulation strategy, while Figure 30 presents the selected methods. Bowen (2009, p.29) maintained that "the qualitative researcher is expected to draw upon multiple (at least two) sources of evidence; that is, to seek convergence and corroboration

through the use of different data sources and methods”. Therefore, method, data source, and analysis triangulation were considered among the five triangulation types identified by Adami and Kiger (2005).

**Figure 29**

*Triangulation Strategy*



**Note.** The text highlighted in red represents the selected research methods.

Methodological triangulation helps to exclude contradictory explanations of observed changes and reduces doubt about findings linked to change (Hinds, 1989). Therefore, an enhanced explanation through methodological triangulation improves the understanding of a phenomenon. More so, methodological triangulation elaborates diverging results, as well as reveals deviant dimensions of a phenomenon, which provides new insights and a better

explanation of a research problem (Oppermann, 2000). Angers and Machtmes (2005) also emphasized the need for triangulation of study methods to validate and substantiate the data from the study. Casey and Murphy (2009) supported this view, asserting that methodological triangulation offsets the gaps in a single research strategy and helps address the bias of studies using single-method designs. Hence, the study employed methodological triangulation, which involved applying two research methods. From the classification of methodological triangulation by Casey and Murphy (2009), i.e., across method triangulation, which incorporates both qualitative and quantitative data collection methods within a single study, and within method triangulation, which involves using multiple data collection methods or approaches within the same research design, within method triangulation was chosen to achieve convergence and corroboration. Additionally, the study considered chronological methodological triangulation to enhance research robustness. Based on the classification of chronological methodological triangulation, which includes simultaneous (using quantitative and qualitative methods together) and sequential (applying one method after the other), the sequential approach was selected.

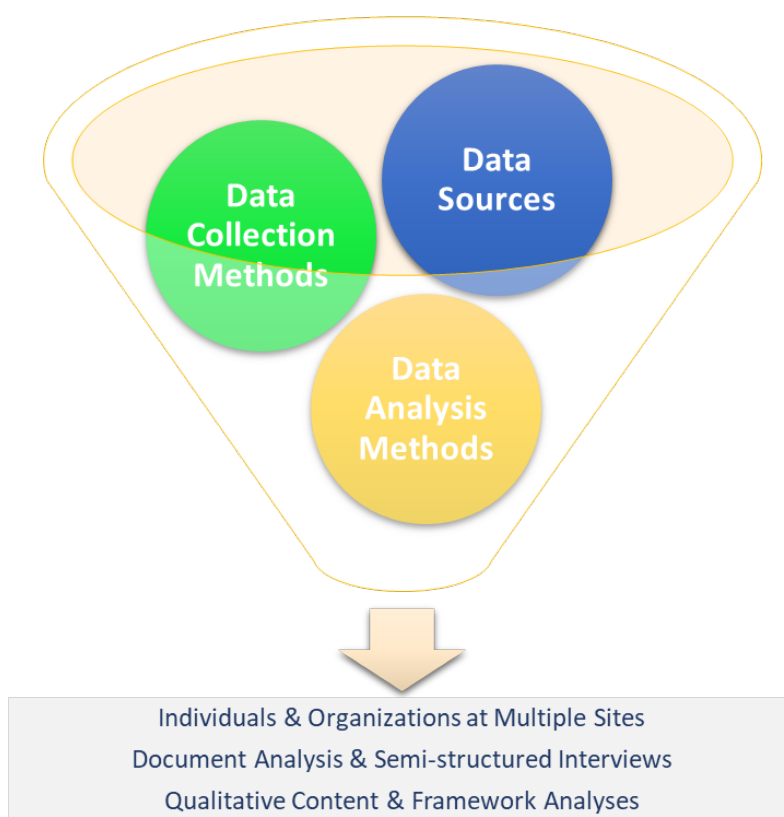
Furthermore, the study applied triangulation of data sources, which involves using the same approach for different datasets to falsify or verify generalizable patterns detected within a dataset. Based on Denzin's (1989) basic types of data source triangulation—person, space, and time—person and space data source triangulation were selected. According to Adami and Kiger (2005), person triangulation entails collecting data at different levels of people and groups, such as individuals and organizations, respectively, while space triangulation requires data collection at multiple sites. Time data source triangulation, which involves gathering data at different points in time, was not utilized in this study because the focus was on findings at a single point in time.

This study also employed data analysis triangulation. Triangulating analyses resulting

from various data collection methods provides a comprehensive view of the situation under study (Lacey & Luff, 2009). According to Thurmond (2001), data analysis triangulation involves combining multiple data analysis methods for validation. The qualitative data analyses incorporated qualitative content analysis and thematic analysis to address the research questions.

**Figure 30**

*Selected Research Methods*



### 3.4 Triangulation Methods for Data Collection

To ensure comprehensive and reliable findings, this study employed a triangulated approach for data collection, integrating multiple qualitative methods. This study used document analysis and qualitative interviews, each contributing unique insights into data security within Nigeria's regulated pharmaceutical industry. Together, these triangulation

methods ensured a rigorous, contextually rich examination of data security issues.

### **3.4.1 Document Analysis**

This study utilized the analysis of institutional documents as a data source. According to Bowen (2009), document analysis is a systematic procedure for reviewing or evaluating printed or electronic documents (computerized and Internet-transmitted). Document analysis has been employed as a research method in qualitative studies (Angers & Machtmes, 2005; Gagel, 1997; Wild et al., 2009). As a research method, document analysis is applicable to qualitative case studies. Bowen (2009) supported its use, justifying its importance in methodological and data triangulation, as well as its immense value in case studies (Bowen, 2009). First, documents are characterized by their exactness and broad scope. According to Yin (1994), documents span a long period, multiple events, and various settings. He added that the inclusion of accurate names, references, and event details makes documents beneficial in the research process. Furthermore, documents that bear witness to past events also provide background and historical information (Bowen, 2009). Such information assists in understanding the historical roots of specific problems and highlights conditions that affect the phenomena being investigated. Institutional documents from health authorities offered insights into the pharmaceutical context in which Nigerian drug manufacturing organizations operated.

Second, the accessibility of public documents allows for easy retrieval without the authors' permission, enabling repeated reviews and analyses in an unobtrusive, nonreactive manner (Merriam, 1998; Bowen, 2009). Moreover, documents contain text (words) and images that have been recorded without any researcher intervention. Atkinson and Coffey (1997) describe documents as "social facts" (p. 47) that are generated, shared, and utilized in a socially organized manner. As such, this research was not altered or influenced by the researcher's presence.

Third, the information within documents raises questions that should be considered in

the context of research. Goldstein and Reiboldt (2004) conducted a document analysis that facilitated the development of new interview questions while performing a longitudinal ethnographic study. Likewise, the analysis of the documents led to new interview questions for this study. Additionally, the data extracted from institutional documents were employed to provide context for the data gathered during the interviews.

Document analysis involves both content analysis and thematic analysis. According to Bowen (2009), document analysis is an iterative process that involves skimming through a cursory examination, conducting a thorough reading, interpreting, and integrating content analysis and thematic analysis. He defines content analysis as the method of organizing information into categories related to the research questions. Content analysis aims to draw systematic inferences based on qualitative data categorized around specific ideas or concepts (Easterby-Smith et al., 2015). According to Hsieh and Shannon (2005) and Flick (2009), content analysis involves examining data to assess the presence, significance, and relationships of the ideas or concepts arising from a theory, hypothesis, research questions, or the data itself. Content analysis begins with an initial review of documents, where significant and relevant portions of texts or other data are identified and separated from those that are not pertinent (Bowen, 2009; Corbin & Strauss, 2008; Strauss & Corbin, 1998).

Furthermore, content analysis helps identify an entity's focus on important issues. Weber (1990) emphasized its usefulness in uncovering and describing the focus or social attention of individuals, groups, and institutions. Additionally, Krippendorff (1980) notes that "[m]uch content analysis research is motivated by the search for techniques to infer from symbolic data what would be either too costly, no longer possible, or too obtrusive by the use of other techniques" (p. 51). Given these applications and constraints, content analysis was instrumental in determining health authorities' focus on data management in drug manufacturing.



Content analysis also provides an opportunity to infer significant issues such as trends, opinions, concepts, and principles. Holsti (1969) maintains that content analysis enables researchers to draw inferences by objectively and systematically identifying specific characteristics within messages. According to Stemler (2000), inferences from content analysis can be supported using alternative data collection methods. He adds that content analytics helps review trends in documents. In an empirical study, content analysis allowed Stemler and Bebell (1998) to move beyond anecdotal impressions and instead develop an evidence-based understanding of mission statement content, making it possible to highlight commonalities, differences, and trends across the sampled institutions. Similarly, analyzing the content of health authorities' guidance on data management allowed conclusions to be drawn regarding data security.

Additionally, content analysis offers an empirical basis for tracking changes in public perception. Stemler (2000) argued that data collected at one time can be objectively compared against data collected at a future time to determine whether changes have occurred in institutional documents. Similarly, data gathered from previous versions of health authorities' guidance were objectively compared with data collected in more recent versions to assess if data security was given greater emphasis in data management.

Interviews were used alongside document analysis due to the inherent limitations of documents in research. According to Bowen (2009), these limitations include biased selectivity resulting from incomplete document collection, challenges in retrieving documents due to deliberate denial of access, and insufficient details to address the research questions because they were created independently of a research agenda. Rossman and Wilson (1985) employed open-ended, semi-structured interviews in conjunction with document analysis to tackle these limitations. Thus, interviews were deemed necessary to avoid over-reliance on documents and to address the potential shortcomings of document analysis.

### 3.4.2 Qualitative Interviews

Qualitative interviews aim to obtain in-depth information about a given topic through which a phenomenon could be interpreted in terms of the meanings that respondents give to it. Qualitative interviews seek to collect information that reflects the meaning and interpretation of phenomena in terms of the interviewee's worldview (Kvale & Brinkmann, 2009). It seeks out why respondents hold those perspectives (King, 2004). Qualitative interviews also make it possible to analyze the data obtained in the context of the participants' social lives (Easterby-Smith et al., 2015). According to Tod (2015), qualitative interviews take a less structured, more flexible, and in-depth approach. She further recommended qualitative interviews where the objective of the research is to investigate a phenomenon of which little is known, get a sense of context, and verify the findings of other data collection methods, all of which apply to this study. Apart from its less structured and naturalistic manner of data collection, qualitative interviews widen the field of understanding of a phenomenon (Easterby-Smith et al., 2015).

Qualitative interviews describe a wide variety of different interview techniques, including focus groups, semi-structured, and unstructured interviews (Alshenqeeti, 2014). Focus-group interviews consist of loosely structured, facilitated conversations among a group of people (Easterby-Smith et al., 2015). According to Barbour and Schostak (2005), a focus-group interview is “an interviewing technique in which participants are selected because they are a purposive, although not necessarily representative, sampling of a specific population, this group being ‘focused’ on a given topic” (p. 46). However, focus-group interviews can be both cumbersome and time-consuming (Alshenqeeti, 2014). Moreover, social pressures can influence responses, and people may be unwilling or too timid to publicly express their views (Easterby-Smith et al., 2015). For this reason, focus-group interviewing was not chosen to obtain qualitative data.

Structured interviews are useful where some information is already available on the

subject (Murphy et al., 1998). The structured interview is primarily organized around a set of predetermined direct questions that require an immediate response, mainly of "yes" or "no" type (Alshenqeeti, 2014). According to Berg (2007), there would be very little freedom for the interviewer and interviewees to conduct such an interview. Therefore, there could be a superficial exchange of information that could lead to missed opportunities to capture the significance and interpretation of a phenomenon in the worldviews of the interviewees. As a result of the risk of losing these insights, structured interviews were not selected as a data collection method.

Unlike a structured interview, an unstructured or open interview is an open situation where more freedom and flexibility are offered to interviewers and interviewees, in terms of planning, organizing, and implementing the content and questions of the interview (Gubrium & Holstein, 2002). According to Tod (2015), this approach is most used in qualitative research methodologies where there is little prior knowledge of the field of study exists. However, an open interview will likely be directed more by the informant's agenda rather than that of the investigator. Furthermore, unstructured interviews can be labor-intensive and costly. Their informal and non-directional nature means they can take a long time to transcribe and analyze. For these reasons, unstructured interviews were not chosen as a data collection method for this study.

The semi-structured interview lies in the middle of a continuum of fully structured or unstructured interviews (Tod, 2015, Figure 28.1). The semi-structured interview is a more flexible format than the structured interview. It allows for further exploration by providing the opportunity to probe and broaden the respondent's responses (Rubin & Rubin, 2012). In addition, semi-structured interviews allow coverage of all relevant areas. More so, semi-structured interviews maintain the flexibility to follow up on unanticipated issues raised by participants. Moreover, the control and direction of such interviews remain with the

investigator, but there is the capacity to respond to the respondent's agenda and views. For this study, open-ended, semi-structured interviews were used to complement document analysis.

Furthermore, face-to-face interviews were chosen to engage participants, though they were conducted remotely. Remote or mediated interviews provide flexibility in scheduling and location, making it easier for participants to take part without needing to travel. According to Easterby-Smith et al. (2015), remote interviews offer participants greater flexibility. Moreover, when there is a strong relationship of trust with the research participant, as in the current study, remote interviewing is a valuable method for conducting follow-up interviews. Mediated interviews can be either asynchronous or synchronous (Easterby-Smith et al., 2015). Asynchronous interviews allow participants to engage at different times, which gives them more flexibility. Also, participants may feel less pressure since they are not required to host or meet with the researcher at a specific time. Asynchronous interviews, such as those conducted via email or on online forums, provide respondents with more time to reflect on their answers, enhancing their ability to control their representations (Easterby-Smith et al., 2015). However, asynchronous interviews may be more prone to distractions and sudden dropout (Tracy, 2013). Therefore, synchronous interviews, which include real-time face-to-face interactions and discussions, were chosen. Synchronous mediated interviews enable live discussions between the interviewer and the respondent (O'Connor et al., 2008) using electronic communication tools. This includes phone conversations (Easterby-Smith et al., 2015) and video conferencing interviews supported by platforms like Skype, Microsoft Teams, and others. Given the requirement for expert interviews amid COVID-related restrictions, the study was well-suited for synchronous, remote, semi-structured interviewing.

### **3.5 Sampling Design**

The sampling design of this study was developed to enable an in-depth qualitative exploration of data management standards and practices, with an emphasis on data security,

within Nigeria's pharmaceutical industry. The study adopted a suitable sampling strategy to align with its objectives and the nature of qualitative research. The sample characteristics and size not only reflected the sampling strategy but also captured a detailed and representative understanding of data security within Nigeria's pharmaceutical sector industry.

### **3.5.1 Sampling Strategy**

This study examined the two broad categories of sampling designs, shown in Figure 31, probability sampling and non-probability sampling. According to Hunt and Lathlean (2015), probability sampling is the preferred method in quantitative research, where the goal is to select a sample from the target population that accurately reflects it, enabling the generalization of findings. In contrast, they assert that non-probability sampling is mainly used in qualitative research, where the emphasis is on individual cases that yield rich, in-depth data rather than a representative sample. The choice between probability and non-probability sampling designs, however, hinges on the research objectives.

Qualitative research typically employs sampling methods where the sample is intentionally targeted and selected to provide detailed, data-rich examples of the phenomenon under study. Hunt and Lathlean (2015) argue that the sample in qualitative research should cover the entire range of relevant cases or settings, allowing for conceptual rather than statistical generalizations. Since the research question did not require examining the relationships between variables, comparing groups of individuals, or generalizing to a larger population, probability sampling designs such as simple random sampling, stratified random sampling, systematic random sampling, and multistage sampling or cluster sampling were not employed. Instead, non-probability sampling was chosen to identify individuals, events, or settings that best illuminate the phenomena of interest and provide rich data.

This study critically examined various non-probability sampling designs and selected the most appropriate approach for addressing the research objectives. Non-probability

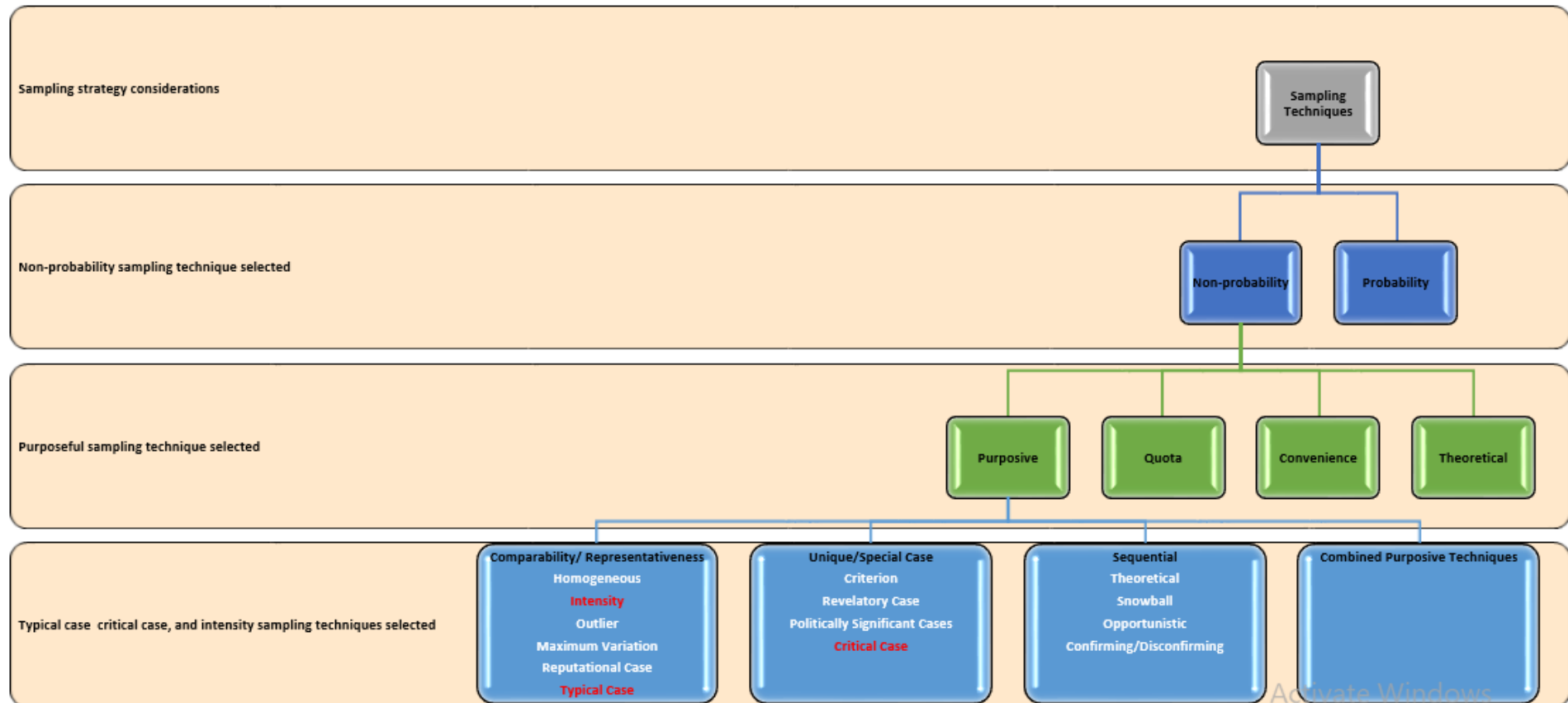
sampling designs include theoretical sampling (Easterby-Smith et al., 2015), convenience sampling, quota sampling, snowball sampling, and purposive sampling (Hunt & Lathlean, 2015). Theoretical sampling arises from data analysis. Hunt and Lathlean (2015) describe theoretical sampling as “a study using a grounded theory design whereby data are collected until data 'saturation' has been achieved and no new themes or perspectives are found” (p. 182). However, this study does not utilize a grounded theory design, as sampling occurs before data collection. Convenience sampling involves taking readily available samples that meet the requirements of a sufficiently large sample (Easterby-Smith et al., 2015) and include those willing to participate in a study (Teddlie & Yu, 2007). However, Hunt and Lathlean (2015) caution against convenience sampling due to significant errors and biases if the sample is not representative of the target population. Easterby-Smith et al. (2015) further note that there's no assurance that any sample obtained through convenience sampling is representative of a specific population of interest. Therefore, convenience sampling was not chosen as a sampling design for this study. Snowball sampling is similar to convenience sampling in certain respects, while quota sampling is a type of convenience sampling. Although snowball sampling addresses the challenge of ensuring a sufficient sample of hard-to-find individuals (Easterby-Smith et al., 2015), it also introduces potential representativeness issues (Hunt & Lathlean, 2015). In contrast, quota sampling aims to ensure that all areas within a sampling design are represented (Easterby-Smith et al., 2015), but bias may arise if the study intentionally or unintentionally excludes certain types of individuals (Hunt & Lathlean, 2015). Due to these potential biases, snowball and quota sampling were not employed in this study.

To effectively address the research questions, purposive sampling techniques were chosen to gather qualitative data from samples. Purposive or purposeful sampling is a method in which “specific settings, individuals, or events are intentionally selected for the valuable information they can provide that cannot be obtained as effectively from other options”

(Maxwell, 1997, p. 87). Teddlie and Yu (2007) defined purposive sampling as “selecting units (e.g., individuals, groups of individuals, institutions) based on specific purposes related to answering the research study’s questions, primarily used in qualitative studies” (p. 77). Hunt and Lathlean (2015) describe purposive sampling as a form of non-probability sampling where decisions about who to include in the sample are made based on various criteria. Purposive sampling techniques involve the selection of individual units or cases based on purpose rather than random selection (Tashakkori & Teddlie, 2003). According to Easterby-Smith et al. (2015), a clear understanding of the required sampling units is assumed and aligns with the study's objectives, with potential participants then queried to determine if they meet the eligibility criteria. To gain a deeper understanding of the population's nature and experiences, a purposeful sample was chosen for the current study.

Several purposeful sampling techniques were considered in the study. Patton (2002) identified various types of purposeful sampling techniques, which include typical cases, maximum variation cases, theory-based cases, extreme or deviant cases, and confirming and disconfirming cases. Building on this framework, Teddlie and Yu (2007) proposed three overarching categories of selective sampling, along with a composite category that incorporates multiple purposeful strategies, each offering distinct approaches for addressing specific research objectives.

First, sampling aimed at achieving comparability and representativeness includes homogeneous sampling, intensity sampling, outlier sampling, maximum variation sampling, reputational case sampling, and typical case sampling strategies. Second, unique and special case sampling includes criterion sampling, revelatory case sampling, sampling politically significant cases, and critical case sampling strategies. Third, sequential sampling comprises theoretical sampling, snowball sampling, opportunistic sampling, and confirming and disconfirming cases.

**Figure 31***Sampling Strategy Considerations*

**Note.** The text highlighted in red represents the selected sampling techniques. The sampling strategy was determined by the author based on non-probability sampling designs (Easterby-Smith et al., 2015; Hunt & Lathlean, 2015) and purposeful sampling techniques (Teddlie & Yu, 2007).



Lastly, combined purposive techniques utilize multiple qualitative methods within a single study. Teddlie and Yu (2007) emphasize that many qualitative studies employ more than one purposeful sampling technique due to the complexity of the issues at hand. For instance, Poorman (2002) combined snowball, homogeneous, maximum variation, and theory-based sampling when selecting participants for focus groups. Given the complexities associated with data security in Nigeria's regulated pharmaceutical industry, a combination of purposive strategies were selected for this research study.

Sampling with a combination of purposive techniques consisted of typical case sampling, critical case sampling, and intensity sampling to deliberately target drug manufacturing environments, individuals, and institutional documents respectively. According to Etikan et al. (2016) and Suri (2011), typical case sampling is used to profile what is average or usual for a specific phenomenon. Typical case sampling provide a general picture of what is "typical" or standard within the population. For example, selecting a mid-sized pharmaceutical company in Nigeria that adheres to standard drug manufacturing practices to represent the average conditions of drug manufacturing in the country. By sampling critical cases, samples are collected that are most likely to provide the desired information. According to Stewig and Stead (2001), such sampling is especially useful when a small number of cases may be sampled. Critical case sampling focuses on the few cases that are most likely sources of essential information or reveal significant insights applicable to similar contexts. For example, interviewing a participant, such as an IT manager from a pharmaceutical company that recently experienced the IP theft. Intensity sampling involves selecting or seeking out rich or exemplary instances of the phenomenon being investigated. For instance, analyzing institutional documents from an organization recognized for its robust data management protocols to explore best practices in depth. According to Etikan et al. (2016) and Suri (2011), intensity sampling allows for the selection of a limited number of rich cases that offer detailed

information and a comprehensive understanding of the phenomenon under study. We now turn to a discussion of the study's sample characteristics and size.

### 3.5.2 Sample Characteristics and Size

The sample for this research comprised five Nigerian pharmaceutical organizations, thirty-one professionals, and three institutional documents. This sample size was purposively selected based on both practical and methodological considerations aligned with qualitative research conventions. First, the study employed a multiple-case study design, which benefits from in-depth exploration rather than broad generalization. Yin (2018) notes that a small number of well-chosen cases in qualitative research can yield rich, contextual insights when the objective is to explore a phenomenon in depth.

**Participating Organizations.** The selection of the participating organizations was guided by theoretical sampling logic, with each organization purposefully chosen for its relevance to the study's objectives—namely, its pursuit of WHO cGMP prequalification and its engagement with data management challenges. This study focused on members of the PMG-MAN (Members, n.d.), specifically the eleven drug manufacturing organizations striving to achieve or maintain the highly regulated standards expected of drug manufacturing organizations (CardinalStone, 2014). Due to access limitations, the study was limited to five of these eleven Nigerian drug manufacturers that participated in the WHO cGMP prequalification and certification process.

**Subject Matter Experts.** This study also targeted individuals with expert knowledge of the subject matter who are most likely to provide sufficiently relevant and in-depth data. They include a sample of professionals from Nigerian drug manufacturing organizations, including IT managers/information systems operations managers, system administrators, information/cyber security analysts, and DPOs who play critical roles: review or implement information system controls; protect data against unauthorized access, corruption, or loss;

establish or maintain data recovery practices. The selection of the four roles for each organization allowed for an estimated 48 experts to participate in this study. Furthermore, these experts ranged in age from 25 to 50 years and were either male or female. Given the essential information sought, persons who do not have a minimum of five years of experience in computer systems and data security in the pharmaceutical industry were excluded from the study.

The sample size comprising thirty-one professionals from five Nigerian pharmaceutical organizations was deemed sufficient for this research because the primary aim was not to generalize findings across the entire pharmaceutical sector in Nigeria but to achieve data saturation—the point at which no new themes or insights emerge from additional interviews (Fusch & Ness, 2015). By the 28th interview, emerging patterns had already become repetitive and stable, and no substantial new codes were identified thereafter, indicating thematic saturation. The final three interviews served as a validation phase, confirming the adequacy of the data collected. This finding was consistent with Guest et al. (2006), who found that data saturation in qualitative studies often occurs within the first 12 to 30 interviews. Thus, the sample size of five organizations and thirty-one professionals was sufficient to ensure credible and transferable findings, offering a robust foundation for thematic analysis across cases.

**Institutional Documents.** Three institutional documents (PIC/S, 2021; WHO, 2016; WHO, 2021) were selected for analysis based on their authority, relevance, and influence within the pharmaceutical regulatory landscape. The criteria for inclusion were as follows:

**Regulatory Authority.** Each document analyzed in this study was published by a globally recognized health authority—specifically, WHO and PIC/S. These institutions play a central role in shaping international regulatory expectations and are widely regarded as standard-setting bodies in pharmaceutical manufacturing. Their guidelines are not only referenced globally but also directly inform the regulatory frameworks adopted by NRAs, such

as NAFDAC.

**Topical Relevance.** The documents specifically addressed data management and integrity within GMP, making them directly pertinent to the study's focus on data security in drug manufacturing. The inclusion of documents that provided explicit guidance on how pharmaceutical data should be handled, maintained, and secured was essential for evaluating gaps in existing guidelines related to data security.

**Current Use in Practice.** The selected documents are actively referenced by pharmaceutical firms seeking WHO cGMP prequalification and thus reflect the de facto standards in the operational environment under study. Their representativeness lies in their widespread use and endorsement as guiding frameworks for regulatory compliance.

Together, these documents formed a robust basis for evaluating regulatory guidance and its alignment—or misalignment—with actual practices in Nigerian pharmaceutical manufacturing.

### 3.6 Research Tools

Semi-structured interviews require an interview guide to maintain an appropriate balance between direction and flexibility. For this study, semi-structured interviews were guided by a list of question items (see Appendix B), informed by the Center for Internet Security (2021) and the Information Systems Audit and Control Association (2021) data security controls. Examining the guidance documents from PIC/S (2021) and WHO (2016; 2021) on data management also provided additional questions for the interview guide. These questions were designed to elicit insights into how Nigerian drug manufacturing practices align—or do not align—with established data management standards and security best practices, directly addressing the research objective of identifying shortcomings in these practices.

The reliability and validity of the interview guide were enhanced through member

checking. Member checking involves interviewing participants who represent the target population using the interview guide (Creswell & Creswell, 2017; Kvale & Brinkmann, 2009; Lincoln & Guba, 1985; Morse et al., 2002; Tong et al., 2007). The interview included recording participants' responses to the questions and probes outlined in the guide. Participants received a summary or excerpts of their interview transcripts along with the corresponding questions from the interview guide and provided feedback on the clarity, relevance, and comprehensiveness of the interview questions. Member checking encouraged participants to determine if the questions adequately captured their experiences, perspectives, and insights regarding the topic being studied. This process ensured that the interview guide aligned with the research objective by confirming it gathered information on data security practices, gaps, and participant perspectives. Member checking also involved exploring participants' areas of concern or discrepancies and seeking clarification or additional insights to ensure a thorough understanding of their viewpoints. Feedback received during the member-checking session led to necessary revisions of the interview guide. The interview guide was finalized for future use in data collection, with adjustments made to enhance the clarity, relevance, and effectiveness of the questions, probes, and topics covered. These adjustments ensured that it would effectively identify gaps in Nigerian drug manufacturing practices related to data security.

### **3.7 Study Procedures and Ethical Assurances**

The study's design followed strict scientific principles, ensuring that all methods used were appropriate for effectively addressing the research questions. The emphasis on ethical assurances required obtaining permission from gatekeepers and informed consent from participants, thus safeguarding their rights and promoting transparency throughout the research process. Additionally, the study established strong protocols for data collection, management, and dissemination to uphold confidentiality and ensure responsible reporting of findings. It outlines the procedures and ethical assurances implemented to maintain the integrity and

validity of the research on data security in Nigeria's pharmaceutical industry.

### 3.7.1 Ethical Assurances

This study obtained ethical approval from the university ethics committees prior to data collection, given the involvement of human subjects. Engaging with human participants in a research project raises significant ethical concerns. These ethical issues emphasize the vital role of ethics in conducting research involving human subjects. According to Shawa (2017), ethics is closely linked to morality and requires incorporating moral considerations when working with human subjects. Guillemin and Gillam (2004, p. 262) state that “ethical dilemmas and concerns are part of the everyday practice of doing research—all kinds of research.” Therefore, it is crucial to thoroughly identify and assess the potential ethical risks that may arise during research. Equally important is taking proactive measures to address these risks by applying appropriate ethical principles. Bell and Bryman (2007) identified 11 categories of ethical principles, as shown in Figure 32, which guided the integration of ethical considerations in this research.

This study also addressed various ethical dimensions. Shawa (2017) outlined domains of ethical consideration in a research project: scientific validity; gatekeeper permission and participant consent; informed consent and participants' rights; data collection and management; dissemination of information. Considering the potential ethical dilemmas associated with the exploratory nature of this study, conducted in several organizations, the following strategies and precautions were implemented to mitigate potential risks.

**Scientific Validity.** Scientific validity is one aspect of ethics related to the coherence of the research protocol. Shawa (2017) suggested a strong alignment between the research topic, the purpose (aim and objective), and the central questions of the research. Thus, the interview guide included question items that reflected the identified phenomenon of interest and the study's purpose. Shawa (2017) also emphasizes the importance of aligning the

information needed to answer research questions with the sources of that information. He asserted that the sampling process and the relevance of the data provided by participants should ensure this alignment and address issues of bias, trustworthiness, and accuracy. The sampling design justified the selection of participants in relation to the research aims and objectives of this study, ensuring that the findings were unbiased, defensible, and credible.

**Figure 32**

*Category of Ethical Principles*



**Note.** Based on the content in “The Ethics of Management Research: An Exploratory Content Analysis,” by E. Bell & A. Bryman, 2007, *British Journal of Management* 18(1) pp. 63-77. (<https://doi.org/10.1111/j.1467-8551.2006.00487.x>).

An additional aspect of scientific validity is the research instruments used for data collection. Shawa (2017) recommends assessing the alignment between the instrument’s questions and those of the research. Specifically, the question items in the interview guide (see Table A1) were derived from data security controls expected in a highly regulated environment, which directly inform the second research question. Thus, the study achieved this alignment to the extent that gaps arise from the absence, ineffectiveness, or inefficiency of data security controls.

**Gatekeeper's Permission and Participant's Consent.** Unauthorized disclosure of sensitive information can lead to legal, economic, social, and health consequences. According to Shawa (2017), researchers must address issues related to research relationships, such as confidentiality, access, secrecy, and deception. Easterby-Smith et al. (2015) highlighted potential problems of deceit and challenges in defining confidentiality and privacy when accessing organizations and individuals. They advocated for ethical responses, including developing relationships with organizations in a non-judgmental manner, obtaining informed consent from all parties involved, and specifying research proposals for access. Shawa (2017) also recommended establishing formal communication with enterprises or authorized institutional representatives to secure explicit permission, ensuring that gatekeepers understand the research's nature, their rights, and the permissions granted. Consequently, the study involved obtaining authorization and access through gatekeeper letters (see Appendix E), and securing participants' consent via informed consent forms before conducting research within the case organizations.

**Informed Consent and Participant's Rights.** In addition to the permission of gatekeepers, the study also sought informed consent. Informed consent and participants' rights are essential components of the study's ethical framework, which upholds the principles of confidentiality, autonomy, and respect for participants. Participants must provide their consent with a thorough understanding of their roles, responsibilities, and rights in the research process. According to Shawa (2017), participants should comprehend the research process, the reasons for their participation, who will utilize it, and how research results will be reported. He also asserts that researchers should inform participants of their right to withdraw from participation without offering a reason during the research process. Obtaining informed consent ensures that participants are fully aware of the study's objectives, potential risks involved, and their rights as participants. As a precautionary measure, this study required that signed consent forms serve



as letters of consent. Shawa (2017) also recommends that researchers draft and provide participants with an information letter that includes the research supervisor's contact details and the affiliated institution for reference. He adds that the information letter should accompany a consent form on a separate page for research participants to complete and sign. Accordingly, this study ensured that information letters accompanied consent letters to debrief research participants (see Appendix F).

**Data Collection and Management.** Data collection has two ethical dimensions. The first concern involves the type of data being gathered, which may raise ethical issues if its collection negatively impacts participants. Shawa (2017) recommends providing a clear justification for such data requirements and implementing safeguards to minimize their impact on participants. However, this study did not pinpoint any potential risks, including psychological or physical harm, or ethical problems related to data collection. The second ethical consideration pertains to the management and security of the collected data. As a precaution, this study ensures that research and personal data from participants were securely stored on cloud storage platforms for five years, utilizing data protection technologies like encryption and access controls.

**Data Dissemination.** Disseminating information was another area of ethical concern for this study. An organization or individuals affiliated with it may be adversely affected by research publications that could be defamatory and damaging to their reputation. Easterby-Smith et al. (2015) recognized these ethical dilemmas and recommended adhering to confidentiality and anonymization requirements. Shawa (2017) supported these recommendations, arguing that research participants should have the right to confidentiality and anonymity when data is disseminated, unless such persons or their guardians waive this right. Consequently, this study employed pseudonyms as a precautionary measure to protect the identities of organizations and participants in its publication.

Ethical dilemmas and unpredictability in qualitative research necessitate proper preparation. Guillemin and Gillam (2004) recommend reflexivity in scenarios of ethical importance during qualitative research. They also suggest that researchers step back and consider their roles in planning, conducting, and writing research to ensure rigorous ethical practices. Thus, this study employed journaling to identify biases, clarify professional experiences on the topic, and avoid those experiences that could influence the analysis or findings. Journaling facilitated insights, helped address unforeseen situations, and ensured that the study remained on track.

### **3.7.2 Study Procedures**

This study began with a literature review that refined the research questions and informed the methodological approach, as shown in Figure 33. A multiple case study design with triangulated data collection and analysis ensured validity and credibility. Subsequent phases were guided by ethical standards, with an emphasis on transparency, informed consent, and confidentiality. The meticulous execution of the study procedures underscored participants' informed consent as a cornerstone of ethical practice.

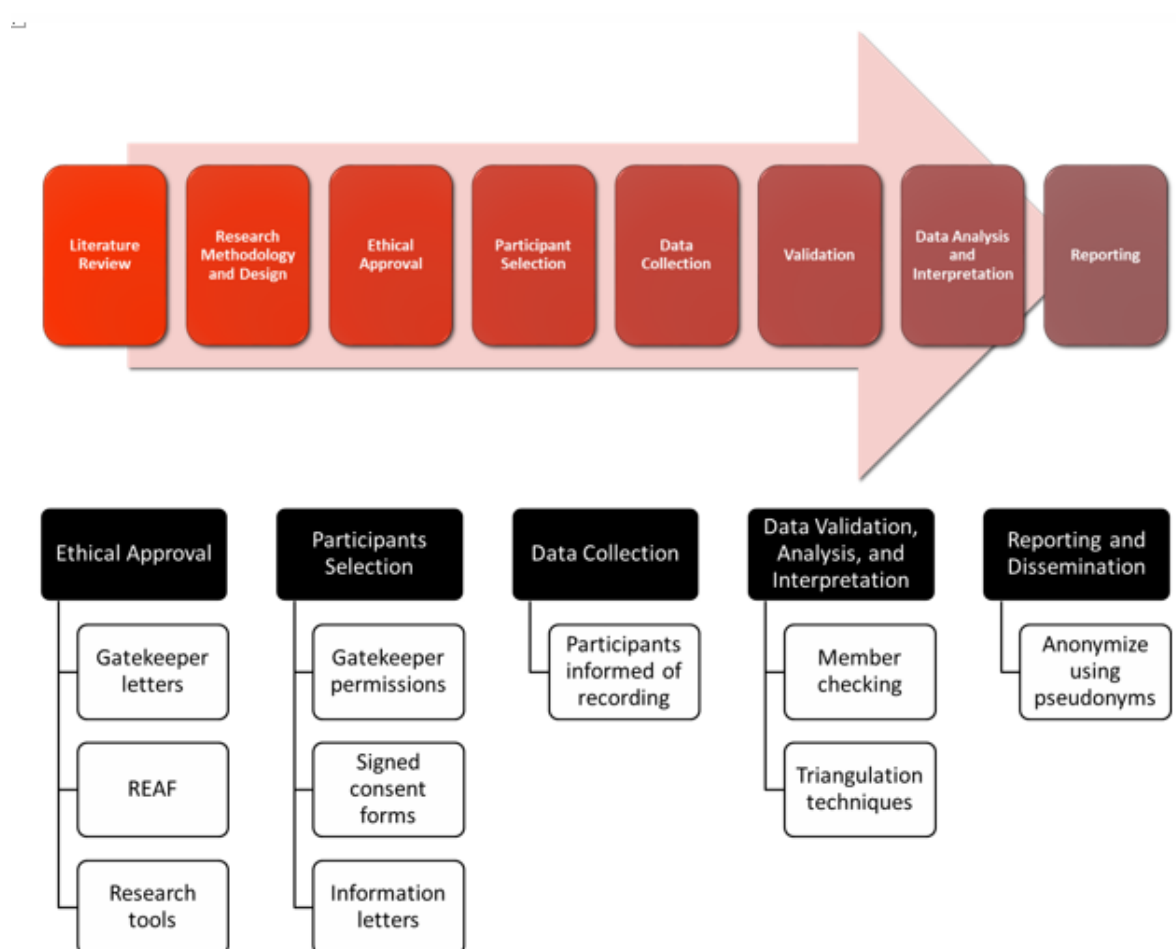
**Literature Search and Review.** Conducting a literature search involved seeking scholarly articles in online databases using specified search terms. The literature review entailed summarizing the latest advancements in the field along with the findings from peer-reviewed articles. This process also included refining the research questions that arose from the literature review. Ethical considerations for this phase emphasized the importance of ensuring transparency by providing the criteria used for the search and review.

**Research Methodology and Design.** Determining the appropriate research methodology—such as interpretivism, qualitative research, and case studies, particularly multiple case study design—required justification of the decisions made. The development of a triangulation strategy for data collection, including document analysis and semi-structured

interviews, and analysis that utilized a combination of qualitative content and thematic analyses enabled validation of data from various sources and methods, thus ensuring the credibility and trustworthiness of the research. Selecting the right sampling strategy, such as purposeful sampling, and techniques like typical case sampling, critical case sampling, and intensity sampling also demanded justification for their choices. The sampling design incorporated scientific validity, ensuring that the selection criteria, participants, and sampling process directly aligned with the research objectives while addressing potential biases, as recommended by Shawa (2017).

**Figure 33**

*Study Procedures and Ethical Assurance*



**Ethical Approval.** Obtaining ethical approval required consent from the University Research Ethics Committee (UREC) to conduct research involving human subjects. The approval process necessitated the development of a comprehensive interview guide that covered relevant topics to effectively address the research questions. The ethical framework enhanced scientific validity by ensuring that the interview questions were aligned with study objectives while protecting participants' rights and well-being. Key documentation, such as the Gatekeeper Letter and the Research Ethics Approval Form, were completed and submitted for review.

**Research Participant Selection.** Recruiting research participants required distributing completed gatekeeper letters to pharmaceutical organizations involved in the case study to secure permissions. This process also included finding participants who could provide valuable insights into the research topic. To uphold ethical integrity, both gatekeeper permissions and informed consent from participants were gathered through signed consent forms. Participants received information letters detailing their rights, including the right to withdraw from the study at any time without needing to explain, thereby ensuring their autonomy and respect throughout the research process. Participation in the study was completely voluntary, with informed consent secured from participants before the interviews started.

**Data Collection.** The data collection step involved gathering information through document analysis and semi-structured interviews. Also, collecting data from multiple sources enabled the comparison of information gathered through document analysis and interviews, as well as from respondents' accounts (Lathlean, 2015). Document analysis required qualitative content analysis, while semi-structured interviews were crucial for engaging participants. These interviews included sessions with IT managers/ information systems operations managers, system administrators, information/cyber security analysts, and DPO's conducted via video conferencing tools. The interviews took place between April 29 and May 28, 2022,

utilizing an interview guide (see Appendix B) and a Questionnaire Template for Demographic Information (see Appendix A) to collect participants' demographics. Prior to the interviews, participants were informed verbally and through informed consent forms that the sessions would be audio recorded. Technological solutions ensured the secure recording and storage of interview data. Ethical assurances during data collection included protecting participant confidentiality and anonymity, as well as complying with secure data management practices.

**Data Validation, Analysis, and Interpretation.** Data validation, analysis, and interpretation were performed after the data is collected. This analysis involved using qualitative content and thematic analyses to identify themes. The process also included validating the findings through member checking and triangulation techniques to ensure trustworthiness and consistency. A comparative analysis compared and contrasted emergent themes from qualitative content and thematic analyses, aiming to pinpoint data security gaps. Interpretation concentrated on situating the findings within the research questions, theoretical framework, and existing literature while assessing their implications for theory, practice, and future research.

**Reporting and Dissemination.** The reporting phases involved presenting the research findings clearly and coherently through written reports, presentations, and a thesis that adhered to academic standards and guidelines. Data dissemination accounted for potential risks, including reputational harm to organizations and participants. To mitigate these risks, pseudonyms were used to anonymize organizations and participants. Ethical considerations ensured that findings were communicated objectively and without bias, preserving participant confidentiality while maximizing the broader impact of the study.

### **3.8 Triangulation Methods and Software for Data Analysis**

This study used triangulation methods for data analysis to enhance the credibility and depth of findings. Selected analytical methods aimed to ensure a robust interpretation of

qualitative data, while alternative approaches were evaluated and excluded due to their irrelevance to the research objectives. The study also considered using specialized software for qualitative data analysis.

### **3.8.1 Selected Data Analysis Method**

This research employed triangulation to demonstrate rigor in qualitative data analysis. Triangulating data from different sources and analyzing various forms of data contribute to the rigor of a study (Lacey & Luff, 2009). First, content analysis was used to categorize and extract data from health authorities' guidance documents, involving a preliminary examination of the documents, the identification of relevant passages of text, and the exclusion of irrelevant data (Bowen, 2009; Corbin & Strauss, 2008; Strauss & Corbin, 1998). This process included organizing information according to the main research questions (Bowen, 2009). Second, respondents' accounts were analyzed to validate the findings from the content analysis, serving as a form of triangulation aimed at enhancing the understanding of data security gaps in the Nigerian pharmaceutical industry.

Thematic analysis was employed to identify and interpret patterns within the interview data relevant to the study's research objectives. It involved systematically coding and organizing interview data to uncover recurring themes (Braun & Clarke, 2006). This process required familiarization with the data, followed by the generation of initial codes, the construction of themes, and the refinement of thematic categories (Nowell et al., 2017).

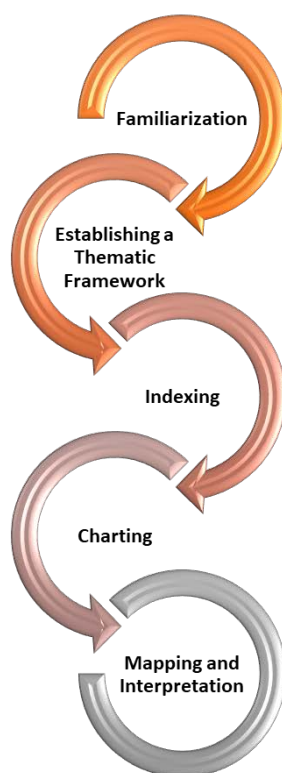
Furthermore, the study considered analytical frameworks such as Thematic Networks (Attride-Stirling, 2001) and the Framework Approach (Ritchie & Lewis, 2003). These frameworks enhance transparency in data analysis by illustrating the connections among the analytical stages (Pope et al., 2000; Ritchie & Lewis, 2003). Such connections allow for in-depth data exploration while maintaining an effective and transparent audit trail. As a result, these frameworks improve the rigor of the analytical processes, enhance the credibility of the

findings (Ritchie & Lewis, 2003), and ensure that the study is methodologically robust.

The study identified framework analysis as a structured approach to enhance the rigor of thematic analysis. Framework analysis aligns well with studies that have specific policy- or practice-oriented objectives, as it accommodates both inductive and deductive coding approaches (Gale et al., 2013; Ritchie & Spencer, 1994). Therefore, it allows for the inclusion of both a priori concepts (as in template analysis) and emergent concepts derived from coding. Framework analysis consists of distinct yet interconnected stages. According to Lacey and Luff (2009), the stages of framework analysis are familiarization, establishing a thematic framework, indexing, charting, and mapping and interpretation, as shown in Figure 34.

**Figure 34**

*Framework Analysis Stages*



**Note.** Based on content from *Qualitative Data Analysis: The NIHR Research Design Service for Yorkshire and the Humber*, by A. Lacey & D. Luff, 2009, National Institute for Health Research.

[https://www.academia.edu/download/61606002/9\\_Qualitative\\_Data\\_Analysis\\_Revision\\_200920191225-129738-301p8i.pdf](https://www.academia.edu/download/61606002/9_Qualitative_Data_Analysis_Revision_200920191225-129738-301p8i.pdf)

**Familiarization.** Familiarization involves transcribing data and entails exploring it to grasp key ideas and recurring themes. This stage requires reviewing notes, reading transcripts, listening to recordings, etc. It allows the researcher to immerse themselves in the material and begin identifying patterns or points of interest.

**Establishing a Thematic Framework.** Identifying a thematic framework involves recognizing important issues, concepts, and themes, as well as establishing an index or framework (Lathlean, 2015). According to Lacey and Luff (2009), the thematic framework is the initial coding framework, which evolves based on both a priori and emerging issues from the familiarization stage. It evolves based on both a priori concepts and emerging issues identified during the familiarization stage.

**Indexing.** Indexing is the systematic application of the index or framework to the textual form of the data, and annotating the text with codes (Lathlean, 2015). In this stage, the thematic framework is applied to the data using textual or numeric codes to identify specific data related to different themes (Lacey & Luff, 2009). This process ensures that all relevant information is categorized accurately for later retrieval and interpretation.

**Charting.** Charting requires significant synthesis and abstraction. This process involves using headings from the thematic framework to create charts from the data, enhancing readability throughout the entire dataset (Lacey & Luff, 2009). Charting also entails extracting data from its original context and reorganizing it according to themes in a graphical format (Lathlean, 2015). Lacey and Luff (2009) state that charts can represent cases for each respondent across themes or themes for each theme across respondents (cases). Charts may exist independently for each major theme, containing data from multiple respondents (Lathlean, 2015).

**Mapping and Interpretation.** Mapping and interpretation involve searching for patterns, relationships, concepts, and explanations within the data through visual displays



(Lacey & Luff, 2009). At this stage, the charts serve to outline the nature and scope of the phenomena, define concepts, create typologies, and identify associations among themes to provide explanations for the findings (Lathlean, 2015). Ritchie and Lewis (2003) assert that the original research question and the themes emerging from the data determine the area of focus. This stage also necessitates techniques and diagrams to explore and visualize ideas from the data in developing and testing interpretations.

The application of framework analysis included developing a coding matrix from the interview transcripts. This approach required digitally recording and transcribing the interview sessions verbatim as a necessary first step. Lathlean (2015) recommended strategies, such as sharing transcripts with interviewees, to ensure the validity of the analysis. Consequently, interviewees received the transcripts to clarify the meaning of their responses, thereby facilitating internal and external validity. An extensive data coding and theme identification process followed data familiarization. According to Ritchie and Lewis (2003), using in-vivo codes (participant-specific words) maintains consistency with the data. Therefore, in-vivo terms used by participants became codes that subsequently formed categories. These categories and initial themes, resulting from grouping similar categories, served as the coding index for organizing the dataset. However, refinement of the coding index occurred throughout the data analysis as new insights emerged.

### **3.8.2 Excluded Approaches**

Among various approaches to qualitative analysis, Bryman (2012) identified analytic induction and grounded theory analysis as two primary strategies. Lathlean (2015) also recognized narrative analysis as another method of qualitative analysis. The analytic induction method reflects characteristics of positivism in research. According to Lathlean (2015):

Analytic induction is a process of analyzing data where the researcher tries to find explanations by carrying on with the data collection until no cases (referred to as

deviant or negative cases) are found that are inconsistent with a hypothetical explanation of a phenomenon. (p.474).

However, this study does not include establishing, confirming, or refuting a hypothesis. Therefore, it did not consider analytical induction as an approach to qualitative analysis. The research design for inductive approaches, such as grounded theory, is not strictly predetermined but develops in response to the resulting data and continuous analysis (Smith & Firth, 2011). Grounded theory analysis is inductive in that the resulting theory emerges from the data through a rigorous, structured analytical process (Lacey & Luff, 2009). The organized and detailed procedure for generating theory from data is the key appeal of grounded theory analysis. While other qualitative analysis approaches may be limited to simple interpretation or description, the purpose of grounded theory analysis is theoretical development (Lacey & Luff, 2009). Grounded theory analysis was not suitable as a data analysis approach for this study, given its goal of building and testing emerging theories.

Conversation, discourse, and narrative analysis are the most common methods for analyzing narratives. According to Lathlean (2015), these methods are suitable for more open forms of text data. Furthermore, their inquiry centers on the narrative itself, regardless of any focus on content, structure, or form. Approaches to narrative analysis, including conversation and discourse analysis, examine the use and significance of language along with techniques aimed at theory development (Smith & Firth, 2011), which were not appropriate for this study.

The derivation of themes is a unique type of analysis that is integrated into both framework and template analyses. Thematic analysis is one of the many ways to examine respondents' discourse regarding their experiences (Mahrer, 1988). It aims to identify significant themes that describe the phenomenon (Daly et al., 1997). This process includes identifying themes through “careful reading and re-reading of the data” (Rice & Ezzy, 1999, p.

258), leading to the development of important topics without the explicit generation of theory (Smith & Firth, 2011). Template analysis is a type of thematic analysis. It involves identifying themes or codes that synthesize and integrate important ideas, experiences, actions, and concepts based on data (Lathlean, 2015). The template approach requires defining a template before conducting in-depth data analysis (Fereday & Muir-Cochrane, 2006). Considering the overall aims of the analysis in addressing questions related to data security gaps in a regulated environment, this study did not necessitate template analysis. The dynamic and exploratory nature of the research questions demanded a more flexible analytical approach. Moreover, predefining a template could have limited the discovery of unexpected insights critical to tackling data security challenges.

### **3.8.3 Software for Qualitative Data Analysis**

Computer programs can simplify and potentially make data analysis more accurate, flexible, and comprehensive. However, they neither affirm nor negate the quality of qualitative research since they are merely tools that are as effective as the researcher using them. Neither the computer nor such programs can accurately interpret text or analyze data effectively (Bergin, 2011; Burnard et al., 2008). That task belongs to the researcher. The process of content and thematic analyses remains consistent, regardless of whether data are analyzed manually or with computer software, as it involves discovering themes and categories from the data (Burnard et al., 2008). Nonetheless, we opted to use a software package for data collection instead of manually analyzing the data.

Qualitative data analysis may be managed and assisted by a spreadsheet or computer-assisted qualitative data analysis software (CAQDAS) packages. CAQDAS, such as NVivo, aid researchers in analyzing qualitative data (Zamawe, 2015). Common CAQDAS include NVivo and ATLAS.ti. CAQDAS, such as ATLAS.ti7 and QSR NVivo10, provide tools for identifying and coding themes, processes, concepts, and contexts to develop or expand existing

theories (Lathlean, 2015). NVivo12 also includes coding retrieval and search functions (Smith & Firth, 2011). Burnard et al. (2008) maintained that CAQDAS simplifies data management, making it easier to handle. They further noted that these software packages are generally useful in qualitative data analysis for sorting, managing, and organizing large volumes of qualitative data; retrieving, annotating, and storing text; locating segments of data, phrases, and words; extracting quotes; and preparing diagrams. However, the CAQDAS that was available was too sophisticated for our needs in sorting and structuring the text efficiently. Furthermore, this study was not viewed as a significant undertaking that would require the analysis of a substantial amount of textual or multimedia data.

Microsoft 365 apps can be applied to qualitative data analysis. For example, Word and Excel were used to organize qualitative data (La Pelle, 2004; Ryan 2004). Additionally, Excel was employed for data preparation, analysis, and presentation (Meyer & Avery, 2009). Moreover, Word tables and macros were utilized for coding and retrieving interview data (Ose, 2016). Excel was also used for coding and thematically analyzing qualitative data (Bree & Gallagher, 2016). Given these applications, this study utilized Microsoft 365 apps to help organize, analyze, and extract insights from qualitative or unstructured data.

### **3.9 Data Collection and Analysis**

The study utilized a comprehensive approach to data collection and analysis. The data collection process involved gathering textual information from institutional documents and conducting interviews, which were recorded and transcribed. Also, combining two analytical methods allowed the study to obtain a richer and more detailed perspective on data security in Nigeria's pharmaceutical industry.

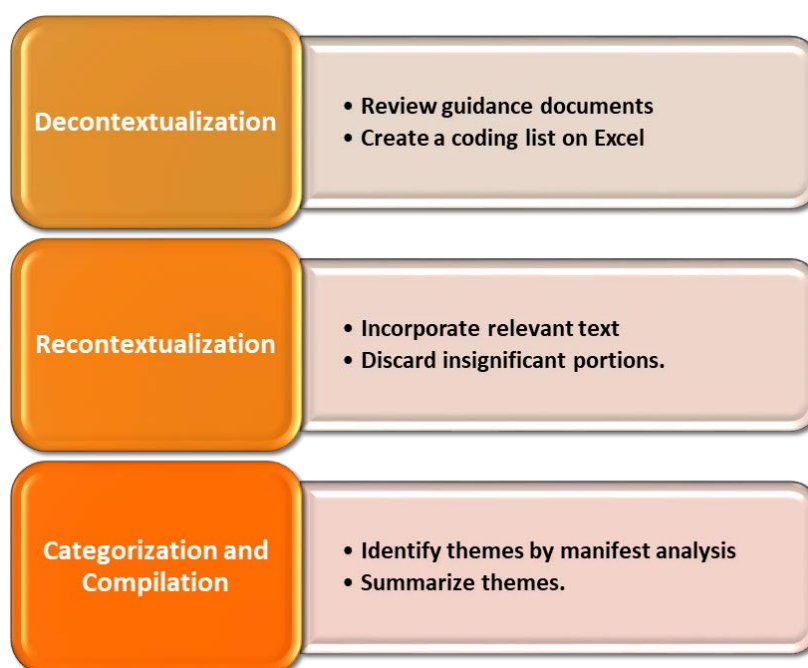
#### **3.9.1 Data Collection and Qualitative Content Analysis**

The data collected consisted of textual information extracted from data management guidance documents. Data analysis utilized qualitative content analysis with a deductive

approach. Consequently, analytic preconceptions guided the analysis process. By employing a predetermined coding framework derived from data security best practices, the categorization of textual information was achieved. The content analysis process, shown in Figure 35 and described below, aligns with the phases outlined by Bengtsson (2016) for qualitative content analysis.

**Figure 35**

*Qualitative Content Analysis Process*



**Note.** Based on the content in “How to Plan and Perform a Qualitative Study using Content Analysis,” by M. Bengtsson, 2016, *NursingPlus Open*, 2, pp. 8-14.

(<https://doi.org/10.1016/j.npls.2016.01.001>).

**Decontextualization.** Decontextualization involved reviewing the guidance documents to familiarize oneself with the data before breaking it down into smaller units of meaning. A coding list created in Microsoft Excel prior to analysis aided in identifying themes for each meaning unit.

**Recontextualization.** Recontextualization involved verifying that all aspects of the

content were addressed regarding the research questions. A review of the original text, along with the coding list and meaning units, led to the inclusion of relevant text that aligned with the study's aim and the exclusion of irrelevant ones.

**Categorization and Compilation.** The categorization process involved identifying themes at a descriptive manifest level. The primary data collection method, document analysis, required consideration of manifest analysis. Manifest analysis ensured adherence to the original meanings and contexts provided by health authorities. With manifest analysis, themes either directly reflected the data from which they originated or aligned with the coding units. The compilation involved creating a table that not only summarized the identified themes but also clarified the process from raw data to results, ensuring the quality and transparency of the work analysis.

### **3.9.2 Data Collection and Thematic Analysis**

The study required an alternative data analysis method from a different data source to validate the findings. This triangulation process involved processing and analyzing interview data through thematic analysis. The thematic analysis used an inductive approach, where codes facilitated the identification of concepts that organized the data into blocks (Bengtsson, 2016). Coding data for analysis ensured that the insights collected during interviews guided the analysis process (Bree & Gallagher, 2016). The inductive approach initially identified themes at the semantic level, focusing on the surface meanings of the data, and then advanced to the latent level to reveal underlying ideas and concepts within the data. The data analysis process, shown in Figure 36 and outlined below, follows the phases of thematic analysis described by Ose (2016).

**Collect the Interview Data.** The data collected comprised interview data in text format. Gathering this data involved recording all interviews and saving the audio output in files. Although the interview guide was followed, there were instances during the interviews

when the discussions deviated from the main topic, offering valuable insights into the interviewees' perspectives of relevance and importance. According to Ose (2016), this method reflects the unstructured nature of interview data.

**Figure 36**

*Thematic Analysis Process*



**Note.** Based on the content in “Using Excel and Word to Structure Qualitative Data,” by S.

O. Ose, 2016, *Journal of Applied Social Science*, 10(2), pp. 147-162.

(<https://doi.org/10.1177/1936724416664948>).

**Transcribe the Audio Recordings.** Transcription involved converting all audio recordings into written text and saving them in Word format to enable analysis. Each interview's data was stored in a separate Word file labeled with the respondent's initials. Colons not only tabbed delineate the Word file, but 'I:' and 'R:' also clearly distinguished between the interviewer's and respondents' quotes, respectively.

**Transfer the Text from Word Documents to Excel Spreadsheets.** This phase involved transferring the text from Word documents to Excel spreadsheets. A blank workbook created in Excel and saved as DataAnalysis.xlsx enabled the copying and pasting of each interview onto a separate sheet.

**Code in Excel.** Coding the interviews in Excel required maintaining separate sheets for each interview throughout the coding process. A detailed coding list created consecutively on a separate sheet called "Codes", shown in Figure 37, included columns for code descriptions and corresponding code numbers (1, 2, 3, etc.). A separate code of "999" indicated insignificant quotes.

**Figure 37**

*Coding List for Interview Data*

45	<u>Undetected data alteration</u>	45
46	<u>Anomaly-based log analysis</u>	46
47	<u>Limited scope of log monitoring</u>	47
48	<u>Erasure of audit trails</u>	48
49	<u>Disabled audit trail functionality</u>	49
50	<u>Device security informed by host-based security app.</u>	50
51	<u>IT security assessment and incident response.</u>	51
52	<u>Under-resourced data security audit</u>	52
53	<u>The inaction of the auditee and management to audit recommendations</u>	53
54	<u>Insignificant</u>	999
55		

**Sort the Coded Interviews.** Two columns, shown in Figure 38, identified the respondents: organizational code and respondent code. Also, a sequential variable in another column, numbered 1, 2, 3, and so forth, was assigned to each interview session to maintain the interview structure. Linking these columns to the quotes involved combining the interviews on the same sheet and using the concatenate function. The code list, included at the bottom of the same sheet as the coded combined interviews, served as the headings when sorting the interview data by Columns G, H, A, B, and C in that order.



**Figure 38***Sorted Interview Data*

	A	B	C	F	G	H
1				Absence of data classification scheme	1	
2	OrganizationA	VIA	243	So, there is no data classification scheme?(OrganizationA_VIA_243)	1	
				This is the way it is for now but because most managers already know information that is confidential, they don't share	1	

**Transfer Quotes and References to Word.** Creating a new blank document in Word made it easier to transfer quotes and references from Excel while keeping their format intact. A second review removed insignificant quotes from the Excel file to reduce data volume before transferring the remaining content to Word. Analyzing the quotes necessitated converting the resulting table into standard text.

**Analyze Interview Data.** The data analysis involved multiple data passes, thematic data categorization, reflection, synthesizing, and condensation to capture the essence of the phenomenon and facilitate the interpretation of findings. This iterative process, driven by data, led to the abstraction of themes. Thematically structuring the codes required selecting the Word “View” menu, the “Outline”, “Show Level 2”, and then dragging and dropping these codes, along with their text, below each identified theme. This process resulted in the organization of codes into themes, which led to the structuring of interview data by thematic area.

### Summary

Chapter 3 provided a detailed account of the research methods and data collection strategies used to explore data security within Nigeria’s pharmaceutical industry. Guided by an interpretivist stance and nominalist ontology, the study adopted a qualitative approach to investigate complex organizational issues and subjective experiences. This approach was selected due to the limited empirical literature on data security in the pharmaceutical sector and the need to generate context specific insights.

A multiple case study design was implemented, justified by the requirement to examine real world phenomena within their regulatory context. This design enabled an intensive,

holistic exploration of data security practices across several drug manufacturing organizations. Multiple cases allowed for both within case and cross case comparisons, improving the robustness and credibility of findings. The research design deliberately excluded phenomenology, narrative, grounded theory, and ethnography, as these methods were deemed less aligned with the study's objectives.

Triangulation was a key feature of the methodology. Data were collected and analyzed through document analysis and semi structured interviews, reducing bias and enhancing validity by corroborating evidence from different sources. Triangulation offered a comprehensive perspective, confirmed findings across datasets, and provided deeper insights into data security gaps. The study applied methodological triangulation, integrating two qualitative methods, and also used person and space triangulation to compare data from multiple organizations and roles.

Document analysis focused on regulatory and institutional documents from recognized authorities, such as WHO and PIC/S, offering historical, contextual, and technical perspectives. This method employed qualitative content analysis using a predetermined coding framework based on data security controls. The analysis involved decontextualization, recontextualization, categorization, and compilation to systematically extract relevant insights.

Semi structured interviews complemented document analysis to address the inherent limitations of written records. Participants included IT/ information systems managers, system administrators, information/cyber security analysts, and DPOs from five pharmaceutical organizations. These interviews, conducted remotely through synchronous video conferencing due to COVID 19 restrictions, provided rich, first hand accounts of data management practices.

Purposive sampling guided the selection of organizations and participants. Typical case, critical case, and intensity sampling techniques targeted organizations with active WHO cGMP prequalification processes and experts with extensive data security experience. This

sampling approach ensured data saturation, with 31 professionals interviewed, leading to stable and repetitive patterns by the 28th session.

Data analysis combined content analysis of documents with thematic analysis of interview transcripts. The framework approach enhanced the rigor of thematic analysis by following structured stages: familiarization, establishing a thematic framework, indexing, charting, and mapping and interpretation. This process generated transparent audit trails, enabling systematic coding and theme development.

Ethical considerations were prioritized throughout the research process. Gatekeeper permissions, informed consent, and confidentiality safeguards were strictly observed. Data were securely stored with encryption, pseudonyms were used to anonymize participants and organizations, and participants retained the right to withdraw at any stage.

Overall, Chapter 3 demonstrated a rigorous and ethically grounded methodology. Through its multiple case design, triangulation of methods, purposive sampling, and structured data analysis, the study achieved a comprehensive and credible examination of data security practices in Nigeria's pharmaceutical industry.

## **CHAPTER 4: DISCUSSION OF RESEARCH FINDINGS**

The purpose of this study is to investigate data security gaps in the pharmaceutical industry. These gaps may be causal factors for data security breaches in these regulated environments. An analysis of data security gaps should reveal areas of drug manufacturing that need improved security.

In the contemporary landscape of empirical studies and research methodologies, rigorously assessing the reliability and trustworthiness of data is a crucial cornerstone to ensure the validity and credibility of research findings. Chapter 4 navigates the complex intricacies of this critical assessment, offering an in-depth exploration of data reliability, trustworthiness, research findings, and their evaluation aspects. The chapter opens with Section 4.1, which explores the concepts of reliability and validity, emphasizing the importance of consistent and stable data to support credible research. It outlines the specific methods used to establish the reproducibility and dependability of the collected data across different contexts. In Section 4.2, the discussion advances to the trustworthiness of data, examined through four key dimensions: confirmability, credibility, dependability, and transferability (Sections 4.2.1–4.2.4). This segment details the strategies employed to safeguard the integrity of the findings, including triangulation, member checks, iterative questioning, reflexivity, reflective commentary, and debriefing sessions (Section 4.2.2). These tools collectively enhance methodological rigor, reduce bias, and ensure that the data accurately reflects participants' perspectives. The chapter proceeds to the results and evaluation of findings in Section 4.3, which forms the core analytical body of the research. Here, the discussion is segmented into four main areas. Section 4.3.1 investigates data security measures and gaps in reference guidelines, including topics such as data management, inventory, flows, access control, retention, backup, recovery, disposal, encryption, and the monitoring of service providers. These findings reveal inconsistencies and unspecified elements that weaken regulatory guidance. Section 4.3.2 examines data security

gaps in drug manufacturing practices, highlighting real-world challenges such as poor data classification, ineffective risk assessments, immature tech-driven data governance, software integrity issues, network and USB security vulnerabilities, and problems with validation and system monitoring. This section emphasizes the risks posed by decentralized global operations and outdated IT security practices. In Section 4.3.3, the focus shifts to the alignment between regulatory guidelines and implementation. The analysis compares prescribed controls with their application in practice, shedding light on areas of compliance, partial implementation, or misalignment across critical components like access controls, data retention, recovery protocols, classification, encryption, and third-party oversight. Finally, Section 4.3.4 deepens this evaluation through a root-cause analysis of the identified data security gaps, uncovering the underlying systemic factors that contribute to weaknesses in the pharmaceutical industry's data protection framework. This chapter, as a whole, highlights the importance of data reliability, trustworthiness, and evaluation in producing meaningful research outcomes, culminating in insights that set the stage for further analysis and discussion.

#### **4.1 Reliability and Validity of Data**

A measure must be both reliable and valid to accurately represent the concept it is intended to assess. However, a measure must be reliable before it can be considered valid. Reliability in quantitative research pertains to the overall accuracy and consistency of the data collection method or measurement tool used in a research study (Adeyemi, 2024). It emphasizes the need for similar results if other researchers replicate a survey on the same sample shortly thereafter, provided the situational conditions remain unchanged. Shou et al. (2022) refer to this as test-retest reliability. However, qualitative research approaches require active involvement, as the researcher typically designs the study and collects, interprets, and reports the data (Topping, 2015). Reliability issues can particularly emerge when interviews are utilized to gather qualitative data. Such issues may stem from the manner in which the

interview is conducted or from the researcher's influence. Tod (2015) asserts that the level of reliability refers to the accuracy and coherence of data collection necessary for an interview. She contends that achieving reliability is more demanding in the context of in-depth, semi-structured, or unstructured interviews as opposed to structured interviews. Semi-structured interviews are interactive and flexible, fostering a deeper understanding of the participant's social constructs and the representation of the research phenomenon. Nonetheless, a well-designed interview schedule can enhance the rigor of the findings (Lincoln & Guba, 1985).

The validity of a study concerns the extent to which the data is considered "true." Quality research often distinguishes between internal and external validity. Internal validity refers to the degree to which research results reflect reality (Lathlean, 2015; Vu, 2021), while external validity pertains to how concepts and abstractions apply to all groups (Findley et al., 2021). However, interpretivism, the epistemology that underpins qualitative research, is less focused on questions of validity and aims to provide a rich portrayal of life and behavior within groups or organizations (Easterby-Smith et al., 2015). Kirk and Miller (1986) argue that validity in qualitative research "is ... a question of whether the researcher sees what he or she thinks he or she sees" (p. 21). According to Tod (2015), the challenge is to demonstrate that the findings accurately reflect the participants' representation of the subject and are not based on bias or misinterpretation. Therefore, we examined quality criteria that enabled us to demonstrate the rigor and trustworthiness of qualitative research.

## **4.2 Trustworthiness of Data**

Reliability and validity are concepts used in the assessment of quantitative research. However, these concepts are inappropriate for evaluating qualitative research (Mays, 2000). Shenton (2004) emphasizes that validity and reliability cannot be approached in the same manner in qualitative research. According to Vu (2021), providing estimates of data reliability

is rare in qualitative research. Additionally, some researchers argue that validity and reliability are not suitable for qualitative research and prefer to use terms like "quality" or "trustworthiness" when discussing data (Welsh, 2002). Nonetheless, researchers should conduct thorough and transparent qualitative research and data analysis (Kirk & Miller, 1986; Lincoln & Guba, 1985; Miles & Huberman, 1994). Lincoln and Guba (1985; 1989) proposed an alternative set of criteria to evaluate qualitative research based on the concepts of trustworthiness or authenticity. According to Shenton (2004), these constructs, shown in Figure 39 align with the criteria used by positivist investigators: confirmability (instead of objectivity); credibility (instead of internal validity); dependability (instead of reliability); transferability (instead of external validity/generalizability).

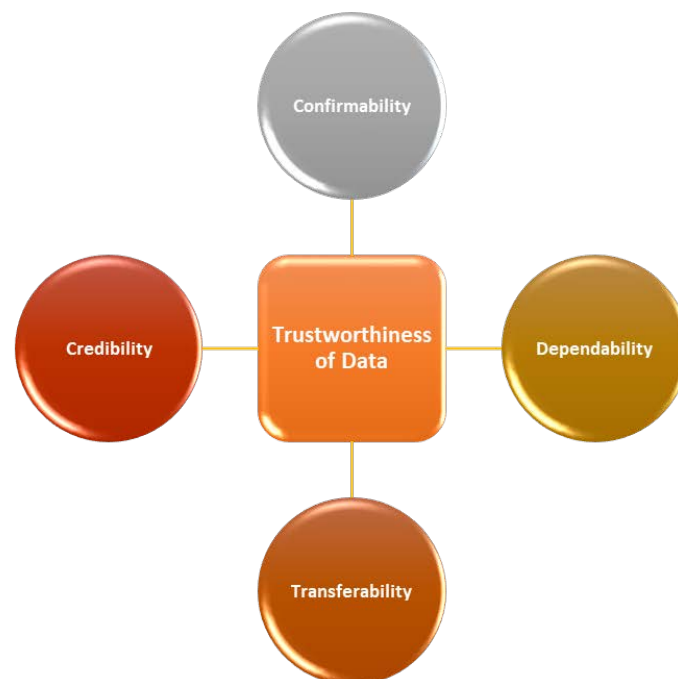
#### **4.2.1 Confirmability**

Researchers have the potential to introduce bias and influence every step of the research process. Confirmability is a qualitative researcher's comparable concern for objectivity, similar to objectivity in quantitative research (Shenton, 2004). It refers to the degree of objectivity, defined as an agreement among two or more individuals who review findings for accuracy and meaning (Ahmed, 2024; Beck, 2009; Nassaji, 2020). Confirmability necessitates that data, findings, and interpretations are interrelated (Topping, 2015). Therefore, steps must be taken to demonstrate that results stem from the data rather than a researcher's predispositions; in other words, the study findings should reflect the insights and experiences of informants rather than the researcher's characteristics and preferences (Shenton, 2004). Miles and Huberman (1994) argue that a key criterion of confirmability is how openly researchers acknowledge their predispositions. According to Carolan (2003), recognition of the researcher's influence, and consequent scrutiny, in qualitative research faces the same amount of critical examination as the research itself. Shenton (2004) asserts that the beliefs guiding the researcher's decisions and the methods

used must be transparent in the research report. He also suggests that researchers should explain their preference for certain approaches over others and acknowledge any weaknesses inherent in the techniques employed. For this reason, we documented field notes detailing observations, statements, and actions taken during the research, along with memos elucidating our interpretations of what we observed. These notes and memos became data.

**Figure 39**

*Constructs of Data Trustworthiness*



**Note.** Based on the content in “Strategies for Ensuring Trustworthiness in Qualitative Research Projects,” by A. K. Shenton, 2004, *Education for Information*, 22, pp. 63-75. (<https://doi.org/10.3233/EFI-2004-22201>).

Furthermore, the audit trail was instrumental in establishing the confirmability of this study. Shenton (2004) confirms that audit trails allow an observer to trace the research process step by step through the decisions made and procedures followed. Audit trails also enable researchers to document and clarify each step and decision made during data coding and analysis (Nassaji, 2020). Consequently, this study demonstrated confirmability by outlining



every step in the data analysis. This approach minimized bias and ensured that the findings accurately reflected participants' responses.

#### 4.2.2 Credibility

Credibility measures the accuracy of a study's findings or the truth value of qualitative research. It reflects the alignment between participants' opinions and their representation by the researcher (Topping, 2015). Beck (2009) connects credibility with trust in the data and confidence that the findings are true. Merriam (1998) posits that the qualitative researcher's equivalent concept of internal validity, i.e., credibility, addresses how well a study's findings align with reality. Shenton (2004) asserts that the credibility of qualitative research, to some extent, hinges on the credibility of the researchers. Consequently, we provided the researcher's background, qualifications, and experiences in this study. In addition to the researcher's biography, we also employed other concepts: triangulation, member checks; prompts, probes, and iterative questioning; reflexivity and reflective commentary; and debriefing sessions as procedures to enhance the credibility of this study.

**Triangulation.** Triangulation is a crucial concept in qualitative analysis. It not only enhances credibility but also reduces the impact of the investigator's bias. Triangulation bolsters credibility by employing different methods, sites, and types of respondents (Ahmed, 2024; Nassaji, 2020). In this study, various methods of triangulation were utilized. According to Brewer and Hunter (1989) and Guba (1981), combining different methods compensates for each method's limitations while leveraging their unique advantages. Alongside interviews, supplementary data were gathered from guidance documents to clarify the gaps in data security. This combination constituted a form of data triangulation through diverse sources. Lathlean (2015) notes that triangulating data sources involves comparing information about a phenomenon collected from distinct phases of fieldwork or accounts from multiple participants and the researcher. She suggested that when various types of data converge on the same

conclusion, it strengthens confidence in those conclusions. Additional forms of triangulation included utilizing a wide range of informants. Triangulation of this sort involves corroborating individual views and experiences against others (Shenton, 2004). This approach creates a comprehensive understanding of the attitudes, needs, or behaviors derived from the contributions of those studied. In Lathlean's (1997) research on lecturer practitioners, presenting her findings to participants served as a means of validating their accounts and a method of triangulation. She compared and contrasted the accounts generated for each participant and assessed the consistency among the cases. This study also employed triangulation by incorporating various data sources and informants.

Additionally, site triangulation can be achieved by involving informants from multiple organizations to reduce the influence of specific local factors tied to a particular institution on the study. According to Shenton (2004), when similar results arise in different settings, they may be perceived as more credible by the reader. He also recommended sampling a range of individuals from various organizations to provide the diversity that underpins indirect reality. Hence, this study employed triangulation by incorporating various sites.

**Member Checks.** Researchers must validate study findings with participants. A critical test for qualitative research accounts is whether individuals whose beliefs and behaviors are supposed to be reported in the accounts recognize those accounts as valid (Lathlean, 2015). Guba and Lincoln (1985) argue that member checks are the most important provision to enhance the credibility of a study. The focus of member checks is on whether informants feel their words accurately reflect their intended meaning. According to Shenton (2004), checks on the accuracy of the data occur "on-site" during and at the conclusion of data collection. Lathlean (2015) and Nassaji (2020) suggested strategies, such as sharing transcripts with respondents to ensure that the analysis is valid. Consequently, those interviewed were provided with transcripts of the dialogues in which they participated, allowing them to read the

interview transcription, verify the data generated, and clarify the meaning of their responses, thus ensuring the validity of the analysis.

**Prompts, Probes, and Iterative Questioning.** We incorporated prompts, probes, and iterative questioning specifically into the interview sessions to uncover intentional lies, contradictions, and repressed experiences of the participants. Probes are one of the strategies for obtaining detailed data (Shenton, 2004). According to Tod (2015), probes and prompts yield richer, deeper data and reveal layers of meaning. Using probes and prompts effectively can help achieve the right balance of depth and breadth in questioning (Legard et al., 2003). Iterative questioning is another strategy where the researcher revisits issues previously identified by an informant and extracts related data using rephrased questions (Shenton, 2004). By employing prompts, probes, and iterative questions, we dismissed suspicious data when contradictions arose and falsehoods were detected.

**Reflexivity and Reflective Commentary.** Qualitative researchers are integral to the research process, and their assumptions, beliefs, and past experiences shape this process. Furthermore, qualitative research offers flexibility and considers context, detail, and complexity (Mason, 2002). However, the subjective nature of an approach where the researcher and the research are closely intertwined presents challenges (Topping, 2015). Qualitative research emphasizes the importance of reflectivity in addressing this challenge, as researchers acknowledge that their social identity and background influence the research process (Lathlean, 2015). Reflexivity or critical self-reflection on the research process and data interpretation, serves as an essential tool for qualitative researchers (Ahmed, 2024; Schwandt, 1997). According to Lathlean (2015), reflexivity demands careful thought from researchers to consider how they impact every facet of the research process, particularly the interpretation of research findings. Consequently, we made a deliberate effort to clarify and explain our contributions to the research so that the analyses could be viewed from this perspective.

Additionally, the investigator should assess the project as it evolves. Shenton (2004) indicates that such evaluations may be conducted through thoughtful commentary, part of which can focus on the effectiveness of the employed techniques. He added that reflective commentary aids in documenting the researcher's initial impressions from each data collection session, as well as identifying trends emerging from the collected data and developing theories. Lincoln and Guba (1989) proposed a progressive subjectivity in which researchers monitor their constructions as they evolve. They argue that reflective commentary is crucial in promoting progressive subjectivity and establishing credibility. Hence, reflective comments on emerging trends, theories, and analytical methods informed the research reports.

**Debriefing Sessions.** Debriefing sessions can draw on the experiences and insights of the researcher's superiors. According to Shenton (2004), these collaborative sessions provide researchers with an opportunity to discuss alternative approaches with the leaders of a research project or those overseeing it, who may point out gaps in the proposed action plan. He also mentioned that these meetings offer feedback to the investigator, allowing them to test their ideas and interpretations, and input from others can help researchers uncover their preferences and biases. Therefore, this study used debriefing sessions between the investigator and the research supervisor to enhance its credibility.

#### **4.2.3 Dependability**

Dependability is closely linked to credibility. Lincoln and Guba (1989) argue that, in practice, demonstrating the latter significantly contributes to ensuring the former. Dependability relates to the transparency of the decision-making and research process (Ahmed, 2024; Nassaji, 2020; Topping, 2015). It also emphasizes the stability of data over time and across various contexts and conditions (Ahmed, 2024; Beck, 2009). Dependability measures or illustrates the coherence and reliability of a study's results. Shenton (2004) provides a thorough methodological explanation and an extensive overview of the study

processes, allowing prospective researchers to replicate the work to achieve similar results. Consequently, we documented the exact methods used for data collection, analysis, and interpretation in a way that the study can theoretically be reproduced by other researchers and yield coherent results. This comprehensive coverage also allows readers to assess the extent to which appropriate research practices were adhered to. To enhance readers' understanding of the methods and their effectiveness, we followed Shenton's (2004) recommendations and included sections dedicated to research design and implementation: a description of what was planned and executed at the strategic level; operational details of data collection, considering the specifics of what was done in the field; and a thoughtful evaluation of the project, appraising the effectiveness of the inquiry process undertaken.

#### **4.2.4 Transferability**

Transferability focuses on the applicability of study results to other groups. It refers to the appropriateness of the description in determining similarity to other situations, allowing findings to be transferred (Topping, 2015). Beck (2009) describes transferability as the ability of findings to apply to other settings. As its name implies, transferability measures whether, and to what extent, study findings apply to various contexts, settings, and circumstances, and it can also be viewed as generalizability. Ahmed (2024), Firestone (1993), Lincoln and Guba (1985), and Nassaji (2020) suggest that investigators ensure readers have enough contextual information about the fieldwork sites to facilitate such transfer. By providing enough details about the field site's context, readers can determine if the prevailing environment resembles another situation they are familiar with and if the conclusions can be appropriately applied to other settings. Cole and Gardner (1979) and Marchionini and Teague (1987) further stressed the importance of communicating the study's boundaries to the reader. Shenton (2004) recommended addressing specific areas upfront to outline these boundaries: the number of organizations participating in the study and their locations; restrictions regarding the types

of individuals who provided data; the number of participants; the methods used for data collection; the number and duration of data collection sessions; and the timeline for data collection. He argued that this additional information should be considered before transference. Shenton (2004) also emphasized the need to provide a detailed description of the phenomenon being studied to enable readers to fully understand it, thus allowing for comparison of the instances of the phenomenon described in the research report with those they observe in their situations. Ahmed (2024) recommended offering detailed information on the sampling techniques and participant selection criteria to help assess whether the findings could be relevant or transferable to similar groups or settings beyond the study's original context. To demonstrate transferability in this qualitative research, this study utilizes thick descriptions, requiring adequate details about the site, participants, and methods or procedures for gathering data during the study. Moreover, the study clearly outlines the sampling process and criteria, helping to illustrate the potential applicability of its findings to other contexts. In addition, the results were presented in a way that allows readers to compare their situation with that of the study.

#### **4.3 Results and Evaluation of Findings**

The recognition of data as a valuable resource in decision-making processes is increasingly acknowledged by business and IT leaders. Scholars have emphasized the importance of data governance in effective data management, highlighting the necessity for a structured approach regarding data security. Understanding and addressing gaps in data security are crucial given the growing reliance on IT systems, data, and the potential economic and social repercussions of data breaches. Over the past decade, there has been a notable issue with data breaches in drug manufacturing operations, causing significant economic damage to various countries. These breaches have resulted in financial losses, theft of IP, and violations of GMP regulations. Despite guidance from health authorities and efforts to improve data

management standards, security breaches continue to occur, threatening sensitive data and the pharmaceutical supply chain. The persistent threat of data breaches underscores the need for research to identify and address data security vulnerabilities in drug manufacturing.

This qualitative study aimed to explore data security gaps in drug manufacturing and identify sustainable solutions to address them. By analyzing existing guidelines and practices, the study sought to identify gaps, assess the alignment of management practices with published guidelines, uncover causal factors contributing to these deficiencies, and propose recommendations for enhancing data security in drug manufacturing. The study's significance lies in its ability to illuminate and address data security challenges in drug manufacturing—protecting sensitive assets such as patient records, proprietary formulas, and research data—thereby enriching knowledge on data governance and influencing policy and practice within Nigeria's highly regulated pharmaceutical industry. The study formulated three research questions to uncover data security gaps in drug manufacturing practices, assess the adequacy of data security provisions in health authorities' guidance, and evaluate the alignment of industry practices with published guidelines. These questions shaped the investigation into the diverse nature of data security challenges in the pharmaceutical industry, facilitating a comprehensive understanding of the issue. This study sought to enrich data governance by introducing a data security model that builds on prior research, guides regulators and pharmaceutical organizations in strengthening data management and integrity, and offers governments a framework to enhance cybersecurity and prevent data security failures in drug manufacturing.

Given the exploratory nature of the research, a qualitative research approach rooted in an interpretivist paradigm was employed to investigate the complexity of data security in pharmaceuticals. The choice of qualitative research, particularly through case studies, offered a more nuanced understanding of the data security challenges encountered in the

pharmaceutical industry. By concentrating on a specific context—the Nigerian pharmaceutical sector—this multiple case study approach enabled an in-depth exploration of the intricacies and dynamics surrounding data security standards and practices. This approach yielded comprehensive and contextually relevant insights that may have been overlooked in more generalized research designs. The research design employed triangulation to enhance the credibility of the findings and to achieve a comprehensive understanding of the research phenomenon. Triangulation integrated multiple data collection methods, including document analysis and semi-structured interviews. Document analysis facilitated a thorough review of existing guidance documents concerning data security in drug manufacturing. Conducting semi-structured interviews with subject matter experts from drug manufacturing organizations involved in implementing and reviewing data security controls provided invaluable firsthand insights into the data security management practices and challenges within the industry. These methods were considered appropriate for exploring the principles and recommendations of regulatory bodies, as well as the perceptions and subjective experiences of practitioners regarding data security in the pharmaceutical sector. Through the use of rigorous research methods, the study offered meaningful insights into the risk and security sensitive pharmaceutical data

Employing purposive sampling allowed for the selection of institutional documents containing data management provisions, organizations operating in a regulated environment, and participants with relevant expertise and experience related to data security in drug manufacturing. This targeted approach ensured that the collected data were highly relevant to the research questions, enriching the analysis with focused insights from industry insiders. Table 8 and Table 9 show the demographic characteristics of the case organization/respondents and published standards, respectively. A key demographic indicator is the healthy mix of 84% men and 16% women among the 31 participants. Additionally, 61% of participants were within



the 31-40 age range. Also, all participants were from the Nigerian pharmaceutical industry, and 61% held mid-level positions within their organizations. Another key characteristic is that the participants' organizations were certified as ISO 9001. As ISO 9001-certified organizations, training programs for quality management systems were likely offered to employees. However, none of these organizations were ISO 27001 certified. Therefore, employees may not have been familiar with information security management systems.

**Table 8**

*Demographics of Respondents*

Demographic characteristic	Count (n)/Percent (%)
Gender	
Male	26 (84)
Female	5 (16)
Other	0 (0)
Age	
Below 20	5 (16)
21-30	19 (61)
31-40	4 (13)
41-50	3 (10)
Above 50	0 (0)
Highest degree/Level of education	
GCE/SSCE	0 (0)
Ordinary National Diploma	0 (0)
Higher National Diploma	0 (0)
Bachelor's Degree	17 (55)
Post-Graduate Diploma	3 (10)
Master's Degree	11 (35)
Ph.D. or higher	0 (0)
Position in the organization	
Junior level	5 (16)
Middle level	19 (61)
Senior level	7 (23)
Years in the organization	
2-5 years	0 (0)
5-10 years	10 (32)
Above 10 years	21 (68)
Role in the organization	
IT Manager/IS Operations Manager	5 (16.1)
System Administrator	13 (42)
Information/Cyber Security Analyst	8 (25.8)
Data Protection Officer	5 (16.1)
ISO 9001 certified organization	
Yes	5 (100)
No	0 (0)
ISO 27001 certified organization	
Yes	0 (0)
No	5 (100)

Ethical considerations were paramount throughout the research process. Measures were put in place to ensure the confidentiality of participants, informed consent, and responsible data management. Adhering to ethical guidelines emphasized the researcher's commitment to maintaining integrity and respect when engaging with participants and handling sensitive data. Ethical assurances were integrated in the study procedures, which included a range of tasks, such as literature review, determining methodology and design, obtaining ethical approval, recruiting participants, collecting data, validating data, analyzing and interpreting data, and reporting. Data analysis was also triangulated and employed a framework approach that featured systematic procedures including familiarization, indexing, charting, mapping, and interpretation.

**Table 9**

*Health Authorities' Guidance Documents Reviewed*

Author	Title	Publication date
World Health Organization	"Guidance on Good Data and Record Management Practices"	2016
World Health Organization	"Guidance on Data Integrity"	2021
Pharmaceutical Inspection Co-operation Scheme (PIC/S)	"Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments"	2021

Qualitative content analysis and thematic analysis techniques facilitated the identification of patterns and themes within the data, providing a structured yet flexible method for data analysis. Comparative analysis enabled the evaluation of congruence between themes identified from qualitative content analysis and thematic analysis. The exclusion of certain analytical approaches, such as analytic induction, grounded theory, and narrative analysis, arose from their incongruence with the research objectives and the nature of the collected data. Data collection encompassed gathering textual data from institutional documents and conducting qualitative content analysis using a deductive approach, employing a coding

framework grounded in data security controls. Subsequently, thematic analysis of interview data through an inductive approach led to the abstraction of themes and the organization of interview data by thematic areas.

#### 4.3.1 Data Security Measures and Gaps in Reference Guidelines

An analysis of content examined data security provisions in published guidelines, with codes derived from controls informed by COBIT and the CSCs. The analysis focused on guidance documents from two globally recognized health authorities—PIC/S (2021) and WHO (2016). In addition, the WHO (2021) guideline, which superseded the 2016 version during the study, was also included in the content analysis. Table 10 summarizes the findings from the content analysis of the three guidance documents. An evaluation of the findings revealed both data security provisions and gaps.

**Table 10**

*Evaluation of Data Management Guidelines based on Data Security Controls*

<b>Coding Frame (Data security control)</b>	<b>Meaning Unit (Provision for data security)</b>	<b>Theme</b>
Data management	<ul style="list-style-type: none"> <li>• “The data governance program should include policies and procedures addressing data management” (WHO, 2021, p.141).</li> <li>• “A data management program developed and implemented upon the basis of sound quality risk management principles is expected to leverage existing technologies to their full potential” (WHO, 2021, p. 178).</li> <li>• Data management encompasses “all those activities performed during the handling of data including but not limited to data policy, documentation, quality, and security” (PIC/S, p .3).</li> </ul>	<ul style="list-style-type: none"> <li>• Data governance program</li> <li>• Technology-backed data management.</li> <li>• Data policies, documentation, quality, and security.</li> </ul>
Data inventory	<ul style="list-style-type: none"> <li>• “All computerized systems in use” (PIC/S, 2021, p.34)</li> </ul>	<ul style="list-style-type: none"> <li>• No provision</li> </ul>
Data flow	<ul style="list-style-type: none"> <li>• The document “the system architecture and data flow, including the flow of electronic data and all associated metadata, from the point of creation through archival and retrieval” (WHO, 2016, p.185).</li> <li>• Provide “a graphical representation of the “flow” of data through an information system” (PIC/S, 2021, p. 61).</li> </ul>	<ul style="list-style-type: none"> <li>• Data flow documentation</li> <li>• Data flow visualization</li> <li>• Data flow map</li> <li>• Data flow evaluation</li> </ul>

Coding Frame (Data security control)	Meaning Unit (Provision for data security)	Theme
	<ul style="list-style-type: none"> <li>“The creation and assessment of a data flow map may be useful in understanding the risks and vulnerabilities of computerized systems, particularly interfaced systems” (PIC/S, 2021, p. 32)</li> <li>Evaluation of data flows (PIC/S, 2021)</li> </ul>	
Data access control lists	<ul style="list-style-type: none"> <li>Prohibit “unauthorized access to, changes to, and deletion of data” (PIC/S, 2021, p.40)</li> <li>Allow “only people with the appropriate authorization to alter a master processing formula” (WHO, 2016, p.177).</li> </ul>	<ul style="list-style-type: none"> <li>Authorized access</li> </ul>
Role-based access control	<ul style="list-style-type: none"> <li>“Systems should support different user access roles (levels) and assignment of a role should follow the least-privilege rule” (PIC/S, 2021, p.40).</li> <li>“Access and privileges should be under the role and responsibility of the individual with the appropriate controls to ensure data integrity” (WHO, 2021, p.149).</li> </ul>	<ul style="list-style-type: none"> <li>Least-privilege rule for user access</li> <li>Role-based access</li> </ul>
Data retention	<ul style="list-style-type: none"> <li>A data retention process that “records all data, (including metadata) for all activities which directly or indirectly impact on all aspects of the quality of medicinal products” (PIC/S, 2021, p.18).</li> <li>A records retention period in which “original records should be complete, enduring and readily retrievable and readable” (WHO, 2016, p.183).</li> <li>Policies and procedures for the retention of data and audit trails under a required or defined retention period (WHO, 2021, p.150).</li> </ul>	<ul style="list-style-type: none"> <li>Data retention process</li> <li>Records retention period</li> <li>Policies and procedures for data and audit trail retention according to specified retention periods.</li> </ul>
Data backup	<ul style="list-style-type: none"> <li>Routine backups in remote locations as a safeguard in case of disasters (PIC/S, 2021; WHO, 2016; WHO, 2021).</li> <li>Validation of the backup and restoration processes (WHO, 2021).</li> <li>Periodic backup and archiving of data by written procedures (PIC/S, 2021).</li> </ul>	<ul style="list-style-type: none"> <li>Routine backups</li> <li>Backup and restoration validation process.</li> <li>Documented procedures for periodic backup and archiving of data</li> </ul>
Data recovery process	<ul style="list-style-type: none"> <li>“Consideration should also be given to ensuring complete and timely data recovery in the event of a disaster” (PIC/S, 2021, p.8).</li> </ul>	<ul style="list-style-type: none"> <li>Complete and timely data recovery</li> </ul>
Data recovery test	<ul style="list-style-type: none"> <li>“Periodic tests to verify the ability to retrieve archived electronic data from storage locations” (WHO, 2016, p.204).</li> <li>Test the ability to retrieve data from storage locations during the validation of the electronic archive. (WHO, 2016)</li> <li>Periodic assessment of the ability to retrieve archived electronic data from</li> </ul>	<ul style="list-style-type: none"> <li>Periodic data recovery test from archive, third-party storage, and storage locations</li> </ul>

Coding Frame (Data security control)	Meaning Unit (Provision for data security)	Theme
	the storage locations and third-party storage after validation (WHO, 2016)	
Protection of recovery data	<ul style="list-style-type: none"> <li>• Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>• No provision</li> </ul>
Isolated data recovery instance	<ul style="list-style-type: none"> <li>• Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>• No provision</li> </ul>
Data disposal	<ul style="list-style-type: none"> <li>• “A documented process for the disposal of records should be in place” (PIC/S, 2021, p.30)</li> <li>• Procedures to “describe the process for the disposal of electronically stored data (PIC/S, 2021, p.52)”.</li> <li>• Controls to prevent and detect risks in the data life cycle for which data disposal is comprised (WHO, 2016)</li> </ul>	<ul style="list-style-type: none"> <li>• Documented data disposal process</li> <li>• Data disposal procedures</li> </ul>
Service provider logs	<ul style="list-style-type: none"> <li>• Contract giver’s access to all relevant data related to products or services, as well as quality system records generated on their behalf and held by the contracted organization.</li> <li>• “Access by the contract giver to electronic records, including audit trails, held in the contracted organization’s computerized systems as well as any printed reports and other relevant paper or electronic records” (WHO, 2016, p.181).</li> <li>• Contact giver’s access to logs audit trails “so that compliance with data integrity and management principles can be assessed and demonstrated” (PIC/S, 2021, p.55).</li> </ul>	<ul style="list-style-type: none"> <li>• Data access and audit trail provisions for auditing by the contract giver.</li> </ul>
Monitoring of service providers	<ul style="list-style-type: none"> <li>• “Initial and periodic re-qualification of supply chain partners and outsourced activities should include consideration of data integrity risks and appropriate control measures” (PIC/S, 2021 p.54).</li> <li>• “Monitoring of contract acceptors and tracking and trending of associated quality metrics for these sites help to identify risks that may indicate the need for more active engagement and allocation of additional resources by the contract giver to ensure quality standards are met” (WHO, 2016, p.179).</li> <li>• “The nature and frequency of the evaluation of the contract acceptor and the approach to ongoing monitoring of their work should be based upon documented assessment of risk” (WHO, 2016, p.181). It also recommended the inclusion of relevant data processes and their risks.</li> <li>• Verification of compliance with the principles and responsibilities during periodic site audits (WHO, 2021). It recommended “the review of procedures</li> </ul>	<ul style="list-style-type: none"> <li>• Ongoing qualification of supply chain partners and outsourced activities</li> <li>• Establishment of quality metrics for risk identification</li> <li>• Evaluation of contract acceptors per documented risk evaluations.</li> <li>• Compliance audit</li> <li>• Data and procedure reviews</li> </ul>

Coding Frame (Data security control)	Meaning Unit (Provision for data security)	Theme
	and data (including raw data and metadata, paper records, electronic data, audit trails and other related data) held by the relevant contract acceptor identified in risk assessment (WHO, 2021, p.145)	
Data encryption in end-user devices	• Encryption is employed as a mechanism to ensure data confidentiality (WHO, 2021)	• Encryption employed for data confidentiality and integrity
Data encryption on removable media	• Encryption is employed as a verification method to minimize data integrity risks (PIC/S, 2021).	
Data encryption in transit		
Data encryption at rest		
Data classification	• Unspecified	• No provision
Data loss prevention	• Unspecified	• No provision
Segmentation of data processing and storage	• Unspecified	• No provision
Decommissioning of service providers	• Unspecified	• No provision

**Data Management Process.** The PIC/S (2021) and WHO (2016) guidance documents outlined the establishment and maintenance of a process for managing data. The PIC/S (2021) guidance describes data management as “all those activities performed during the handling of data including but not limited to data policy, documentation, quality, and security” (p .3). According to the WHO (2016) guidance, “a data management program developed and implemented upon the basis of sound quality risk management principles is expected to leverage existing technologies to their full potential” (p. 178). The WHO (2021) guidance states that “the data governance program should include policies and procedures addressing data management” (p. 141).

Both PIC/S (2021) and WHO (2016; 2021) guidance documents advocate for the establishment and maintenance of data management processes. They emphasize the importance of data management, including policies, documentation, quality, and security. This shared focus on data governance and leveraging existing technologies reflects a comprehensive approach to data management.

**Data Inventory.** Although the PIC/S (2021) guidance references inventory, it emphasizes “all computerized systems in use” (p. 34), rather than specifically addressing data

inventory. Similarly, neither the WHO (2016) nor the WHO (2021) guidance documents include explicit provisions for maintaining a structured data inventory.

This findings indicate a significant gap in these regulatory documents concerning data inventory. While the PIC/S (2021) guidance acknowledges computerized systems, it does not explicitly underscore the importance of maintaining a comprehensive inventory of data assets. The omission of such guidance, both in PIC/S (2021) and WHO (2016; 2021) documents, suggests a limited emphasis on systematically tracking and managing data assets, which is crucial for ensuring data integrity, traceability, and security.

**Data Flows.** Both the WHO (2016) and PIC/S (2021) guidance documents addressed the documentation of data flows. The WHO (2016) guidance recommended “documenting the system architecture and data flow, including the flow of electronic data and all associated metadata, from the point of creation through archival and retrieval” (p. 185). The PIC/S (2021) guidance specified “a graphical representation of the “flow” of data through an information system” (p. 61). It also suggested that “the creation and assessment of a data flow map may be useful in understanding the risks and vulnerabilities of computerized systems, particularly interfaced systems” (p. 32) and recommended the evaluation of data flows. However, WHO (2021) guidance did not specify visual representation or documentation for data flows.

Although both the PIC/S (2021) and WHO (2016) guidance documents recognized the importance of documenting data flows, there were differences in the level of detail provided. PIC/S (2021) guidance places greater emphasis on the creation, visualization, and risk-based evaluation of data flow maps. Conversely, WHO (2021) guidance does not mandate any visual representation or structured documentation, which may lead to gaps in understanding how data moves through systems and the risks associated with those movements.

**Data Access Control Lists.** Both the PIC/S (2021) and WHO (2016) guidance documents addressed the configuration of data access control lists. The PIC/S (2021) guidance

emphasized user access controls by prohibiting “unauthorized access to, changes to and deletion of data” (p. 40). Similarly, the WHO (2016) guidance highlighted that “only people with the appropriate authorization to alter a master processing formula” (p. 177). Although the WHO (2021) guidance did not explicitly require access control, it mentioned it.

Collectively, the PIC/S (2021) and WHO (2016; 2021) guidance documents underscore the importance of access control in preventing unauthorized access and ensuring proper authorization. These requirements align with essential data security principles, which emphasize the importance of access controls in protecting sensitive data.

**Role-based Access Control.** The PIC/S (2021) and WHO (2021) guidance documents outline the establishment and maintenance of role-based access control. The PIC/S (2021) guidance stated that “systems should support different user access roles (levels) and assignment of a role should follow the least-privilege rule” (p.40). The WHO (2021) guidance detailed access and privileges based on roles and responsibilities:

Access and privileges should be following the role and responsibility of the individual with the appropriate controls to ensure data integrity (e.g., no modification, deletion or creation of data outside the defined privilege and following the authorized procedures defining review and approval where appropriate) (p.149).

However, there were no provisions for role-based access control in the WHO (2016) guidance.

This shift in guidance reflects a significant evolution in access control best practices. Newer versions of the guidance documents (PIC/S, 2021; WHO, 2021) emphasize the importance of establishing and maintaining role-based access control, ensuring that access and privileges align with the roles and responsibilities of individuals. This approach not only reinforces data integrity but also minimizes security risks by applying the principle of least privilege.



**Data Retention.** The PIC/S (2021) guidance specified a data retention process that “records all data, (including metadata) for all activities which directly or indirectly impact on all aspects of the quality of medicinal products” (p.18). Similarly, the WHO (2016) guidance recommended a records retention period in which “original records should be complete, enduring and readily retrievable and readable” (p.183). Further, the WHO (2021) guidance outlined the need for defined policies and procedures to govern the retention of data and audit trails according to a defined retention period.

Collectively, these guidance documents provide clear direction on data retention, highlighting the necessity of maintaining not only data and metadata but also comprehensive records for quality assurance and regulatory compliance. The emphasis on data retention underscores the significance of preserving data integrity over time. Establishing policies and procedures for data retention and audit trails is therefore essential for ensuring data integrity and ongoing compliance with regulatory expectations.

**Data Backup.** The PIC/S (2021) and WHO (2016; 2021) guidance documents addressed data backups in pharmaceutical manufacturing. All three emphasized the need for routine backups, particularly in remote or secure locations, as a safeguard against data loss due to disasters. The WHO (2021) guidance went further by stressing the importance of validating both backup and restoration processes, while the PIC/S (2021) guidance highlighted the requirement for periodic data backups and archiving, following documented procedures.

The emphasis on data backup in the PIC/S (2021) and WHO (2016; 2021) guidance documents underscores the critical importance of continuity in regulated environments, such as pharmaceutical manufacturing. The consistent recommendation across all three documents to conduct routine backups in remote or secure locations underlines a shared commitment to disaster resilience and business continuity. The WHO (2021) guideline's emphasis on validating both backup and restoration processes represents a shift beyond basic procedural

compliance toward a risk-based approach, where the focus extends beyond data duplication to ensuring the functional reliability of recovery mechanisms.

**Data Recovery.** The PIC/S (2021) guidance recommended a process for data recovery, emphasizing that “consideration should also be given to ensuring complete and timely data recovery in the event of a disaster” (p.8). Although the WHO (2016) guidance did not outline a data recovery process, it specified the need for “periodic tests to verify the ability to retrieve archived electronic data from storage locations” (p.204). It further recommended that such retrieval capabilities should be tested during the validation of the electronic archive. Post-validation, the guidance called for periodic assessments to ensure data can still be retrieved from both on-site and third-party storage locations. Although the WHO (2021) guidance briefly mentioned disaster recovery, it offers no detailed elaboration. While the PIC/S guidance recommended timely data recovery, the WHO (2016) and WHO (2021) guidance documents did not address the establishment and maintenance of an isolated instance for recovery data.

All three guidance documents acknowledge the importance of data backup and recovery, emphasizing regular backups, validation of backup processes, and periodic testing of data retrievability. This shared emphasis reflects a common understanding of the need to ensure data availability in the event of system failures or disasters. However, none of the documents provide detailed operational guidance or mandate the implementation of an isolated recovery instance—an increasingly essential control in the face of modern cybersecurity threats. The absence of such provisions indicates a regulatory gap that may limit the effectiveness of disaster recovery efforts, particularly in safeguarding business-critical data in high-risk environments.

**Data Disposal.** Both the PIC/S (2021) and WHO (2016) guidance documents addressed the disposal of data. The PIC/S (2021) guidance document recommended that “a documented process for the disposal of records should be in place” (p.30), and outlined procedures to

“describe the process for the disposal of electronically stored data” (p.52). These provisions govern the disposal of records and electronic data after the defined retention period. The WHO (2016) guidance document suggested controls to prevent and detect risks in the data life cycle, of which data disposal is a part, whereas the WHO (2021) did not address data disposal.

The PIC/S (2021) guidance document reinforce the necessity of a structured and documented approach to data disposal, recognizing its role in preventing unauthorized access and potential data breaches. Similarly, WHO (2016) underscore the importance of risk controls across the entire data life cycle, implicitly including disposal, though without offering procedural specifics. In contrast, the WHO (2021) guidance omits any reference to data disposal, highlighting a regulatory gap in addressing the secure and compliant termination of data after its retention period.

**Service Provider Logs.** The PIC/S (2021) and WHO (2016) guidance documents provided for the collection of service provider logs. Both documents specified the contract giver’s access to all relevant product or service data, as well as quality system records generated on its behalf and maintained by the contracted organization. The WHO (2016) guidance document also stated, “access by the contract giver to electronic records, including audit trails, held in the contracted organization’s computerized systems as well as any printed reports and other relevant paper or electronic records” (p.181). Additionally, the PIC/S guidance document emphasized the necessity of access for audit purposes “so that compliance with data integrity and management principles can be assessed and demonstrated” (p.55).

All three guidance documents address the collection of logs from service providers and the access of contract givers to relevant data for auditing purposes. This provision is essential for compliance assessment, as well as for ensuring transparency and accountability in outsourcing arrangements.

**Monitor Service Providers.** The PIC/S (2021), WHO (2016), and WHO (2021) guidance documents emphasized the importance of monitoring service providers. The PIC/S guidance document advised that “initial and periodic re-qualification of supply chain partners and outsourced activities should include consideration of data integrity risks and appropriate control measures” (p.54). The WHO (2016) guidance document proposed:

Monitoring of contract acceptors and tracking and trending of associated quality metrics for these sites help to identify risks that may indicate the need for more active engagement and allocation of additional resources by the contract giver to ensure quality standards are met (p.179).

The WHO (2016) guidance also specified ongoing monitoring of contractors’ activities periodically, as determined through risk assessment. It further recommended that “the nature and frequency of the evaluation of the contract acceptor and the approach to ongoing monitoring of their work should be based upon documented assessment of risk” (p.181). Additionally, it suggested including relevant data processes and their associated risks. The WHO (2021) guidance specified verifying compliance with principles and responsibilities during periodic site audits. It further recommended “the review of procedures and data (including raw data and metadata, paper records, electronic data, audit trails, and other related data) held by the relevant contract acceptor identified in risk assessment” (p.145).

All three guidance documents underscore the importance of continuously assessing and monitoring service providers, supply chain partners, and outsourced activities for data integrity risks and compliance with quality standards. This provision stress the need for control over data, even when essential activities are outsourced.

**Data Encryption.** The PIC/S guidance document identified encryption as a verification method to reduce data integrity risks. While the WHO (2016) guidance document did not

address encryption, the WHO (2021) recommended encryption as a means to ensure data confidentiality.

PIC/S (2021) and WHO (2021) both emphasize encryption as a means to safeguard data confidentiality and integrity, underscoring its relevance in maintaining data security throughout the product life cycle. While the absence of encryption guidance in the WHO (2016) document reflects a lag in adapting to evolving cybersecurity threats, the inclusion of encryption in recent documents marks progress.

**Unspecified Elements.** The PIC/S (2021), WHO (2016), and WHO (2021) guidance documents did not include a data classification scheme. They also lacked guidance on segmenting data processing and storage based on sensitivity, as well as on isolating and protecting recovery data. Additionally, these documents did not address the implementation of data loss prevention solutions. Finally, none of the three guidance documents addressed the secure decommissioning of service providers.

The evaluation of the PIC/S (2021) and WHO (2016; 2021) guidance documents' data security provisions offers valuable insights into the strengths and weaknesses of these guidelines, establishing a foundation for future improvements and standardization in data security practices within the Nigerian pharmaceutical industry. While both health authorities highlight key aspects of data security controls, emphasizing data management, flows, encryption, backup, retention, disposal, recovery processes, access control, service provider logs, and monitoring, there are significant areas requiring further clarification and guidance. These include data inventory and classification, along with more advanced security measures such as data loss prevention, data processing and storage segmentation, secure decommissioning of service providers, and the isolation and protection of recovery data. These gaps reveal potential vulnerabilities in the pharmaceutical security framework that could be exploited, leading to data breaches or loss. We anticipated these results due to

the global pharmaceutical industry's ongoing focus on specific aspects of data security, particularly data integrity (Tabersky et al., 2018). Additionally, the study results align with the theoretical framework indicating that data integrity, best practices in data security, and management controls can address data-related risks. This outcome highlights the need for more specific and detailed provisions in critical areas to enhance data security in the Nigerian pharmaceutical industry.

#### 4.3.2 Data Security Gaps in Drug Manufacturing Practices

A thematic analysis of respondents' accounts enabled the identification of gaps in manufacturing practices. Table 11 presents the findings of the thematic analysis, categorizing the emerging themes as follows: challenges in data classification and loss prevention; ineffective data risk assessment; immature tech-centric data management; data ownership assumptions and unchecked data sharing; data governance challenges and risk mitigation in a globally distributed environment; deficiencies in software integrity assessment; inconsistencies in network security measures and monitoring practices; USB security risks; challenges in system validation and configuration control; data resilience challenges in modern IT ecosystems; data privacy vulnerabilities in external systems; data integrity gaps in operations and supply chain; inadequate data security monitoring; challenges prioritizing data security and response. An evaluation of these findings confirmed data security gaps in drug manufacturing practices.

**Table 11**

*Evaluation of Data Management Practices in terms of Data Security Controls*

Code	Organizing Theme
<ul style="list-style-type: none"> <li>• Absence of data classification scheme</li> <li>• Absence of data loss prevention solutions</li> </ul>	<ul style="list-style-type: none"> <li>• Challenges in data classification and loss prevention</li> </ul>
<ul style="list-style-type: none"> <li>• Infrequent data risk assessment</li> <li>• Inadequate data risk assessment</li> <li>• Lack of standard for data risk assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Ineffective data risk assessment</li> </ul>
<ul style="list-style-type: none"> <li>• Technology-driven, access-controlled data management process.</li> <li>• Cloud-based, high-availability data management</li> </ul>	<ul style="list-style-type: none"> <li>• Immature tech-centric data management.</li> </ul>

Code	Organizing Theme
<ul style="list-style-type: none"> <li>• Presumed data ownership.</li> <li>• Uncontrolled data sharing</li> </ul>	<ul style="list-style-type: none"> <li>• Data ownership assumptions and unchecked data sharing</li> </ul>
<ul style="list-style-type: none"> <li>• Presumed uninterrupted access to globally stored data.</li> <li>• Due diligence checks employed for GMP adherence and data integrity in the supply chain.</li> <li>• Non-disclosure agreements with vendors for data integrity communication</li> <li>• Regulatory concerns for data held in multiple locations.</li> <li>• SLAs and access controls employed to mitigate risks in contracts, supply chains, and outsourcing.</li> <li>• SLAs and informal methods are key to monitoring third-party service levels.</li> <li>• Insufficient data protection during third-party shutdowns or bankruptcies.</li> <li>• Non-disclosure agreements with service provider to control post-contract data access.</li> </ul>	<ul style="list-style-type: none"> <li>• Data governance challenges and risks in a globally distributed environment</li> </ul>
<ul style="list-style-type: none"> <li>• Minimal software and firmware integrity verification</li> <li>• Controlled software and firmware updates</li> </ul>	<ul style="list-style-type: none"> <li>• Deficiencies in software integrity assessment</li> </ul>
<ul style="list-style-type: none"> <li>• Firewalls, end-point security, intrusion prevention implementations</li> </ul>	<ul style="list-style-type: none"> <li>• Inconsistencies in network security measures and monitoring practices</li> </ul>
<ul style="list-style-type: none"> <li>• USB drive usage controlled by domain policy.</li> <li>• Prohibition on the use of USB drives</li> <li>• Uncontrolled use of USB drives</li> </ul>	<ul style="list-style-type: none"> <li>• USB Security Risks</li> </ul>
<ul style="list-style-type: none"> <li>• Informal system validation</li> <li>• System validation using templates and checklists.</li> <li>• Controlled changes to system configuration.</li> </ul>	<ul style="list-style-type: none"> <li>• Challenges in System Validation and Configuration Control</li> </ul>
<ul style="list-style-type: none"> <li>• Technology-driven recovery objectives.</li> <li>• Extended RPO for third-party data risks</li> <li>• Hybrid data backup storage</li> <li>• Intrusion prevention for DoS attack mitigation.</li> <li>• API support for legacy system data access.</li> <li>• Inadequate clarity on data recovery test scope and frequency.</li> <li>• Insufficient accountability for data changes or loss in outsourced archives.</li> <li>• Inadequate measures for continued readability in data archives.</li> <li>• Reliance on third parties for electronic data retention compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Data resilience challenges in modern IT ecosystems</li> </ul>
<ul style="list-style-type: none"> <li>• Evaluation of external system controls for data privacy through information requests.</li> <li>• Dependence on non-disclosure agreement for encrypting data held with third-party.</li> <li>• Dependence on cloud provider encryption for stored and in-transit data.</li> <li>• Unencrypted stored data</li> </ul>	<ul style="list-style-type: none"> <li>• Data privacy vulnerabilities in external systems</li> </ul>
<ul style="list-style-type: none"> <li>• Supply chain partner qualification via confidentiality agreements.</li> <li>• Insufficient electronic data integrity checks.</li> <li>• Insufficient safeguards against test data in production systems</li> </ul>	<ul style="list-style-type: none"> <li>• Data integrity gaps in operations and supply chain</li> </ul>
<ul style="list-style-type: none"> <li>• Partial implementation of audit trails</li> <li>• Limited audit trail review</li> <li>• Undetected data alteration</li> <li>• Anomaly-based log analysis</li> <li>• Limited scope of log monitoring</li> <li>• Erasure of audit trails</li> <li>• Disabled audit trail functionality</li> </ul>	<ul style="list-style-type: none"> <li>• Inadequate data security monitoring</li> </ul>
<ul style="list-style-type: none"> <li>• Device security informed by host-based security app.</li> <li>• IT security assessment and incident response.</li> </ul>	<ul style="list-style-type: none"> <li>• Challenges prioritizing data security and response</li> </ul>

Code	Organizing Theme
<ul style="list-style-type: none"> <li>• Under-resourced data security audit</li> <li>• The inaction of the auditee and management to audit recommendations</li> </ul>	

**Challenges in Data Classification and Loss Prevention.** The presence or absence of a data classification scheme influenced the implementation of DLPSs in pharmaceutical organizations. OrganizationE established a data classification scheme, while OrganizationA lacked one, resulting in the absence of DLPSs. According to RespondentVIA from OrganizationA,

We are yet to do data classification to be able to implement data loss prevention. So, without that classification, we won't be able to implement DLP which track whatever anybody is sending outside of the domain or from our email platform.

RespondentAAD from OrganizationB confirms that “we need to put certain technical controls. So, that is also a work in progress”.

The inconsistent adoption of data classification and technical controls across organizations highlights the challenges encountered in effectively implementing data classification and loss prevention measures.

Data classification and loss prevention are critical components of data security in drug manufacturing organizations, where the protection of sensitive data is paramount. Effective data classification is vital for understanding the sensitivity and importance of various data types, enabling the implementation of appropriate security measures. Data classification helps identify which data requires encryption based on its sensitivity level (CIS Critical Security Controls Version 8, n.d., ISACA, 2012b). Therefore, data classification by data owners is essential for maintaining confidentiality. Additionally, data classification is crucial for successful DLP. Classifying data is often necessary before DLPSs can scan repositories to assess what should or should not be classified as confidential (Alneyadi et al., 2016). Consequently, DLPSs depend on data classification to effectively monitor and control



data flow both within and outside the organization. DLPSs safeguard sensitive data from being accessed by unauthorized individuals or being lost through illicit channels (Spooner et al., 2018; Pujeri et al., 2023). These solutions track end-user activities, data transmitted over the network, and data movement (AlKilani et al., 2019). Best practices include developing a clear and comprehensive data classification scheme that organizes data based on sensitivity and criticality, as well as implementing DLPSs (ISACA, 2012b; CIS Critical Security Controls Version 8, n. d.; Cybersecurity Audit Program, n. d.). However, inconsistencies in data classification practices among pharmaceutical organizations—some of which lack a comprehensive classification scheme and, consequently, lack DLPSs—create significant gaps in data security.

**Ineffective Data Risk Assessment.** Data risk assessments in pharmaceutical organizations were infrequent, insufficient, and often lacked standardization. The frequency of data risk assessments was not clearly defined for OrganizationA. According to RespondentOAD:

It depends on the audit, timeframe, and the deliverables we are supposed to provide.

What I do is based on materiality. I determine the criticality and impact if the data were exposed. That is what I do until I do an in-depth audit on risk assessment.

For OrganizationB, data risk assessments were not guided by published standards. RespondentNON indicated a planned adoption of ISO standards, stating, “we are in the process of obtaining certification for ISO 90001 and 27001”. Also, data risk assessment was not explicitly conducted in OrganizationA. According to RespondentVIA,

We don't do a data risk assessment. In the organization, every department is supposed to perform, I think quarterly risk assessment, and then submit to Internal Audit, which I believe is also part of the risk assessment that will be within their scope.

The absence of clear processes reflects ineffective data risk assessment practices across pharmaceutical organizations.

Effective data risk assessments play a critical role in identifying potential threats and vulnerabilities that may compromise data security. Data risk assessment is a foundational practice that protects sensitive data and enables proactive management of data-related risks, compliance with regulations, cost reduction, and overall enhancement of data security. Therefore, conducting regular and thorough data risk assessments is essential. Every organization should identify, analyze, and address risks associated with data security (Jiao, 2020). This requirement becomes particularly important amid significant changes in the enterprise's internal and external landscapes. Effectively managing risk involves a commitment to identifying and analyzing emerging risk factors, as well as acquiring and implementing control measures to prevent ongoing threats to data security (Jiao, 2020). Best practices entail defining a structured and consistent process for assessing data-related risks. Referring to recognized frameworks, such as NIST SP 800-30 Rev. 1 (NIST, 2012), and using data privacy impact assessment templates (Sample DPIA Template, n. d.; Template for Data Protection Impact Assessment, n. d.) can provide a standardized approach. However, the variability in approach and frequency across pharmaceutical organizations, combined with data risk assessments that do not follow published standards, results in inconsistent and potentially inadequate data risk management, creating a gap in data security.

**Immature Tech-centric Data Management.** Data management in pharmaceutical organizations highlights distinct approaches: a technology-driven, access-controlled data management process; and a cloud-based, high-availability data management solution. OrganizationA maintained a high-availability, cloud-focused data management process. RespondentVIA explained that user and operational data were backed up in the cloud. He added that data backup was stored on-premises, and high availability was facilitated by replication

between critical servers both on-premises and in the cloud. He maintained that, “if one server is down, once we can bring it up, we're able to pick all the configurations and the policies from the other servers, be it cloud or on-premises”. OrganizationE, however, followed a technology-based, access control-driven data management process. RespondentTDA notes,

What we use is, is Microsoft SharePoint. That's like the general data repository that we have deployed. So as a given, you're only allowed to view certain data and certain content that your roles and permissions allow. And that's also tied to the corporate apps a user has access to.

These differing data management approaches, despite all being technology-driven, also highlight the varying levels of maturity in data management practices across pharmaceutical organizations.

Data management is essential for organizations that depend on data to make decisions and enhance business outcomes. A solid data management process is critical for drug manufacturing organizations to preserve data quality, security, and accessibility while ensuring compliance with standards and regulations. Best practices address data ownership, sensitivity, handling, retention limits, and disposal requirements (CIS Critical Security Controls Version 8, n.d.). An effective data management process in drug manufacturing, backed by technology, ensures data is collected, stored, processed, and utilized efficiently and securely to achieve business objectives. Nonetheless, the selection of cloud-based or access control-driven processes for data management depends on a pharmaceutical organization's specific needs and risk tolerance. Inconsistency in approaches, however, creates a potential gap and indicates a need for a more unified strategy to manage data effectively and securely across different platforms.

**Data Ownership Assumptions and Unchecked Data Sharing.** There were ambiguities surrounding data ownership and instances of uncontrolled data sharing within

pharmaceutical organizations. In Organization C, data ownership was assumed. Respondent AAR states, “for whatever cloud platform that is in use, the customer is the owner of the data. The customer is the number one data controller. So, we are responsible for the data and not the third party”. Respondent JNW also asserted that “the users of data are responsible since they are owners of the data”. In Organization E, data ownership was not clearly defined. Respondent RID confirmed that “Right now, it isn’t”. Furthermore, uncontrolled data sharing with contract acceptors, supply chain partners, or outsourcing activities occurred in Organization D. Respondent JIB noted that

The heads of departments that interface with these vendors determine the sensitivity of the data that they are supposed to release to them. So, there's no particular process that is used to measure or determine or control the kind of data that's shared with such vendors.

The unchecked data sharing and assumptions across pharmaceutical organizations regarding data ownership highlight the need for clearer accountability measures.

Effective data management requires clearly defined data ownership, a complex issue that necessitates careful consideration of ethical, legal, and regulatory factors. Clearly defined data ownership is essential for appropriately managing and protecting data throughout its life cycle. Patients, cloud service providers, vendors, regulators, and third-party collaborators, such as contract research organizations and academic institutions, all have a stake in pharmaceutical data ownership. Defining data ownership is crucial for establishing accountability regarding data security. Data security governance requires organizations to establish and maintain obligations for data owners (CIS Critical Security Controls Version 8, n.d., ISACA, 2012b), who may determine how data is shared and the level of access granted. Best practices include clearly defining roles and responsibilities for data ownership within the organization, implementing strict access regulations, establishing

the infrastructure and processes to manage metadata, and documenting and auditing data access (ISACA, 2012b; ISACA, 2018a; CIS Critical Security Controls Version 8, n. d.). Therefore, management practices should encompass establishing clear guidelines and agreements with third parties concerning data access, usage, and protection. However, a lack of clarity resulting in undefined data ownership and uncontrolled data sharing, especially with supply chain partners and contract acceptors, creates a potential gap in data security.

### **Data Governance Challenges and Risks in a Globally Distributed Environment.**

Pharmaceutical organizations employ various measures to manage data risks, vendor relationships, and compliance with GMP requirements: presumed uninterrupted access to globally stored data; non-disclosure agreements (NDAs) with vendors for data integrity communication; due diligence checks employed for GMP adherence and data integrity in the supply chain; SLAs and access controls employed to mitigate risks in contracts, supply chains, and outsourcing; SLAs and informal methods are key to monitoring third-party service levels; insufficient data protection during third-party shutdowns or bankruptcies; NDAs with service provider to control post-contract data access.

Due diligence checks were employed in OrganizationA to communicate GMP requirements and address data integrity risks in the supply chain. According to RespondentTOL,

What we do is we contact more than one ISP or vendor for particular service. And then when we get them, we do a verification check on them. If we get a reputation that is bad for business, we do not engage the vendor. If the feedback we get is good enough and the price is competitive, we go for them.

The impact of laws on data held in various geographical locations was considered in OrganizationB. RespondentSIS emphasized the importance of GDPR compliance, stating, “we check to see that our cloud service providers also comply with that”.

OrganizationC assumed continuous access to data stored in different geographical locations. RespondentJNW asserted, “I have access to my data anytime I want it. So, there are no restrictions to you managing your data residing on the service provider’s platform. He added, “the last experience we had with Google there was no restriction. We're able to move away from Google to Microsoft unhindered. So that also tells you that we have control over whatever data that will switch from their platform”.

OrganizationD and OrganizationB utilized NDAs with their system vendors to convey data integrity requirements. RespondentJIB explained, “with regards to GMP and management of our vendors, the engagement of vendor starts with them signing the non-disclosure with us”. He noted, “our vendors are mostly players also in our industry. So, while we are pushing out our non-disclosure agreements to them to sign, most of the time they also are reciprocating by sending theirs”. Along with NDAs, OrganizationD employed service-level agreements and access controls to mitigate risks from contract acceptors, supply chain partners, and outsourced activities. RespondentJIB stated, “our supply chain partners before they're engaged, there is service agreements”. He added that access is granted based on a need-to-know basis in addition to service-level and NDAs.

OrganizationA conducted service-level monitoring through SLAs and informal methods. RespondentTOL remarked, “we have SLA with them and regularly review the SLA. If we are not satisfied, we let them know that we are not continuing with the service and call them up”.

OrganizationC assumed continuous availability for data hosted by third parties. RespondentJNW stated, “we can always receive our data from any service provider whenever we want. Assuming we want to move to another service provider, nothing stops us. However, OrganizationB did not provide for the inaccessibility of data due to third-party closure or

bankruptcy. According to RespondentSIS, “I’m not sure that we do. I guess that’s something that we need to work on”.

OrganizationB managed risks from contracts, supply chain partners, and outsourcing activities through access control and NDAs. RespondentSIS remarked, “if they need to access our systems for any reason at all, explicit permissions are given to them”. He added that once access is granted, “it’s monitored to ensure that access is controlled properly”.

OrganizationD referenced NDAs to control service provider access to data after contract expiration. RespondentJIB pointed out that

There is an extent to which you can decommission any data that you made available to a vendor. So, if it’s information that they’ve already downloaded and is available with them, the only thing you’ll be banking on is the non-disclosure that you signed with them.

These findings highlight the need for more comprehensive oversight and standardized risk management practices for globally distributed data.

Managing data risks associated with third parties necessitates effective oversight and comprehensive risk management strategies in a globally distributed environment. Third-party data risk management entails identifying potential threats, assessing the probability of their occurrence, and implementing measures such as collecting logs, monitoring, and securely decommissioning service providers (CIS Critical Security Controls Version 8, n. d.), along with due diligence (ISACA, 2019), entering both contractual and NDAs (ISACA, 2014; ISACA, 2019), and establishing access controls (ISACA, 2012b). Due diligence is a form of risk assessment that evaluates the security practices and privacy policies of third-party vendors or service providers, as well as their overall reputation before engagement. Pharmaceutical organizations must carry out thorough due diligence to ensure that third parties comply with data security and privacy standards. This process also involves assessing

third parties' data protection measures, security protocols, and compliance with relevant regulations. NDAs detail confidential information that parties are willing to share for a specific purpose but do not wish to disclose to third parties or the public. Establishing contractual obligations with third parties that delineate their data protection responsibilities can complement NDAs, provided both binding documents are properly drafted and enforced. Access control mechanisms can also be utilized to mitigate third-party data risks by restricting access to data based on a user's role or job function. Additionally, pharmaceutical organizations may require third parties to conform to several regulations such as GDPR and NDPR to address regulatory risks. Best practices include regularly monitoring and auditing third-party data access, ensuring adherence to organizational policies and contractual obligations, and establishing clear exit strategies for data access following contract termination or closure (ISACA, 2012b; CIS Critical Security Controls Version 8, n. d.). Conducting due diligence checks by some pharmaceutical organizations serves as a means of communicating GMP requirements and addressing data integrity risks. However, disparities in handling data accessibility issues in the event of third-party closure or bankruptcy lead to data security gaps.

**Deficiencies in Software Integrity Assessment.** Pharmaceutical organizations employ various practices for software integrity assessment. In OrganizationB, the integrity of the software was verified through the execution of substantive tests that evaluated both the input and output controls within the ERP application. According to RespondentAEM, "I just check for the GL (General Ledger) integrity in the sense that going from top-down approach, GL would report into the Trial Balance, which in turn report the financial statement". She added, "So, I do a substantive test and the software aspect of it. So, that's how I verify the integrity of the application software we are using right now". There were minimal to no software and firmware integrity checks in OrganizationE. RespondentAAJ explained that "only software -



applications, drivers, firmware, and so on- are obtained directly from the original developers or the manufacturers”. RespondentAAJ further stated that “only persons with administrator rights can install software or firmware-related resources”, while RespondentEKA claimed that in OrganizationC, “only IT administrators that are trained and have an experience that has such permission to make changes to software and firmware”.

These varying practices highlight the challenges associated with conducting software integrity assessments.

Integrity verification checks that data has not been tampered with and ensures it is authentic and complete. Furthermore, integrity checks for software and firmware are crucial for maintaining data integrity. Good practices involve using verification mechanisms to confirm the authenticity and integrity of software components (Cybersecurity Audit Program, n. d.). However, the varying methods of software integrity verification among pharmaceutical organizations, with some lacking proper checks, highlight a gap in ensuring the authenticity and reliability of data.

**Inconsistencies in Network Security Measures and Monitoring Practices.** A variety of network security measures were employed in pharmaceutical organizations, including firewalls, VLANs, endpoint security, intrusion prevention, and network monitoring implementations. RespondentAFA from OrganizationE indicated that firewalls, including host-based firewalls, were configured with rules to “protect against data-related threats”. In addition to firewalls, RespondentCOS from OrganizationE highlighted intrusion prevention systems and endpoint solutions as essential network security measures. The network infrastructure in OrganizationB was organized with multiple VLANs located behind a firewall. According to RespondentCOG,

It's difficult for an external party to have access or transmit information directly to an internal VLAN. That traffic ends on the firewall. Once it is an illegitimate traffic it drops out on the firewall. The firewall will not accept or transmit it inwards.

Additionally, monitoring tools were implemented in OrganizationB to track user activities and identify anomalies. RespondentCOG added,

We have monitoring tools that monitors every user's activity. So, when we have such, maybe in terms of network flooding, we will notice it. We will know a particular system that is flooding the network, immediately investigate, and isolate such systems from the network

He also emphasized the proposed implementation of a network access control (NAC) solution to enable detailed control and monitoring of user activities within the network.

The diverse network security measures and monitoring practices across pharmaceutical organizations reveal inconsistencies in network security among organizations.

Network security and monitoring are essential for protecting sensitive data, detecting and preventing threats, and responding to incidents. Effective network security measures and monitoring mechanisms are crucial for safeguarding sensitive information and preventing unauthorized access. Best practices employ security measures and related management procedures to protect data across all connectivity methods, while also establishing and maintaining comprehensive network monitoring (CIS Critical Security Controls Version 8, n.d.): implementing and actively managing network devices; establishing and maintaining a secure configuration process for network infrastructure; maintaining and enforcing network-based URL filters; utilizing DNS filtering services; blocking unnecessary file types; implementing DMARC; deploying and maintaining email server anti-malware protections; validating security measures; performing periodic external penetration tests and addressing test findings; monitoring network traffic for unauthorized access or anomalies (ISACA, 2012b;

ISACA, 2012b; CIS Critical Security Controls Version 8, n.d.). Various network security measures have been implemented in several pharmaceutical organizations, including intrusion prevention systems and firewalls.

Although these measures are critical, the inconsistency in implementations indicates a lack of uniform standards in network security and a potential data security gap.

**USB Security Risks.** Pharmaceutical organizations adopted various policies regarding the use of USBs and removable media for file transfer. Some organizations strictly prohibit USB use, others allow it with safeguards, and some permit it without restrictions. OrganizationB prohibited the use of USBs for file transfers. RespondentCIG asserts “in our environment, the use of USB is disabled. It's part of the domain policy”. Additionally, RespondentAAI from OrganizationA stated,

We don't use mobile devices and USB devices. We don't use it at all but be whatever reason you must use a USB device, maybe to copy something, it is not being practiced again. I must be clear. We don't really copy confidential information into USB devices.

In OrganizationD, removable media is used to transfer data. According to RespondentSNW, “we try as much as possible to discourage transferring data back and forth on removable media. The management is still deliberating whether to remove that completely”. He explained that controls are in place to prevent system compromise from viruses and malware on media, noting, “if that flash drive has some virus on it, the anti-malware system flags it and takes the necessary action. The action could be from quarantine to deleting immediately. That is done in real time.” He also emphasized the importance of user sensitization and awareness in the safe use of technology.

The inconsistent practices across organizations reveal the risks associated with removable media.

USB devices are commonly used for data transfer and storage. They facilitate quick

and easy data exchange, leading to an enhanced user experience and increased productivity. Effective data transfer and removable media practices require a balance between security and convenience. Best practices include using encryption to protect data on removable devices, implementing DLPSs to prevent unauthorized data transfers, restricting USB flash drive usage to specific organization-approved brands, managing access to removable devices on computer systems or logging unauthorized usage attempts, and providing return information for lost USB drives (ISACA, 2012b; ISACA, 2019; CIS Critical Security Controls Version 8, n.d.; Chapple, 2018). However, the inconsistency among pharmaceutical organizations in the use of USB drives for data transfer—some prohibiting their use while others lacking clear policies—presents a potential data security gap.

**Challenges System Validation and Configuration Control.** The system validation processes varied significantly across pharmaceutical organizations, with some adopting an informal approach and others utilizing templates and checklists. In OrganizationE, the process of system validation was informal. According to RespondentAFA, “it’s an informal process right now, but I know that we’re working towards formalizing that process”. In contrast, OrganizationD employed templates and checklists to facilitate system validation, which was a requirement from its contract providers. RespondentSAG notes,

We have carried out validation on some of the systems, but I can't say for sure that every new system in terms of hardware that we buy will validate it because we have done validation before on the existing systems.

Furthermore, some organizations enforced security baselines, while others restricted system changes to a limited number of IT administrators. In OrganizationE, a security baseline was maintained. RespondentAAJ affirmed, “all new systems or legacy systems need to meet certain baseline security requirements. He continued, “so I get a new system today and want to deploy it, there must be anti-malware protection in place as baseline before your system goes

into operation. He added, “disk encryption has to be in place”. What’s more, system configuration changes in OrganizationD adhered to access control processes. RespondentSAG maintained that “no user can make any change on the system except some IT administrators even with limited privileges”.

The inconsistent practices across organizations highlight challenges in system validation and configuration control.

System validation and configuration control are essential elements in ensuring the reliability and security of drug manufacturing systems. It also promotes resilience against security risks. Establishing robust protocols for managing changes, as well as accrediting and certifying systems (ISACA, 2019), ensures that systems meet predefined requirements, operate reliably, and comply with security standards, thereby minimizing the risk of operational failures and security breaches. While some organizations have made strides to formalize their system validation processes and maintain security baselines, the informal validation practices of others raise concerns about the robustness of their systems against security threats, highlighting a gap in data security.

**Data Resilience Challenges in Modern IT Ecosystems.** Pharmaceutical organizations employ various strategies, technologies, and practices to for data resilience: technology-driven recovery objectives (recovery point objectives [RPO] and recover time objectives [RTO]); extended RPO for third-party data risks; hybrid data backup storage; intrusion prevention for DoS attack mitigation; API support for legacy system data access; inadequate clarity on data recovery test scope and frequency; reliance on third parties for electronic data retention compliance; insufficient accountability for data changes or loss in outsourced archives; inadequate measures for continued readability in data archives.

OrganizationB defined technology-driven downtime (risk tolerance) factors. According to RespondentDSA, “the Azure Recovery Services Vault takes backup every 2 minutes, and

this is what informs our RPO and RTO”. OrganizationC, however, maintained a lengthy RPO to guard against third-party closure or bankruptcy. Respondent AAR states,

Once a month, we physically download data from Microsoft, and we store them on-premise. So, we have an application server on-premise where we physically try to do replication as well. So, if anything goes wrong in the cloud, we still have our data on-premise.

Furthermore, the nature of work in OrganizationD necessitated both on-site and off-site backup data storage. Respondent PEM explained, “backup is in the cloud. We ensure that the data remains available in the cloud, and then, backups are also available in the data centers”. Although OrganizationD implemented automated backups, these mainly focused on data. Respondent PEM added, “the scope of the backup is basically the data. Right now, we're not so particular about system state backups”. OrganizationE adopted a cloud storage infrastructure. According to RespondentDSA, “Now, we don't do physical backup. All our data is backed up in the cloud”.

For distributed denial-of-service (DDoS) prevention, Organization E deployed intrusion prevention systems (IPS). According to Respondent DSA, “we have an IPS system that detects and prevents DDoS”. OrganizationD relied on third-party systems to address DDoS. Respondent PEM maintained, “that risk taken up by our cloud service provider. So, in signing up for their services will ensure that they have redundant systems in place to ensure that such attacks do not affect us”.

What’s more, OrganizationC used an application programming interface (API) for data access on legacy system software. Respondent EKA explains,

For new systems assessing data on legacy systems, these days almost every system comes with API. So, once there is an API on the legacy system, the new system will be able to integrate with it to be able to pull whatever information that is required.

However, OrganizationE did not have measures in place for data access when support for legacy system software ceased. According to Respondent AAJ, “we’ve not had that that instance. We’ve not had to do deal with that, thankfully”.

Regarding data recovery tests, OrganizationD did not adequately define their scope. RespondentPEM maintained, “we are still in the process of designing that testing process”. In OrganizationA, information regarding the scope and frequency of data recovery tests was not adequately communicated. According to RespondentNMU, “I cannot say exactly how often. I wasn’t around when the last backup was taken but I saw the documentation. Regarding the interval, I am not certain, unless I go through the policy that addresses that”.

Regarding data archiving, OrganizationE archived data periodically. RespondentDSA stated, “after 90 days, the data in the cloud is archived”. OrganizationC transferred the risk of deliberate or inadvertent alteration or loss of data in the archived facility to third parties. According to RespondentAAR, “that risk has been transferred to the cloud provider. So, they are responsible for maintaining the physical infrastructure that houses the server. So, we transfer that risk to them”. Nonetheless, OrganizationC took no steps to ensure that data remains readable following the retirement of a system in the archive facility. Also, OrganizationE lacked measures to maintain the accessibility, readability, and integrity of data throughout all periods of archiving. According to OrganizationE, “we are still working on that. But I know there are loopholes, and all of that, but it’s something that we’re still working on”.

Furthermore, some organizations had little to no enforcement for electronic data retention, while others, like OrganizationE, retained all electronic data. OrganizationRID noted, “right now, all data is retained”. He added, “even if a user exits the system, the data that he or she worked with remains retained on the system”. Data retention in OrganizationC depends on available space, as explained by RespondentJNW, “there’s a data retention period, I think between 7 to 10 years or thereabout, but not less than seven years for physical documents

as per laws”. He added, “It all depends on the available space you're able to provide in the cloud”. OrganizationC also relied on a third party for electronic data retention compliance. According to RespondentAAR, “we rely on the third party, Microsoft, that houses our data in the cloud and what we do is to make data available anytime”. OrganizationA depended on the default data retention settings of third-party systems. RespondentNMU stated, “we use Microsoft default data retention mechanisms for the ones that are stored in the cloud infrastructures. And for the ones that are stored in the cloud storage in the OneDrive, we also rely on the Microsoft default setting”. Regarding data disposal, OrganizationC securely disposes of sensitive data by retaining hard drives or destroying hard drives and USB flash drives.

The varied approaches across pharmaceutical organizations underscore the data resilience challenges inherent in operating within modern IT ecosystems.

Data resilience is crucial for ensuring the continuous availability of critical data within pharmaceutical organizations. Data availability controls are essential for drug manufacturing to prevent disruptions and maintain business continuity. Best practices include RPOs based on the criticality of data (ISACA, 2019), implementing automated backup and recovery solutions, regularly testing data recovery processes, establishing data retention processes and periods that comply with industry regulations, and employing policies and procedures to control access, modifications, and transmission of historical and archived data (ISACA, 2018a; CIS Critical Security Controls Version 8, n.d.). Data backup, recovery, retention, and archiving ensure that data can be accessed and used when needed (CIS Critical Security Controls Version 8, n.d.). The frequency of data backups and recovery points is determined by the recovery point objective RPO (Chapple et al., 2018), which reflects the acceptable data loss an organization can tolerate. If data becomes inaccessible, data recovery can restore lost or corrupted data from backup or storage media. However, the



effectiveness of data recovery relies on the protection of the data intended for recovery. Testing recovery processes ensures that data recovery functions when needed. Additionally, a robust data retention policy supports data recovery efforts. Drug manufacturing organizations must guarantee that data is retained for the required period and deleted at the end of that period. The retention period is often dictated by legal or regulatory requirements, as well as business needs. Furthermore, archiving enables organizations to meet legal and regulatory obligations for data retention. However, the responsibility for data stored in a third-party archived facility ultimately depends on the terms of the contract between the data owner and the service provider.

Additionally, the maximum duration a business can tolerate being without access to its critical systems and applications before it starts to experience severe consequences, known as the RTO (Chapple et al., 2018), is an essential consideration when accessing data from legacy systems and addressing the risk of DoS attacks. One of the quickest methods to access data from a legacy system is via direct access to an API. In contrast, a DoS attack leads to the unavailability of systems or services, thereby affecting its RTO. Nevertheless, intrusion prevention and detection systems assist in detecting and preventing DoS attacks. Establishing RPOs and RTOs is crucial for ensuring data availability, and senior leadership plays a vital role in this endeavor.

However, the differing approaches to ensuring data availability, with some pharmaceutical organizations maintaining lengthy data recovery points for risks such as third-party closures or bankruptcies, while others have unclear scopes and frequencies for data recovery tests, create a data security gap. Furthermore, the minimal enforcement of electronic data retention by certain pharmaceutical organizations and a shift in the risk of alteration or loss of archived data to third parties by others highlight a lack of control and oversight.

**Data Privacy Vulnerabilities in External Systems.** Pharmaceutical organizations employ a variety of practices to ensure data confidentiality in third-party systems and data storage. These include evaluating external system controls for data privacy through information requests, relying on NDAs to encrypt data held with third parties, utilizing cloud provider encryption for stored and in-transit data, and qualifying supply chain partners via confidentiality agreements.

OrganizationD based its assessment of third-party system controls for data confidentiality on requests for information. According to RespondentSNW, “we try to get this information from third parties, contractors, vendors, and partners to ensure that their systems are protected and have adequate levels of protection”. Additionally, OrganizationB depended on NDAs with third parties for encrypting data at rest. RespondentCIG stated, “we leverage more on the non-disclosure agreement signed with such vendors”, and added, “we leverage more on the security control that is built into Office 365”. Also, OrganizationA relied on CSP encryption for data at rest. RespondentAAI explained, “for physical data stored on the cloud, we rely on the vendor default encryption”. However, data at rest was unencrypted on OrganizationA’s premises. According to RespondentAAI, “for data stored on-premise, we don’t use any form of encryption to protect them. They are just stored as they are generated”. What’s more, OrganizationA relied on the cloud service provider’s encryption for data in transit. RespondentAAI maintained, “we also rely on the built-in TLS encryption by the vendor for this transmission”.

The practices reveal that pharmaceutical organizations relied heavily on the controls of their third-party partners for data confidentiality.

Data hosting by third parties provides advantages such as cost savings, scalability, and the delegation of infrastructure management tasks. The confidentiality of sensitive data, whether stored on-premise or on third-party platforms, is crucial in drug manufacturing.

Ensuring stakeholder trust in data residing in external systems necessitates a comprehensive approach to data privacy. Sensitive data should be encrypted to maintain its privacy. Best practices include employing strong encryption protocols to protect data at rest, in use, and in transit (Cybersecurity Audit Program, n.d.; CIS Critical Security Controls Version 8, n.d.; ISACA, 2012), as well as anonymizing or de-identifying patient-level data when sharing clinical trial information with third-party researchers. As such, pharmaceutical organizations must establish consistent encryption practices for all data, irrespective of its storage location—whether on local systems or in the cloud. Additionally, effective anonymization and de-identification techniques should be rigorously applied to ensure that shared data cannot be traced back to individual patients, thereby maintaining privacy and compliance with ethical and regulatory standards. Pharmaceutical organizations must also conduct thorough evaluations of third-party systems, assessing their access controls, encryption measures, and overall security stance (ISACA, 2019; Khan et al., 2025). However, the evaluation of third-party system controls for data confidentiality—based on requests for information from some pharmaceutical organizations—indicates a partial assessment and a reactive approach to safeguarding data confidentiality. Such partial assessments of third-party system controls, along with reliance on vendor-built security measures, reveal shortcomings in ensuring data confidentiality.

**Data Integrity Gaps in Operations and Supply Chain.** Pharmaceutical organizations use various strategies to ensure data security and integrity throughout their supply chain and operational processes. OrganizationA qualified its supply chain partners through confidentiality agreements. RespondentOAD confirmed that due diligence checks were performed on vendors, stating, “when we assess and qualify our vendors and supply chain partners, we decide the kind of information we give them. If corporate company organization, they sign a non-disclosure agreement”. Regarding data integrity checks, OrganizationB lacked

measures to review or verify the integrity of electronic data. According to RespondentAIG, “we do not have any technical means for doing that but it’s one of those things that we also want to put in place”. Also, OrganizationE did not have adequate measures to ensure both the completeness and accuracy of data, nor did they guarantee the complete and correct transfer of data. RespondentAAJ mentioned, “we haven’t had to deal with that”. Furthermore, OrganizationE did not have measures in place to prevent production systems from processing test data. RespondentAAJ remarked, “we haven’t had this challenge”. What’s more, OrganizationD considered implementing non-repudiation to ensure the authenticity and integrity of transactions. According to RespondentSNW, “emails sent from our domain can be trusted as having come from us as the source and haven’t been tampered with. So, we are working on that too to ensure that this is put in place”.

Despite these varied approaches, the lack of sufficient electronic data integrity checks and safeguards against test data in production systems emphasizes the need for measures to address data integrity gaps in operations and supply chain management.

The importance of data integrity in drug manufacturing operations cannot be overstated. Data integrity is essential for maintaining the quality and safety of pharmaceutical products (Khan et al., 2025). It is crucial in drug manufacturing to ensure that data is both accurate and trustworthy. Pharmaceutical organizations must implement stringent data integrity controls to guarantee that data remains reliable throughout the manufacturing process. Best practices include conducting data integrity checks at various processing stages (ISACA, 2019; Cybersecurity Audit Program, n.d.) to uphold the quality and trustworthiness of data used in decision-making and regulatory compliance. These checks prevent the processing of test data in production systems, ensure the accurate transfer of data between systems, and verify the integrity of the data itself. Strong data integrity practices are vital for maintaining stakeholder trust and confidence in a pharmaceutical

organization's products and processes. However, differing levels of data integrity assurance across organizations indicate a security gap, with some lacking measures to prevent production systems from processing test data, verify electronic data integrity, and ensure accurate data transfer.

**Inadequate Data Security Monitoring.** Data security monitoring was inconsistently implemented across various organizations with partial implementation of audit trails, limited review processes, undetected data alterations, anomaly-based log analyses, a narrow scope of log monitoring, erasure of audit trails, and disabled audit trail functionalities. Audit trails were implemented in some systems within OrganizationD. RespondentAOL stated that audit trails were deployed on critical systems, “but we're working to get granular so that we can also monitor activities on individual systems”. AAlso, there was little to no review of these audit trails. RespondentAOL confirmed, “that isn't happening yet. But hopefully, very soon, we'll be able to put that in place along with every other thing”. Although some Software-as-a-Service offerings from certain CSPs included audit trails, they did not capture data modifications. RespondentCNW from OrganizationA noted, “when it comes to modification of data, we don't get such notification”.

He further emphasized that logs are reviewed only when anomalies are detected in OrganizationA. RespondentCNW mentioned, “if it is not an anomaly, we don't bother reviewing the audit trail because the audit trail is a huge file that even when you are looking, you don't know what you're what you're searching for”. Log review was of limited scope in OrganizationC. RespondentIAM pointed out this shortcoming, stating that, “the compensating control we have for that is the use of a monitoring tool. The monitoring tool in place checks for the network generally but it does not address data-related events, which is a bad thing”. Logs and audit trails were also deleted periodically within OrganizationC. RespondentJNW indicated, “every six months we purge the audit trails on the database. And then again, the

backup that we take gets overwritten after certain days”. Moreover, audit trail functionality was disabled. According to RespondentIAM, “Audit trail is not enabled. And we have been on it. The IT Department claims that they don't have enough space for it”. Regarding the verification of audit trail functionality, she added, “this audit trail has been an issue, but I believe we are going to rectify it very soon since the external auditors booked the organization for its lack”. These practices highlight the necessity for improved audit trail management and data security monitoring solutions.

Effective data security monitoring is crucial for detecting unauthorized access or breaches. Logs and audit trails are vital for monitoring and investigating security incidents. Best practices include implementing comprehensive logging mechanisms to capture relevant events and activities, as well as conducting regular log reviews (ISACA, 2012b; CIS Critical Security Controls Version 8, n. d.). Audit trails are particularly important for tracking changes to data and identifying potential security incidents (ISACA, 2019). Therefore, pharmaceutical organizations must adopt comprehensive monitoring solutions that encompass audit trails, log monitoring, and routine reviews of data-related activities. By collecting and analyzing this information, drug manufacturing organizations can pinpoint potential security threats, detect security incidents, and enact measures to prevent unauthorized access to sensitive data (Chapple et al., 2018). Logging and monitoring also aid in assessing the effectiveness of access controls. Recording access, modification, and disposal of sensitive data are essential components of data security that ensure sensitive information remains protected (CIS Critical Security Controls Version 8, n. d.). However, the inconsistent review of audit trails and disabled functionality in some pharmaceutical organizations highlights a gap in monitoring and tracking data-related activities.

**Challenges Prioritizing Data Security and Response.** The effectiveness of security measures varied significantly across pharmaceutical organizations, influenced by resource

availability and management's commitment to addressing data security issues. In OrganizationA, the security applications installed on individual devices determined the security status of those devices. RespondentCCH noted that a designated individual was responsible for monitoring and responding to security incidents, as well as conducting security assessments. He explained that “he is part of the team that works on the vulnerability and penetration test that assesses our level of exposure and close all the gaps”. In OrganizationB, the data security audit was under-resourced. RespondentENW claimed, “the only software that I use, I brought it myself”. Additionally, there were instances where both the auditee and management in OrganizationC failed to act on recommendations made in audits, particularly regarding issues of audit trail functionality. RespondentIAM expressed her frustration, “we are fighting a battle and I hope we win. We are still on it. It is always in our audit report.

These disparities highlight the challenges in prioritizing data security and response.

Prioritizing data security and response is crucial for managing potential risks and safeguarding sensitive data. Regular audits are vital for enhancing an organization's security posture. Data security audits assess current practices and offer feedback for improvement. Best practices include providing auditors with ongoing training in new techniques and emerging technologies to enhance their skills, as well as a robust program established by management for implementing corrective actions (ISACA, 2019). Therefore, pharmaceutical organizations must dedicate adequate resources to conduct comprehensive security audits and address identified vulnerabilities. Executives and their teams should also work closely with auditors to investigate all highlighted data security issues and collect feedback on these matters to strengthen security measures (Jiao, 2020). Such collaboration ensures that necessary security measures are executed, potential threats are consistently monitored, and security protocols are routinely updated to address emerging risks. However, inadequately resourced data security audits in certain pharmaceutical organizations, along

with the inaction of auditees and management regarding audit recommendations in others, demonstrate a lack of prioritization for data security audits and, consequently, a significant data security gap.

Overall, there were significant gaps and inconsistencies in data security practices across various organizations within the Nigerian pharmaceutical industry. These gaps are evident in multiple aspects of data security, including risk assessment, management processes, software integrity, third-party risks, and more. We anticipated that certain practices would not align with data security best practices due to the lack of established standards. Regulatory authorities in sub-Saharan Africa encounter challenges in enforcing basic regulations (Giralt et al., 2017), much less specifying data security standards. Consequently, some drug manufacturers depend on self-developed practices, resulting in substantial data security gaps in drug manufacturing. Furthermore, drug manufacturers face obstacles like inadequate infrastructure, unreliable power supply, outdated technology, and a weak engineering foundation (Adigwe & Onavbavba, 2024; Akande-Sholabi & Adebisi, 2020), which divert their focus and resources away from ensuring data security. The resources made available after addressing these challenges are then redirected toward data integrity, which is a priority for the industry regulator. The study's findings align with the theoretical framework, emphasizing that effective data management practices, guided by management controls and data security best practices, are essential for protecting sensitive pharmaceutical data.

The lack of standardized practices and uniform implementation of security measures presents a significant risk to sensitive data in Nigeria's pharmaceutical industry, as some drug manufacturing companies do not adhere to best practices. This assessment emphasizes the need for an industry-wide model to ensure the effectiveness and consistency of data security practices. It also highlights the importance of strong internal audits and proactive



management of data security risks to prevent potential breaches.

### 4.3.3 Alignment between Guidelines and Practices

A comparative analysis of guidelines and real-world practices assessed their alignment in terms of data security. By assessing practices against these guidelines, we can determine the extent to which industry standards influence drug manufacturing operations regarding data security. Table 12 and Figure 40 present an evaluation and distribution of alignment between guidelines and practices related to data security.

Critical areas such as data management processes, data flow, data access control lists, role-based access control, data retention, data recovery processes, data recovery tests, data encryption, service provider logs, and monitoring of service providers show varying degrees of alignment. Current practices for data inventory, isolation for data recovery instances, protection of recovery data, data classification, data loss prevention, and segmentation of data processing and storage indicate areas of data security that require urgent attention. We examined the key points highlighted in the table:

**Table 12**

*Alignment of Guidelines and Practices in terms of Data Security Controls*

Data security control	Guidelines	Management practice	Degree of Alignment
Data management process	<ul style="list-style-type: none"> <li>• Data governance program</li> <li>• Technology-backed data management.</li> <li>• Data policies, documentation, quality, and security</li> </ul>	<ul style="list-style-type: none"> <li>• Technology-driven, access-controlled data management process.</li> <li>• Cloud-based, high-availability data management</li> <li>• Presumed data ownership.</li> </ul>	<ul style="list-style-type: none"> <li>• Partial</li> </ul>
Data inventory	<ul style="list-style-type: none"> <li>• Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>• Not practiced</li> </ul>	<ul style="list-style-type: none"> <li>• Significant gap</li> </ul>
Data flow	<ul style="list-style-type: none"> <li>• Data flow documentation</li> <li>• Data flow visualization</li> <li>• Data flow map</li> <li>• Data flow evaluation</li> </ul>	<ul style="list-style-type: none"> <li>• Not practiced</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal</li> </ul>
Data access control lists	<ul style="list-style-type: none"> <li>• Authorized access</li> </ul>	<ul style="list-style-type: none"> <li>• Authorized and approved access request</li> </ul>	<ul style="list-style-type: none"> <li>• Strong</li> </ul>
Role-based access control	<ul style="list-style-type: none"> <li>• Least-privilege rule for user access</li> </ul>	<ul style="list-style-type: none"> <li>• Access provisioning based on role requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Strong</li> </ul>

Data security control	Guidelines	Management practice	Degree of Alignment
	<ul style="list-style-type: none"> <li>• Role-based access</li> </ul>		
Data retention	<ul style="list-style-type: none"> <li>• Data retention process</li> <li>• Records retention period</li> <li>• Policies and procedures for data and audit trail retention following defined retention periods</li> </ul>	<ul style="list-style-type: none"> <li>• Reliance on third parties for electronic data retention compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal</li> </ul>
Data backup	<ul style="list-style-type: none"> <li>• Routine backups</li> <li>• Backup and restoration validation process.</li> <li>• Documented procedures for Periodic backup and archiving of data</li> </ul>	<ul style="list-style-type: none"> <li>• Hybrid data backup storage</li> </ul>	<ul style="list-style-type: none"> <li>• Strong</li> </ul>
Data recovery process	<ul style="list-style-type: none"> <li>• Complete and timely data recovery</li> </ul>	<ul style="list-style-type: none"> <li>• Extended RPO for third-party data risks</li> <li>• Technology-driven recovery objectives.</li> </ul>	<ul style="list-style-type: none"> <li>• Partial</li> </ul>
Data recovery test	<ul style="list-style-type: none"> <li>• Periodic data recovery test from archive, third-party storage, and storage locations</li> </ul>	<ul style="list-style-type: none"> <li>• Inadequate clarity on data recovery test scope and frequency.</li> <li>• Inadequate measures for continued readability in data archives.</li> <li>• Insufficient accountability for loss or alteration of data in outsourced archives</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal</li> </ul>
Protection of recovery data	<ul style="list-style-type: none"> <li>• Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>• Not practiced</li> </ul>	<ul style="list-style-type: none"> <li>• Significant gap</li> </ul>
Isolation of data recovery instance	<ul style="list-style-type: none"> <li>• Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>• Not practiced</li> </ul>	<ul style="list-style-type: none"> <li>• Significant gap</li> </ul>
Data Disposal	<ul style="list-style-type: none"> <li>• Documented data disposal process</li> <li>• Data disposal procedures</li> </ul>	<ul style="list-style-type: none"> <li>• Retain hard drives.</li> <li>• Destroy hard drive and USB flash</li> </ul>	<ul style="list-style-type: none"> <li>• Partial</li> </ul>
Service provider logs	<ul style="list-style-type: none"> <li>• Contract giver's data access and audit trail for auditing</li> </ul>	<ul style="list-style-type: none"> <li>• Partial implementation of audit trails</li> <li>• Limited audit trail review</li> <li>• Undetected data alteration</li> <li>• Anomaly-based log analysis</li> <li>• Limited scope of log monitoring</li> <li>• Erasure of audit trails</li> <li>• Disabled audit trail functionality</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal</li> </ul>
Monitoring of service providers	<ul style="list-style-type: none"> <li>• Ongoing qualification of supply chain</li> </ul>	<ul style="list-style-type: none"> <li>• Presumed uninterrupted access</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal</li> </ul>

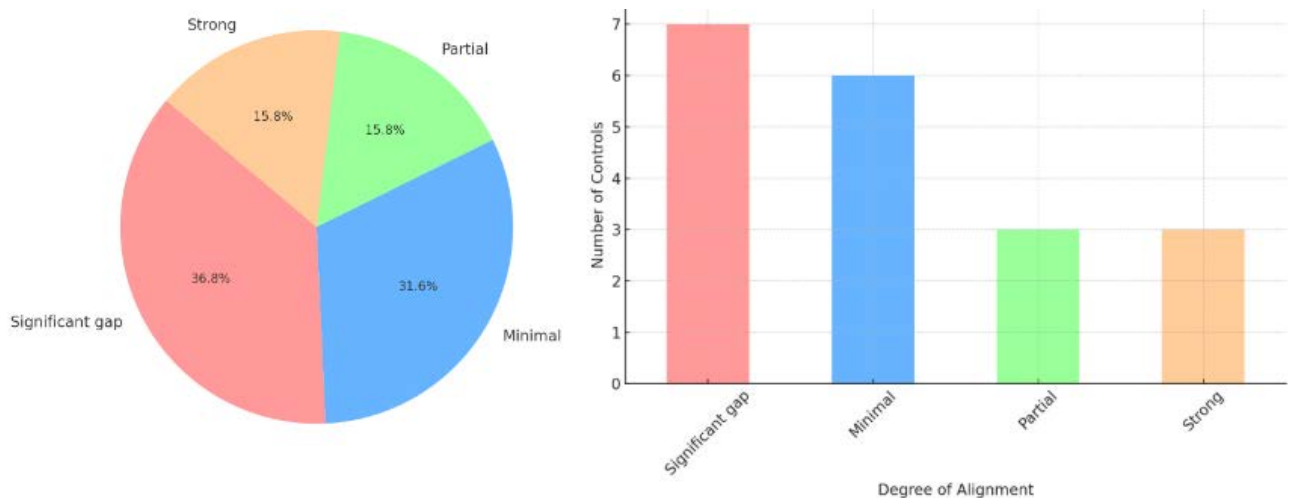
<b>Data security control</b>	<b>Guidelines</b>	<b>Management practice</b>	<b>Degree of Alignment</b>
	partners and outsourced activities <ul style="list-style-type: none"> <li>• Establishment of quality metrics for risk identification</li> <li>• Evaluation of contract acceptors per documented risk evaluations.</li> <li>• Compliance audit</li> <li>• Data and procedure reviews</li> </ul>	to globally stored data. <ul style="list-style-type: none"> <li>• Due diligence checks employed for GMP adherence and data integrity in the supply chain.</li> <li>• NDAs with vendors for data integrity communication</li> <li>• Consideration for GDPR compliance for data held in multiple locations.</li> <li>• SLAs and access controls employed to mitigate risks in contracts, supply chains, and outsourcing.</li> <li>• SLAs and informal methods are key to monitoring third-party service levels.</li> <li>• Insufficient data protection during third-party shutdowns or bankruptcies.</li> <li>• NDAs with service provider to control post-contract data access.</li> </ul>	
Decommissioning of the service provider	<ul style="list-style-type: none"> <li>• Not specified</li> </ul>	<ul style="list-style-type: none"> <li>• Not practiced</li> </ul>	<ul style="list-style-type: none"> <li>• Significant gap</li> </ul>
Data classification	<ul style="list-style-type: none"> <li>• Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>• Absence of data classification scheme</li> </ul>	<ul style="list-style-type: none"> <li>• Significant gap</li> </ul>
Data loss prevention	<ul style="list-style-type: none"> <li>• Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>• Absence of data loss prevention solutions</li> <li>• USB drive usage controlled by domain policy.</li> <li>• Uncontrolled use of USB drives</li> </ul>	<ul style="list-style-type: none"> <li>• Significant gap</li> </ul>
Data encryption at rest, in transit, on removable media, and in end-user devices	<ul style="list-style-type: none"> <li>• Encryption employed for data confidentiality and integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Evaluation of external system controls for data privacy through information requests.</li> <li>• Dependence on non-disclosure agreement for encrypting data held with third-party.</li> <li>• Dependence on cloud provider encryption for stored and in-transit data.</li> <li>• Unencrypted stored data.</li> </ul>	<ul style="list-style-type: none"> <li>• Minimal</li> </ul>

Data security control	Guidelines	Management practice	Degree of Alignment
		<ul style="list-style-type: none"> <li>Supply chain partner qualification via confidentiality agreements.</li> </ul>	
Segmentation of data processing and storage	<ul style="list-style-type: none"> <li>Unspecified</li> </ul>	<ul style="list-style-type: none"> <li>Not practiced</li> </ul>	<ul style="list-style-type: none"> <li>Significant gap</li> </ul>

**Data Management Process.** The alignment of management practices and guidelines is partial. The guidelines emphasize the importance of a robust data governance program, which includes defining roles, responsibilities, and processes related to data handling, implementing policies for data quality and security, as well as providing technology support. The management practice involves technology-driven data management processes and cloud-centered approaches.

**Figure 40**

*Distribution of Degree of Guideline/Practice Alignment*



**Data Inventory.** One notable data security gap exists concerning data inventory. Both guidelines and management practices failed to address data inventory. The guidelines lack specific requirements for data inventory, leaving room for interpretation. Similarly, the management practices do not provide any insight into the establishment and maintenance of data inventories.

**Data Flow.** The guidelines require data flows to be visualized and documented.

Unfortunately, the management practices do not appear to align with this requirement, as they do not maintain data flow documentation.

**Data Access Control Lists.** The alignment of the guidelines and management practices regarding authorized data access is strong. Controlled access guarantees that only authorized individuals can access sensitive data.

**Role-based Access Control.** The principle of least privilege for data access is a vital aspect of data security. This concept is clearly emphasized in the guidelines, and management practices align with this provision by highlighting authorized and approved access requests.

**Data Retention.** The guidelines outline the requirements for a data retention process, specify record retention periods, and detail policies and procedures for retaining data and audit trails according to defined retention periods. Management practices partially align with these standards by depending on third parties for electronic data retention compliance.

**Data Backup.** Both guidelines and management practices highlight routine backups and validation procedures, which is a strong alignment. Regular backups, validation procedures, recorded backups, and archiving processes are essential for data recovery and business continuity.

**Data Recovery Process.** The alignment between the guidelines and management practices is strong regarding data recovery processes. Both stress the importance of complete and timely data recovery, which is essential for maintaining the availability of pharmaceutical data.

**Data Recovery Test.** The guidelines and management practices regarding data recovery processes are strongly aligned. Both stress the importance of thorough and timely data recovery, which is vital to preserving the availability of pharmaceutical data.

**Protection of Recovery Data.** The guidelines did not require the protection of recovery data, and management practices did not incorporate measures for safeguarding recovery data.

This highlights a significant gap in data security.

**Isolation of Data Recovery Instance.** The guidelines did not require isolating data recovery instances, and management practices lacked measures for this isolation, highlighting another significant gap in data security.

**Data Disposal.** Both guidelines and management practices partially align regarding data disposal. While retaining and destroying hard drives and USB flash drives is a reliable method for disposing of sensitive data, having documented data disposal processes and procedures is crucial for ensuring the permanent and secure removal of sensitive data when it is no longer needed.

**Service Provider Logs.** The guidelines emphasize the importance of contract givers obtaining access to data and audit trails for auditing purposes. However, management practices did not adequately address access to service provider logs, which highlights a gap in alignment.

**Monitoring of Service Providers.** Both guidelines and management practices emphasized risk assessment and the qualification of supply chain partners and outsourced activities. However, the establishment of quality metrics and ongoing inspections were not practiced adequately. This alignment is only partial. Also, inadequate measures to ensure data access following the bankruptcy or closure of a third party create data security gaps between guidelines and practices.

**Decommissioning of Service Provider.** The guidelines did not address secure decommissioning of service providers, and management practices lacked effective procedures for this process. While the reference to NDAs with service providers to monitor data access after contract termination is a positive step, it may require additional measures. This significant gap raises concerns regarding data management when relationships with service providers conclude.

**Data Classification.** Neither the guidelines nor management practices addressed data classification. The lack of data classification schemes creates a significant data security gap.

**Data Loss Prevention.** Both guidelines and management practices failed to address DLP, indicating a significant data security gap. Uncontrolled data sharing, the use of USB drives without management oversight, and the absence of DLPSs pose serious concerns.

**Data Encryption.** The alignment between the guidelines and management practices concerning data encryption was minimal. The guidelines highlighted the necessity of using encryption to ensure data confidentiality and integrity. Although NDAs and encryption by cloud service providers may provide some protection, unencrypted data stored on-site indicates a significant gap in data security.

**Segmentation of Data Processing and Storage.** Neither the guidelines nor the management practices addressed data segmentation. This absence of segmentation represents a significant gap in data security.

**Service Provider Logs.** Although the guidelines emphasize the necessity for contract givers to access data and audit trails for auditing purposes, management practices reveal a lack of alignment in the implementation of audit trails and reviews. Disabled audit trail functionality, limited log monitoring, untracked data modifications, and periodic deletion of audit trails highlight a deficiency in the monitoring and auditing of data access and modifications.

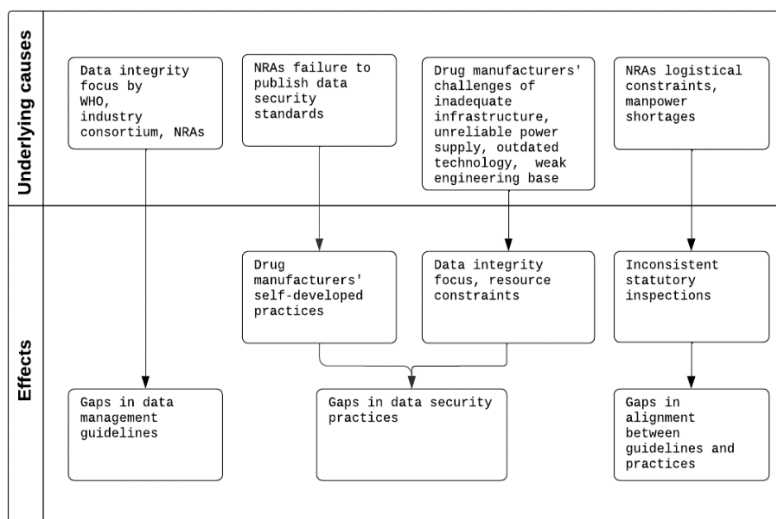
Overall, the alignment of data management practices with the guidelines regarding data security showed variations across different aspects, including areas that were strongly aligned, partially aligned, minimally aligned, or had significant gaps. We anticipated these results because Nigerian pharmaceutical organizations do not adequately adhere to GMP standards. According to Adigwe (2023), no Nigerian pharmaceutical company is listed on the WHO prequalified list, a benchmark for evaluating drug manufacturers' compliance with GMP. This

gap highlights the role of industry regulators in ensuring that pharmaceutical manufacturers meet international GMP standards. However, NAFDAC and other sub-Saharan African drug regulators face challenges in effectively performing their core regulatory functions (Giralt et al., 2017). For instance, government regulatory officials are responsible for conducting GMP inspections of pharmaceutical manufacturers. Unfortunately, these statutory inspection schedules are not consistently adhered to due to challenges like logistical constraints and manpower shortages (Adigwe & Onavbavba, 2024). The study's findings align with the theoretical framework, demonstrating that positive outcomes, such as GMP compliance, occur when management practices are influenced by management controls designed to ensure regulatory compliance. Addressing these gaps and improving alignment is crucial for protecting pharmaceutical data, enhancing medicine security, and achieving a more thorough GMP inspection. This approach may involve the implementation of specific data security policies, practices, and technologies to tackle the alignment gaps identified in Table 12.

#### **4.3.4 Root-Cause Analysis of Data Security Gaps**

Figure 41 illustrates the root causes contributing to data security gaps in Nigeria's pharmaceutical industry.



**Figure 41***Root Causes of Data Security Gaps*

These causes include the lack of attention given to data security by public health organizations such as the WHO, industry consortia like PIC/S, and NRAs, as well as the absence of data security standards, challenges faced by NRAs, and difficulties encountered by drug manufacturers. Addressing these issues is essential for strengthening the industry's data security framework.

**Summary**

Chapter 4 of this study emphasized the importance of reliable and valid measures for accurately representing a research concept accessed. Reliability issues in qualitative research were noted that stem mainly from the researcher's involvement in the study, particularly during interviews. The chapter pointed out the challenges of achieving reliability in in-depth, semi-structured, or unstructured interviews as opposed to structured ones. Additionally, it highlighted the focus of qualitative research in providing a comprehensive understanding of life and behavior within groups rather than strictly adhering to validity norms.

This chapter discussed the trustworthiness of data, acknowledging that traditional concepts of reliability and validity in quantitative research do not apply to the study. Instead,

trustworthiness was achieved based on confirmability, credibility, dependability, and transferability. Confirmability required demonstrating that findings are derived from data rather than researcher bias. Credibility ensured that the research findings accurately reflect the participants' perspectives. Dependability involved showing the consistency of data over time, while transferability addresses the applicability of the study's findings in different settings. The study employed various methods, such as triangulation, member checks, and iterative questioning to achieve these aspects of trustworthiness, thereby ensuring the relevance and integrity of its findings. The research participant group comprised 31 individuals, primarily men (84%), with women accounting for 16% of the respondents. A significant portion, 61%, fell within the 31-40 age range. Participants were exclusively from the Nigerian pharmaceutical industry, with most (61%) holding mid-level positions in their organizations. A notable characteristic of the participant organizations was their ISO 9001 certification, suggesting that they had received training in quality management systems. However, none of these pharmaceutical organizations held ISO 27001 certification, indicating that their employees may not be familiar with information security management systems.

A comprehensive review of the data security provisions and gaps in health authorities' guidance documents, particularly from PIC/S and WHO, was conducted. Qualitative content analysis examined the guidelines published by these bodies, which highlighted their requirements for ensuring data security in the pharmaceutical industry. A critical evaluation of these guidelines revealed both provisions and gaps in data security relevant to this sector. The need for robust data management was emphasized in the PIC/S and WHO guidance documents, which stipulated the establishment and maintenance of comprehensive processes that include various activities such as policy development, documentation, quality control, and security measures. This approach reflects a holistic perspective on data management, encompassing data governance and the use of technology. However, a significant gap was

identified in the guidance documents concerning the maintenance of detailed data inventories. Although PIC/S mentioned computerized systems, it did not specifically address the need for a comprehensive data inventory, underestimating the importance of tracking and managing data assets, which are crucial for data integrity and security—an area that could be improved in future guidelines. Emphasis was placed on documenting and visualizing data flows, considered essential tools for understanding and mitigating the risks associated with computerized systems. The flow encompassed the movement of electronic data and its associated metadata, from the moment of creation to the archiving and retrieval processes. Graphical representations and data flow maps were highlighted as valuable tools for comprehending the intricacies and vulnerabilities of interface systems. PIC/S and WHO (2016) guidance documents acknowledged that data flows are crucial. However, variations existed in the level of detail provided. PIC/S prioritized creating and evaluating data flow maps, while WHO (2021) lacked mandates for visual representation or documentation, which potentially led to gaps in managing data movement and associated risks. Access control emerged as a crucial theme, with the guidance documents recommending strict measures to prevent unauthorized data modification. Establishing data access control lists and implementing role-based access controls were advised as essential strategies for ensuring data integrity. The guidelines advocated for restricting access to sensitive data only to those with the necessary authorization, adhering to the principle of least privilege. The PIC/S and WHO documents addressed data access control, emphasizing the importance of preventing unauthorized access and ensuring proper authorization, in line with fundamental data security principles. Notably, the newer versions of the guidance documents stress the need for role-based access control, significantly improving the alignment of access and privileges with individual roles and responsibilities. Data retention and backup were identified as critical components of data security. The guidance documents provided clear recommendations,

emphasizing the importance of preserving data, metadata, and records over time for quality and regulatory purposes. They highlighted the necessity of regular backups, particularly in remote areas, to safeguard against disasters. Additionally, they recommended validation processes for these backups and restoration procedures to ensure data availability even in worst-case scenarios. Emphasis was also placed on data recovery processes, highlighting the need for complete and timely data recovery in the event of a disaster. Although the WHO (2016) guidance document did not specify a process for data recovery, it suggested regular tests to assess the ability to retrieve archived electronic data, underscoring the importance of testing recovery mechanisms. Provisions for data availability controls highlight the need for regular backups, validating backup processes, and consistently testing data recovery capabilities, all of which are essential for ensuring business continuity and data availability. A crucial aspect is the secure disposal of data after the retention period. Procedures and processes for disposing of electronically stored data were recommended to ensure it is eliminated appropriately and securely when no longer needed. The PIC/S document provided guidelines for data disposal, highlighting the importance of proper data disposal to prevent breaches. WHO (2016) emphasized risk control during the data life cycle, whereas WHO (2021) did not include specific instructions for data disposal, indicating a gap. The monitoring of service providers was seen as a critical area, with guidance recommending risk assessment and ongoing qualification of supply chain partners and outsourced activities. This requirement included reviewing the procedures and data held by contractors to ensure compliance with data integrity and management principles. Service provider monitoring stressed controlling data integrity risks and ensuring adherence to quality standards, even with outsourcing. Access to electronic records and audit trails by contract givers was deemed essential for compliance assessments and demonstrations. The guidance documents addressed collecting and accessing logs from service providers for audit purposes, which is vital for transparency

in outsourcing and compliance evaluation. Although encryption was noted as a key security measure for maintaining data confidentiality, the WHO (2021) and PIC/S (2021) documents did not offer comprehensive guidelines. Additionally, the guidance documents lacked a complete set of guidelines for data classification, loss prevention, and the segmentation of data processing and storage. These gaps, along with the absence of specific protocols for securely decommissioning service providers, highlight missed opportunities for enhancing data security practices.

A range of data security gaps were revealed through thematic analysis of respondents' insights into drug management practices in the Nigerian pharmaceutical industry. These gaps were categorized into multiple categories themes: challenges in data classification and loss prevention; ineffective data risk assessment; immature tech-centric data management; data ownership assumptions and unchecked data sharing; data governance challenges and risk mitigation in a globally distributed environment; deficiencies in software integrity assessment; inconsistencies in network security measures and monitoring practices; USB security risks; challenges in system validation and configuration control; data resilience challenges in modern IT ecosystems; data privacy vulnerabilities in external systems; data integrity gaps in operations and supply chain; inadequate data security monitoring; challenges prioritizing data security and response. A significant disparity in data classification practices was observed among pharmaceutical organizations, with some lacking essential comprehensive classification schemes for effective DLP and systematic approaches to implement DLPSs. Data risk assessment practices varied significantly; in some instances, the frequency of assessments was neither specified nor informed by published assessment standards. This indicated a lack of rigor and uniformity in assessing potential data-related vulnerabilities in pharmaceutical organizations, leading to inconsistent and potentially inadequate risk management. The approaches to data management processes varied. Some

pharmaceutical organizations implemented high-availability, cloud-focused strategies that prioritized robust data backup and recovery mechanisms, while others leaned toward technology-based, access control-driven processes. The diverse data management strategies highlight the priorities and varying levels of maturity among pharmaceutical organizations in managing their data. This disparity also suggests a need for a more unified approach across platforms, as some methods failed to address critical areas. Data ownership and sharing issues were prominent as well, as in some cases, data ownership was only assumed, resulting in unrestricted data-sharing practices, especially when dealing with contract acceptors and supply chain partners. The ambiguity surrounding data ownership and unrestricted data sharing created potential security risks. Third-party data risks also presented challenges due to inconsistent management. Some pharmaceutical organizations conducted due diligence to communicate GMP requirements and reduce data integrity risks in supply chains. While several organizations employed due diligence checks for GMP communication and data integrity risk mitigation, others lacked sufficient measures to address data inaccessibility caused by third-party closures and did not have a comprehensive strategy to manage the impact of data stored in different geographical regions. The findings indicated a gap in effectively managing and protecting data held by third parties or on a global scale. Software and firmware integrity were maintained through practices that included minimal checks and controlled changes, highlighting the need for more rigorous verification methods to ensure security and integrity within organizations. Network security measures also varied, with some pharmaceutical organizations employing advanced strategies, such as intrusion prevention systems and firewalls, while others had less comprehensive security infrastructures, suggesting a lack of uniform standards. Another area of concern was the inconsistent control of removable media for data transfer, as some organizations strictly prohibited the use of USB drives, reflecting their awareness of the associated risks, while others were still debating their

policies on this matter. System validation processes differed among pharmaceutical organizations, with some relying on informal procedures and others using structured templates and checklists. The informal validation practices and absence of a standardized approach raised concerns about system robustness and identified gaps in ensuring that systems are functional and adequately secure. Additionally, data availability, recovery, archiving, and retention practices showed significant variations. Some pharmaceutical organizations had specific plans for managing data downtime risks, archiving, and retention, while others were less stringent in their strategies. Some pharmaceutical organizations had established strategies for addressing data unavailability risks, archiving, and retention, while others were more lax in their approaches. Data archiving and retention issues were evident, as some pharmaceutical organizations failed to enforce electronic data retention. These disparities, along with undefined scopes and frequencies for data recovery tests, indicated varying levels of preparedness and capability in effectively managing data life cycle processes. Inconsistent practices were also observed regarding data confidentiality, integrity, and auditing. Some pharmaceutical organizations relied on third-party systems and agreements to ensure data integrity and confidentiality, reflecting a reactive approach and a partial evaluation of third-party computer systems. Other pharmaceutical organizations lacked strong mechanisms to uphold the integrity of electronic data and featured inconsistent reviews of audit trails, indicating gaps in maintaining data accuracy and in documenting and monitoring data-related activities. Data security audits were under-resourced in certain pharmaceutical organizations, emphasizing a lack of prioritization of audit findings and recommendations. The inconsistency and variability in these areas underscored the need for more standardized and comprehensive approaches to data security in the Nigerian pharmaceutical industry.

An evaluation of the alignment between data management guidelines and practices concerning data security revealed varying levels of consistency. While the guidelines stressed

robust data governance, encompassing defined roles, responsibilities, and technological support, management practices were often influenced by access control or technology. Neither the guidelines nor management practices specified requirements or insights about data inventory practices, highlighting a significant gap. The absence of guidance left an essential aspect of data security unaddressed. The management practices did not sufficiently maintain data flow documentation as required by guidelines, reflecting a gap in managing and addressing data movement and its associated risks. Regarding authorized data access, both guidelines and management practices were closely aligned, focusing on controlled access to sensitive data. They effectively underscored the principle of least privilege for data access. However, the management practices did not meet the data retention requirements set forth by the guidelines, leading to issues with long data retention, which resulted in extended data recovery points and unclear data recovery tests. Both the guidelines and management practices were coherent in terms of data backups and validation procedures, emphasizing their importance for data recovery and ensuring business continuity. The data recovery processes were well-aligned, with guidelines and management practices stressing complete and timely recovery. Nonetheless, the guidelines did not specify the protection of recovery data, and the management practices lacked necessary measures, highlighting a data security gap. The data disposal processes in both the guidelines and management practices were aligned, ensuring the secure removal of data when it is no longer needed. However, management practices did not adequately cover the crucial elements of service provider logs and monitoring, which are vital for compliance and risk management. There were also gaps in the decommissioning of service providers, as management practices lacked sufficient decommissioning procedures, and the guidelines did not provide specific recommendations. Data classification, loss prevention, and encryption were areas that neither guidelines nor management practices addressed sufficiently, indicating serious data security gaps. The lack of data loss prevention



solutions, uncontrolled data sharing, the use of USB drives without management oversight, the absence of encryption for stored data, and the fact that data segmentation was not addressed presented significant security risks. Additionally, the implementation and review of access logs and audit trails were inadequate, revealing shortcomings in monitoring and auditing data access and modifications. A critical data security gap was highlighted due to the failure to perform software and firmware integrity checks. The alignment between drug manufacturing practices and guidelines varied, with some areas showing strong alignment, others partial, and several significant gaps. Overall, the level of alignment between drug manufacturing practices and guidelines regarding data security varied, with strong, partial, or minimal alignment, along with notable gaps identified in several areas.

These data security gaps in Nigeria's pharmaceutical industry arise from regulatory neglect, a lack of standards, and challenges faced by drug manufacturers. These gaps have implications not only from a business perspective but also regarding patient trust. Addressing these gaps and improving alignment with best practices is essential for ensuring the security of pharmaceutical data.

## **CHAPTER 5: IMPLICATIONS, RECOMMENDATIONS, AND CONCLUSION**

Data breaches in drug manufacturing organizations have had significant negative impacts on economies. This qualitative study sought to examine data security gaps within drug manufacturing and employed a multiple case study design, using a mix of purposeful sampling strategies suited to its exploratory nature. Data were collected through document reviews and semi-structured interviews after obtaining approval from the university's ethics committee. The final sample size was smaller than anticipated, which may limit the generalizability of the findings but enabled deeper, more nuanced exploration. Some respondents declined to answer certain questions, potentially affecting data analysis and interpretation; their decisions were respected, and follow-up interviews were conducted to understand their reluctance. Despite clarifying the research purpose and assuring confidentiality, some participants continued to withhold responses to sensitive questions. Furthermore, replicating this study in other pharmaceutical contexts may present challenges due to the specific operational environment and unique characteristics of Nigeria's pharmaceutical industry. These contextual factors may limit reproducibility and the transferability of the findings.

Chapter 5 synthesizes the study's key insights, presenting a structured discussion of implications, targeted recommendations, future research opportunities, and final reflections. It begins with an exploration of the broader implications of the findings for both theory and practice (Section 5.1), organized into three subsections. The first subsection examines implications for regulatory guidelines, identifying critical data security gaps in health authority provisions (Section 5.1.1). These include the absence of guidance on data inventory, weak or missing classification standards, insufficient directives for data loss prevention, limited segmentation of sensitive data, a lack of protocols for securely decommissioning service providers, and inadequate support for isolated and protected data recovery systems. Collectively, these deficiencies reveal systemic regulatory weaknesses that undermine security resilience. The section also brings attention to the implications for current pharmaceutical practices (Section 5.1.2). It explores the challenges posed by inadequate data classification, poor implementation of loss prevention strategies, and ineffective data risk assessment. Additional concerns include tech-immature data management processes, ambiguous data ownership, uncontrolled data sharing, and governance limitations within globally distributed environments. This section also underscores the impact of insufficient software integrity controls, inconsistent network and USB security practices, and weak configuration validation. Broader issues such as privacy vulnerabilities in third-party systems, unreliable supply chain data, and insufficient monitoring capacity are shown to heighten security risks across the data life cycle. Furthermore, data resilience challenges in modern IT ecosystems and difficulties in prioritizing data security and response further compound these operational vulnerabilities. These insights highlight the operational consequences of data governance failures and stress the need for robust, context-aware security controls. The third subsection assesses the alignment—or lack thereof—between regulatory expectations and practical implementation and their implications (Section 5.1.3). It highlights discrepancies between documented

standards and observed practices across critical control areas, including access management, retention, recovery, encryption, and third party oversight. This analysis reinforces the need to synchronize policy and practice to achieve consistent and effective data protection. Moving from implications to action, the chapter then introduces a suite of prescriptive recommendations tailored to different stakeholder groups (Section 5.2). High level recommendations are presented for international health organizations, industry consortia, and national regulators such as NAFDAC (Section 5.2.1), including updates to regulatory frameworks, standards publications, and GMP inspections. Specific guidance is also directed at Nigerian drug manufacturers (Section 5.2.2), addressing organizational, physical, and technological controls. The chapter's centerpiece is the introduction of the Pharmaceutical Industry Data Security Model, a structured framework for managing data security across technical and operational domains. The chapter details its validation process, demonstrating adaptability through real world feedback, use case simulations, and scenario based stress testing (Sections 5.2.3 and 5.2.4). Key attributes of the model include alignment with international standards, a modular design, and applicability to both regulatory and industrial contexts. A phased implementation strategy is then outlined, emphasizing gradual deployment (Section 5.2.5), followed by a discussion of cultural dimensions in implementation (Section 5.2.6). Factors such as power distance, uncertainty avoidance, and time orientation are explored for their potential influence on adoption and effectiveness. Looking forward, the chapter proposes future research directions (Section 5.3), including the exploration of AI, ML, and blockchain technologies to further strengthen data protection in the pharmaceutical sector. Finally, concluding reflections are offered (Section 5.4), summarizing the study's implications and contributions to academic theory and professional practice. The chapter demonstrates how theoretical and practical insights can inform scalable, real-world solutions while expanding

underexplored literature by situating pharmaceutical data security within a developing country context.

## **5.1 Implications**

The data security gaps present in both reference guidelines and drug manufacturing practices, highlights significant vulnerabilities in current frameworks. Issues such as ineffective data risk assessment, immature tech-centric data management processes, and challenges in data governance have implications for data security. Addressing these gaps is essential for enhancing data resilience in the pharmaceutical industry.

### **5.1.1 Implications of Data Security Gaps in Reference Guidelines**

Table 10 highlighted the data security gaps in the health authorities' guidance documents due to the absence of critical control provisions: data inventory, data classification, data loss prevention, segmentation of data processing and storage, secure decommissioning of service providers, and isolation and protection of recovery data. The lack of these provisions poses implications for the security of critical infrastructure within the pharmaceutical sector, as shown in Figure 42. First, the absence of guidance on data inventory may lead to a lack of visibility and control over data assets, inefficiencies, and data mismanagement. Second, the absence of direction regarding data classification creates ambiguity and inconsistency, potentially resulting in inadequate protection. Third, the lack of provisions for data loss prevention heightens the risk of unauthorized disclosure or data compromise. Fourth, insufficient guidance on the segmentation of data processing and storage creates a scenario in which a single security breach could jeopardize the data integrity of a drug manufacturer. Also, the absence of provisions for secure decommissioning of service providers increases the potential for residual data exposure or unauthorized access following the termination of service provider contracts. Lastly, the lack of provisions for isolated and protected data recovery instances raises concerns about the effectiveness of data recovery mechanisms in scenarios

involving data loss. Given the threat landscape, we anticipate that these gaps will hinder health authorities, such as NAFDAC, from effectively guiding data security practices in Nigerian drug manufacturing organizations.

### **5.1.2 Implications of Data Security Gaps in Drug Manufacturing Practices**

Table 11 highlighted the data security gaps in drug manufacturing operations: challenges in data classification and loss prevention; ineffective data risk assessment; immature tech-centric data management; data ownership assumptions and unchecked data sharing; data governance challenges and risk mitigation in a globally distributed environment; deficiencies in software integrity assessment; inconsistencies in network security measures and monitoring practices; USB security risks; challenges in system validation and configuration control; data resilience challenges in modern IT ecosystems; data privacy vulnerabilities in external systems; data integrity gaps in operations and supply chain; inadequate data security monitoring; challenges prioritizing data security and response. These gaps hinder the achievement of data security objectives and compromise the security of sensitive pharmaceutical data as well as overall patient safety, as illustrated in Table 13.

**Challenges in Data Classification and Loss Prevention.** Data traffic within pharmaceutical organizations poses potential risks for data loss. Without a structured classification scheme, these organizations struggle to prioritize data protection efforts, leaving highly sensitive information exposed. Additionally, failing to classify and prevent data loss increases the chances of unauthorized parties accessing and stealing sensitive data, thereby heightening the risk of data breaches. Furthermore, the lack of DLP mechanisms means potential leaks or unauthorized data transfers can go undetected, posing significant threats to IP. In an industry where data confidentiality is crucial, not deploying DLPSs can lead to data breaches, which may result in substantial financial losses and harm the reputation of drug

manufacturers. Moreover, the absence of data classification and DLPSs complicates incident response efforts, making it difficult to quickly identify and mitigate the effects of data breaches.

**Ineffective Data Risk Assessment.** Risk is ever-present. Inconsistent and insufficient data risk management increases vulnerability to data-related threats and undermines the overall data security posture. Moreover, without a standardized approach to risk assessment, various departments within a drug manufacturing organization may enact inconsistent security measures, creating gaps in the overall security framework. This inconsistency can lead to a fragmented security posture, making it difficult to enforce uniform policies and procedures. Furthermore, a lack of comprehensive risk assessment procedures suggests that a pharmaceutical organization may not fully understand the range of risks it faces, resulting in unidentified threats that could be exploited by malicious actors. This oversight can lead to significant financial losses, legal repercussions, and damage to an organization's public image.

**Figure 42***Implications of Data Security Gaps in Guidelines*

Absence of guidance on data inventory	Lack of direction regarding data classification	Lack of provisions for data loss prevention	Insufficient direction for segmentation of data processing and storage	Absence of provisions for secure decommissioning of service providers	Lack of provisions for isolated and protected data recovery instances
<ul style="list-style-type: none"> <li>•Lack of visibility and control over data assets</li> <li>•Inefficiencies</li> <li>•Data mismanagement</li> </ul>	<ul style="list-style-type: none"> <li>•Ambiguity and inconsistency, potentially leading to inadequate protection</li> </ul>	<ul style="list-style-type: none"> <li>•Heightens the risk of unauthorized data exposure or compromise</li> </ul>	<ul style="list-style-type: none"> <li>•A single security breach could compromise a drug manufacturer's data</li> </ul>	<ul style="list-style-type: none"> <li>•Heightens the risk of residual data exposure or unauthorized access post-service provider contract</li> </ul>	<ul style="list-style-type: none"> <li>•Raises concerns about the resilience of data recovery mechanisms in data loss scenarios</li> </ul>



**Table 13***Implications of Data Security Gaps in Drug Manufacturing Practices*

<b>Gaps in data security practices by theme</b>	<b>Implications</b>
Challenges in data classification and loss prevention	<ul style="list-style-type: none"> <li>• Unauthorized access to sensitive data.</li> </ul>
Ineffective data risk assessment	<ul style="list-style-type: none"> <li>• Heightened vulnerability to data-related risks</li> <li>• Undermine overall security posture.</li> </ul>
Immature Tech-centric Data Management	<ul style="list-style-type: none"> <li>• Accountability ambiguity</li> <li>• Data mishandling</li> </ul>
Data Ownership Assumptions and Unchecked Data Sharing.	<ul style="list-style-type: none"> <li>• Compromised integrity and confidentiality</li> <li>• Undermined trust.</li> </ul>
Data Governance Challenges and Risks in a Globally Distributed Environment	<ul style="list-style-type: none"> <li>• Increased security incidents risk</li> <li>• Legal and operational challenges.</li> </ul>
Deficiencies in Software Integrity Assessment	<ul style="list-style-type: none"> <li>• Increased susceptibility to tampering</li> </ul>
Inconsistencies in Network Security Measures and Monitoring Practices	<ul style="list-style-type: none"> <li>• Heightened vulnerability to cyber threats</li> <li>• Inadequate detection of security breaches</li> </ul>
USB security risks	<ul style="list-style-type: none"> <li>• Malware infections</li> <li>• Data loss due to theft, corruption, and media loss</li> <li>• Loss of confidentiality</li> </ul>
Challenges in System Validation and Configuration Control	<ul style="list-style-type: none"> <li>• Increased vulnerability to breaches</li> <li>• Operational disruptions.</li> </ul>
Data Resilience Challenges in Modern IT Ecosystems	<ul style="list-style-type: none"> <li>• Business disruptions.</li> </ul>
Data Privacy Vulnerabilities in External Systems	<ul style="list-style-type: none"> <li>• Loss of confidentiality</li> <li>• Regulatory non-compliance.</li> </ul>
Data Integrity Gaps in Operations and Supply Chain Security	<ul style="list-style-type: none"> <li>• Compromised pharmaceutical operations and supply chain</li> </ul>
Inadequate data security monitoring	<ul style="list-style-type: none"> <li>• Undetected data breaches</li> </ul>
Challenges Prioritizing Data Security and Response	<ul style="list-style-type: none"> <li>• Increase vulnerability to breaches</li> <li>• Unresolved security issues.</li> </ul>

Inadequate data risk assessment also erodes trust with stakeholders and tarnishes the organization's reputation, jeopardizing its long-term viability and success. Additionally, the failure to conduct regular risk assessments implies that new and evolving threats might not be identified promptly, leaving a pharmaceutical organization exposed to emerging cyber threats and data breaches. What's more, ineffective data risk assessment hampers an organization's ability to recognize and address emerging threats, putting manufacturing systems and data at risk of exploitation. These gaps, combined with the lack of a standardized approach to assessing data risks, undermine the overall security posture.

**Immature Tech-centric Data Management Process.** Underdeveloped processes often fail to meet the desired management objectives. Various approaches to data management,

some of which neglect important areas, create confusion about responsibility and accountability, while also heightening the chances of data overload. This scenario could lead to mishandling, unauthorized access to sensitive data, and an increased risk of breaches.

**Data Ownership Assumptions and Unchecked Sharing.** Data without ownership lacks protection. When data ownership is not clearly assigned, there is a risk that no one will take responsibility for its security. The absence of defined data ownership can create confusion and inefficiencies within pharmaceutical organizations, as employees may be uncertain about who is responsible for managing and protecting specific data assets. This lack of accountability can lead to improper data handling practices and an increased risk of breaches, while such ambiguity can also impede effective data governance and elevate the risk of data-related incidents. Furthermore, the lack of clarity heightens the risk of unauthorized access and data breaches, undermining confidence and jeopardizing organizational reputation along with its relationships with stakeholders. Additionally, failing to establish clear guidelines and agreements with third parties regarding data access, usage, and protection can result in data being mishandled or accessed by unauthorized individuals, leading to potential breaches. Moreover, uncontrolled sharing practices, particularly with third parties, can create confusion concerning accountability and responsibility. More specifically, unchecked sharing of data with external partners without proper oversight and control can expose sensitive data to unauthorized access, potentially resulting in data breaches.

**Data Governance Challenges and Risks in a Globally Distributed Environment.** Third-party risks arise when contractors, consultants, vendors, and service providers access drug manufacturing data. Also, laws can significantly impact the data held by third parties in various geographical locations for pharmaceutical organization. Without thorough due diligence, pharmaceutical companies might inadvertently engage unreliable third parties, exposing themselves to significant risks such as data breaches, legal penalties, and reputational

damage. Furthermore, failure to implement measures to ensure data accessibility in the event of third-party bankruptcy or closure can lead to data loss, legal complications, business disruptions, and operational challenges. Inadequate handling of data across different geographical locations can also result in privacy and jurisdictional issues stemming from data sovereignty concerns, as well as potential legal repercussions, compliance violations, and possible financial penalties.

**Deficiencies in Software Integrity Assessment.** Unauthorized bypassing of security measures designed to control or limit software installation on a system is a tactic used by attackers to gain unauthorized access or take control of a system. Unauthorized tampering or software modifications carry serious implications, including data breaches, operational disruptions, and compromised product quality. While administrators have the rights to install and modify software and firmware, unauthorized changes or tampering with software, firmware, and data may go undetected. The lack of comprehensive software and firmware integrity checks heightens the risk of undetected tampering or unauthorized modifications. Relying exclusively on substantive tests for software integrity verification is inadequate, as it may not identify all potential vulnerabilities. Moreover, depending solely on substantive tests for software integrity verification could ignore vulnerabilities beyond input and output controls, putting pharmaceutical organizations at risk of undetected software tampering or exploitation.

**Inconsistencies in Network Security Measures and Monitoring Practices.** Unsecured networks are susceptible to data breaches. Differences in network security and monitoring practices reveal a lack of standardized protocols for detecting and protecting against unauthorized access and irregularities, thereby increasing the risk of data breaches. Inconsistent application of network security measures creates loopholes that attackers can exploit to gain access to critical systems and data.

**USB Security Risks.** While USB devices offer a convenient method for transferring data between computers, they also present security risks. Various practices related to USB drive usage create potential vulnerabilities that can lead to malware infections, data theft, data loss, data corruption, and loss of confidentiality. Malware infections can occur when compromised USB drives are connected to networked computers, potentially propagating malicious software throughout a pharmaceutical organization's systems. Data theft may happen if USB drives containing sensitive data are stolen or misplaced, resulting in unauthorized access and potential data breaches. Data corruption and loss of confidentiality can arise if USB drives are damaged, unencrypted, or lost.

**Challenges in System Validation and Configuration Control.** System validation issues that compromise product quality pose potential safety risks to patients. Without standardized validation procedures across various operational environments, pharmaceutical organizations encounter difficulties in ensuring consistent system performance and security. The lack of uniform validation procedures and inconsistent implementations among organizations creates varying levels of system reliability and security risks, which can result in operational disruptions and breaches. Also, inadequate configuration control measures may lead to unauthorized alterations of system settings, heightening the risk of security vulnerabilities.

**Data Resilience Challenges in Modern IT Ecosystems.** The unavailability of crucial data within the pharmaceutical supply chain can threaten the timely delivery of medications, potentially compromising patients' health outcomes. Practices that do not align with the RPO and RTO, unenforced data retention policies, unclear scope and frequency of data recovery tests, and a failure to assume responsibility for data risks in archived facilities pose threats to business continuity and worsen logistical challenges across the industry. Inconsistent practices regarding data recovery objectives (RPO and RTO) and data recovery testing can hinder a

pharmaceutical organization's ability to respond effectively to data loss incidents. Also, neglecting to take ownership of risks related to data in archived facilities can leave pharmaceutical organizations vulnerable to potential data loss and operational disruptions. Unenforced data retention policies may also lead to the loss of vital data, while unclear data recovery testing procedures can result in inadequate preparation for data recovery scenarios.

**Data Privacy Vulnerabilities in External Systems.** Data privacy risks in external systems arise from a lack of comprehensive control and oversight. Partial assessments of third-party system controls may result in a limited understanding of security risks and potential vulnerabilities, increasing the likelihood of unauthorized access or data breaches. Moreover, relying on NDAs and vendor-built security controls may not provide adequate protection against unauthorized access or data breaches, as some pharmaceutical organizations depend on the vendor's security measures rather than implementing their own. Such reliance suggests that these organizations might lack direct oversight of the encryption methods utilized by third-party systems or cloud service providers. Therefore, relying solely on the default encryption provided by vendors may not meet the organization's specific security needs or regulatory requirements, potentially putting sensitive data at risk. Also, inconsistencies in encryption practices, such as neglecting encryption for locally stored data while depending on encryption for cloud-stored data, introduce vulnerabilities that could lead to unauthorized access or breaches.

**Data Integrity Gaps in Operations and Supply Chain Security.** The lack of data integrity in drug manufacturing poses potential errors, inaccuracies, and risks of data manipulation. These issues can compromise the efficacy and safety of medications, leading to serious health risks for patients. Also, inadequate measures to ensure accurate data transfer, verify data integrity, or prevent the mishandling of test data in production systems jeopardize the quality and safety of pharmaceutical products.

**Inadequate Data Security Monitoring.** Inadequate or ineffective monitoring of data protection measures renders systems vulnerable to unauthorized access or breaches. The absence of audit trails in some systems, disabled audit trail functionality, deletion of audit trails, limited log monitoring, and minimal or no review of audit trails create blind spots in tracking data-related activities, potentially allowing data breaches and other security incidents to go unnoticed.

**Challenges in Prioritizing Data Security and Response.** Insufficient data security audits and inaction on audit recommendations suggest that potential weaknesses in security measures remain unaddressed. Such deficiencies create significant gaps in a pharmaceutical organization's security framework, which can be exploited by malicious actors. Unresolved audit recommendations leave pharmaceutical organizations exposed to security breaches and regulatory violations, which could lead to unauthorized access to sensitive data, financial losses from data breaches, and damage to their reputation.

The heightened risks of data breaches in the pharmaceutical industry, a vital component of Nigeria's critical infrastructure, carry serious implications for operational integrity and public trust.

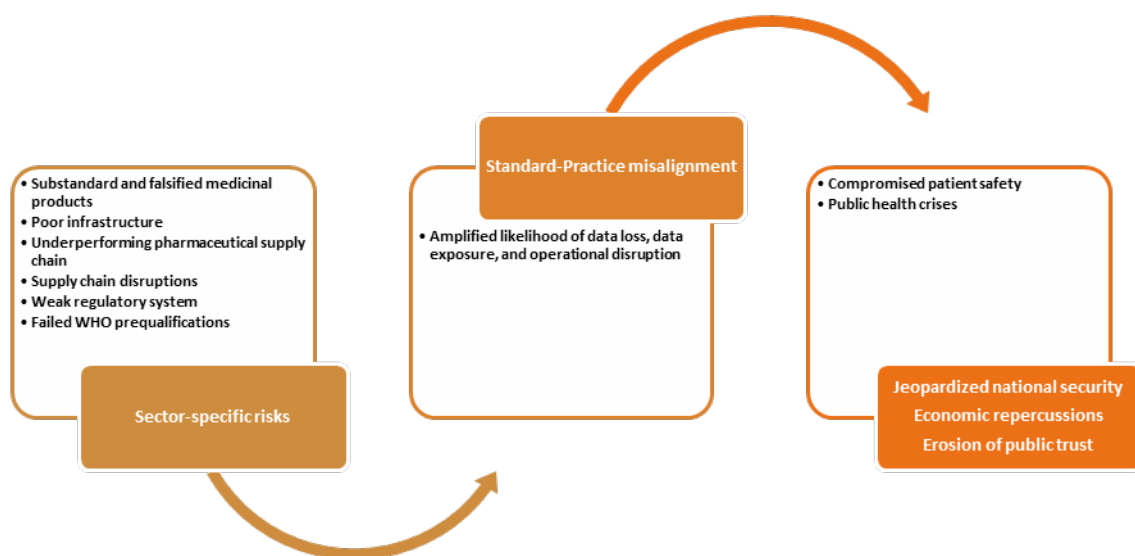
### **5.1.3 Alignment between Guidelines and Practices**

Table 12 illustrated the degree of alignment between data management guidelines and drug manufacturing practices in terms of data security. The conformity of drug manufacturing practices with guidelines varied across different aspects: areas of strong alignment included data access control lists, role-based access control, and data backup; partial alignment was seen in the data management process, data recovery process, and data disposal; minimal alignment was noted in data flow, data retention, data recovery testing, service provider logs, monitoring of service providers, and data encryption at rest, in transit, on removable media, and in end-user devices; significant gaps were identified in data inventory, protection of recovery data,

isolation of the data recovery instance, decommissioning of the service provider, data classification, data loss prevention, and data processing and storage segmentation. The discrepancies and misalignments between management practices and guidelines within the Nigerian pharmaceutical industry worsen sector-specific risks, as depicted in Figure 43, increasing the likelihood of data loss, data exposure, and operational disruptions. This situation could ultimately compromise patient safety and trigger public health crises, leading to jeopardized national security, economic consequences, and reduced public confidence. We assert that discrepancies between guidelines and drug manufacturing practices expand the vulnerabilities of drug manufacturing systems.

**Figure 43**

*Implications of Standards-Practices Misalignment on Data Security*



This study addressed the problem statement, which highlighted alarming reports of data breaches in the regulated pharmaceutical industry. This study addressed the problem statement, which highlighted alarming reports of data breaches in the regulated pharmaceutical industry. The study's purpose is also reflected in the findings, which revealed data security gaps within Nigeria's pharmaceutical sector, their underlying causes, and the broader implications for regulatory compliance, patient safety, medicine security, and national security. Moreover, the

results align with the theoretical framework, suggesting that effective and efficient management controls—together with best practices in data security—are essential for achieving well-managed, adequately secured data and ensuring GMP compliance. Conversely, ineffective or absent management and data security controls increase the risk of data breaches.

## **5.2 Recommendations for Application**

International health organizations, industry consortia, and NRAs such as NAFDAC play a crucial role in improving data security within the pharmaceutical sector. Nigerian drug manufacturing companies must also take an active part in addressing their own data security vulnerabilities. The collaborative efforts of regulators and manufacturers will result in a stronger data security posture across the industry.

### **5.2.1 International Health Organizations, Industry Consortia, NAFDAC**

International health organizations, industry consortia, and regional regulators should incorporate data security best practices into their data management guidelines to better support the pharmaceutical industry. Health authorities should emphasize data inventory, classification, and loss prevention while providing clear guidance on data processing and storage segmentation, isolated and protected data recovery environments, and the secure decommissioning of service providers. Specifically, NAFDAC should establish a data security regulatory framework that aligns with global pharmaceutical standards while being tailored to the unique needs of the Nigerian pharmaceutical industry. Establishing this framework would require publishing data security standards and providing the necessary resources to conduct GMP inspections of pharmaceutical manufacturers in accordance with these standards. Moreover, these statutory inspections would address misalignment between standards and practices, thereby strengthening the critical national infrastructure.



### 5.2.2 Nigerian Drug Manufacturing Organizations

Nigerian drug manufacturing organizations face significant gaps in data management practices that require targeted solutions, as indicated in Table 14, to ensure data security and compliance. Challenges in data classification and loss prevention necessitate effective data classification strategies and the deployment of DLPSs. Frequent and comprehensive risk assessments, guided by NIST SP 800-30 and DPIA templates, are recommended to address ineffective data risk assessments. Immature tech-centric data management can be addressed with a comprehensive data inventory, clear data ownership policies, and secure data disposal practices. To tackle assumptions about data ownership and unchecked data sharing, it is essential to implement clear data ownership policies, role-based access controls, and data access control lists. Data governance challenges in globally distributed environments require due diligence, NDAs, periodic requalification, and the secure decommissioning of service providers. Monitoring service providers, establishing contractual agreements, and conducting compliance audits further strengthen data governance. Software integrity issues can be addressed through regular checks on software and firmware integrity. Inconsistencies in network security measures require active management of network devices, secure configuration processes, network-based URL filters, DNS filtering services, and robust email server protections. Measures such as DMARC implementation, periodic external penetration tests, and network traffic monitoring for unauthorized access or anomalies also play critical roles. USB security risks can be mitigated through encryption, logging unauthorized usage attempts, and implementing data loss prevention solutions, while issues in system validation and configuration control can be addressed with change management procedures, the accreditation and certification of systems, role-based access controls, and the enforcement of data access control lists. Data resilience challenges in modern IT ecosystems requires robust data retention, recovery, and archiving practices, along with application resiliency and

automated backups of data, application configurations, and software files. To address data privacy vulnerabilities in external systems, encrypting data at rest, in use, and in transit is essential. Data integrity gaps in operations and supply chains should be addressed using ALCOA+ principles and regular data integrity checks. Improving inadequate data security monitoring involves logging and monitoring access, modification, and disposal of sensitive data. Lastly, organizations that struggle to prioritize data security and response must invest in well-resourced data security audits and enforce corrective actions by both auditees and management. The solutions were classified into five domains of controls, as shown in Table 14.

We selected four core domains to guide the development of the data security model: Data Protection Controls; Data Availability Controls; Data, Software, and Firmware Integrity Controls; Third-Party Data Security Controls. These domains were selected for their direct alignment with pharmaceutical data priorities: compliance with regulatory frameworks; protection of IP, clinical, manufacturing data; business continuity and data resilience across globally distributed systems; data quality, traceability, and trust in scientific and operational records. The Data Protection Controls safeguard sensitive pharmaceutical data across its entire life cycle. They protect sensitive R&D data, clinical trial records, and proprietary formulations from unauthorized access and regulatory non-compliance. The Data Availability Controls ensure uninterrupted access to critical data and applications throughout system failures, cyberattacks, or disasters. They maintain uninterrupted access to manufacturing data, batch records, and lab systems, which are vital for continuous production and regulatory audits. The Data, Software, and Firmware Integrity Controls preserve the authenticity and reliability of data and digital systems through integrity validation mechanisms. They ensure data integrity in GxP-compliant environments, safeguarding clinical outcomes, product quality, and regulatory credibility. The Third-Party Data Security Controls mitigate data security risks posed by third-party vendors, contract manufacturers, and outsourced IT providers. They

protect the confidentiality and integrity of sensitive data shared with contract research organizations, contract manufacturing organizations, and IT service providers in the global pharmaceutical supply chain.

We excluded Network and Infrastructure Security Controls, as well as the Strategic Layer of Controls, from the proposed model. While essential, the Network and Infrastructure Security Controls focus on broader IT infrastructure defense. They are considered foundational and managed by IT/OT infrastructure teams, but are not unique to risks specific to pharmaceutical data. The Strategic Layer of Controls is critical, but is viewed as an organizational enabler rather than an operational control layer. The model instead emphasizes actionable technical and operational domains directly tied to pharmaceutical data protection.

The proposed model also includes data security protocols comprising topic-specific policies deduced from secure data management. These overarching policies, illustrated in Figure 44, provide a unifying framework under which related data management activities (see Table 5)—some of which span multiple phases—are organized to ensure consistent governance across the Holistic Manufacturing Data Life Cycle, as shown in Table 15. This policy framework that is subsequently mapped to the model's control domains to form the Pharmaceutical Industry Data Security (PhIDS) Model, as shown in Figure 45. We now turn to a discussion of the model's control domains.

**Data, Software, Firmware Integrity Controls.** The PhIDS Model emphasizes the importance of data integrity by incorporating ALCOA+ principles; however, this control domain introduces an additional layer of technical integrity verification. As illustrated in Figure 46, this control domain provide a more comprehensive view of integrity compared to ALCOA+. This perspective encompasses software and firmware integrity, acknowledging that unauthorized modifications or tampering can compromise the integrity of electronic data.

**Table 14***Solutions to Data Security Gaps in Drug Manufacturing Practices*

<b>Data security gaps in drug manufacturing practices</b>	<b>Recommendations</b>	<b>Control Domain</b>
Data ownership assumptions and unchecked data sharing	Data Management Policy; data ownership; role-based access controls; data access control list	<b>Data Protection Controls</b> This domain focuses on protecting sensitive data throughout its life cycle—from creation and classification to access and disposal.
Immature tech-centric data management	Data Management Policy; data inventory; data ownership; secure data disposal	
Challenges in data classification and loss prevention	Data Classification Policy; data classification; data loss prevention solution deployment	
Data privacy vulnerabilities in external systems	Data Encryption Policy; Privacy Policy; encryption of data at rest, in use, and in motion;	
USB security risks	Encrypt data on USB devices; log unauthorized attempts to use them; data loss prevention solution deployment	
Challenges in system validation and configuration control	Changes management procedures; Accreditation and certification of systems; role-based access controls; data access control list	
Inadequate data security monitoring	Logging and monitoring access, modification, and disposal of sensitive data	<b>Data Availability Controls</b> This domain ensures resilience, recovery, and uninterrupted access to data and applications during outages or disasters
Data resilience challenges in modern IT ecosystems	Data Backup and Recovery Policy; Data Archiving, Retention, and Disposal Policy; data retention; data recovery; data recovery test; data archiving; application resiliency; automated data, application configuration, and software file backup	
Data integrity gaps in operations and supply chain	Data Quality Assessment Policy; ALCOA+, data integrity checks;	<b>Data, Software, and Firmware Integrity Controls</b> This domain reinforces data authenticity and system trustworthiness through integrity verification technologies.
Deficiencies in software integrity assessment	Software and firmware integrity checks	
Data governance challenges and risks in a globally distributed environment	Third Party and Vendor Security Policy; due diligence; non-disclosure agreements; initial and periodic requalification; contractual	<b>Third-Party Data Security Controls</b>

<b>Data security gaps in drug manufacturing practices</b>	<b>Recommendations</b>	<b>Control Domain</b>
	agreements; service provider monitoring; compliance audits; secure decommissioning of service providers	This domain mitigates risks introduced through vendors, outsourced IT providers, and contract manufacturers.
Inconsistencies in network security measures and monitoring practices	Implement and actively manage network devices; establish and maintain a secure configuration process for network infrastructure; maintain and enforce network-based URL filters; utilize DNS filtering services; block unnecessary file types; implement DMARC; deploy and maintain email server anti-malware protections; validate security measures; periodic external penetration tests and remediating test findings; monitor network traffic for unauthorized access or anomalies	<b>Network and Infrastructure Security Controls</b> This domain encompasses the essential safeguards for securing network and IT infrastructure components.
Challenges prioritizing data security and response	Well-resourced data security audits; corrective actions by auditees and management	<b>Strategic Layer of Control</b> This domain is focused on structured risk assessments, audits, corrective actions, and active prioritization by management.
Ineffective data risk assessment	Frequent and comprehensive risk assessment by DPO following NIST SP 800-30 and DPIA templates	

**Table 15***Policy Mapping Aligned PhIDS and Manufacturing Data Life Cycle*

<b>Stage</b>	<b>Security data management activities</b>	<b>Data governance consequences</b>	<b>Relevant Policy</b>	<b>Rationale for Policy Inclusion</b>
<b>Creation</b>	<ul style="list-style-type: none"> <li>Classify data according to its importance and sensitivity.</li> <li>Conduct quality checks and validation to verify data accuracy and integrity.</li> <li>Ensure adherence to consent, ethical, and legal requirements.</li> </ul>	<ul style="list-style-type: none"> <li>Implement accurate data classification.</li> <li>Ensure compliance with data standards.</li> <li>Maintain conformity with data protection regulations.</li> </ul>	Data classification policy; Data quality assessment policy; Privacy policy	Ensures data is properly categorized, validated, and collected in compliance with ethical and legal standards.

Stage	Security data management activities	Data governance consequences	Relevant Policy	Rationale for Policy Inclusion
<b>Collection</b>	<ul style="list-style-type: none"> <li>Establish secure data collection protocols to ensure that data is obtained solely from authorized sources.</li> <li>Encrypt data collected via smart terminals and IoT sensors to protect it from unauthorized access.</li> <li>Validate and monitor data sources to prevent malicious or inaccurate data entry</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced data integrity by preventing unauthorized data collection.</li> <li>Secure, real-time data collection</li> <li>Ensure trustworthiness of data sources through source validation</li> </ul>	Data encryption policy; Privacy policy; Third-party and vendor security policy	Supports secure acquisition, encryption at source, and validates sources (especially if third-party vendors are involved).
<b>Processing</b>	<ul style="list-style-type: none"> <li>Encrypt data both before and after processing to ensure confidentiality.</li> <li>Establish access controls to restrict who can process or modify data.</li> <li>Use secure preprocessing methods to remove inconsistent or redundant data and ensure only authorized personnel can access processing functions.</li> </ul>	<ul style="list-style-type: none"> <li>Ensure secure data processing.</li> <li>Maintain access restrictions to safeguard sensitive data.</li> <li>Promote data accuracy and security during preprocessing.</li> </ul>	Access control policy; Data encryption policy; Data cleansing policy	Limits access, ensures encryption, and removes redundant/inaccurate data during preprocessing.
<b>Storage</b>	<ul style="list-style-type: none"> <li>Implement encryption, access control, and user authentication measures.</li> <li>Establish retention policies aligned with business needs and regulatory requirements.</li> <li>Employ backup and recovery strategies to ensure data availability</li> </ul>	<ul style="list-style-type: none"> <li>Safeguard data by preventing unauthorized access and breaches.</li> <li>Comply with policies and regulations.</li> <li>Implement measures to prevent system failures and data loss.</li> </ul>	Data backup and recovery policy; Access control policy; Data encryption policy	Protects stored data from loss, breaches, and unauthorized access; ensures data availability.
<b>Usage</b>	<ul style="list-style-type: none"> <li>Define access policies according to roles and responsibilities.</li> <li>Establish for data processing to maintain consistency and reliability.</li> <li>Monitor and audit data usage to ensure adherence to policies and regulations.</li> </ul>	<ul style="list-style-type: none"> <li>Maintain adequate access and controls.</li> <li>Ensure accurate and secure data processing.</li> <li>Promote accountability and transparency in data utilization.</li> </ul>	Access control policy; Data management policy; Data quality assessment policy	Governs proper role-based use, ensures policies guide operations, and maintains data accuracy during usage.
<b>Visualization</b>	<ul style="list-style-type: none"> <li>Apply access controls to prevent unauthorized access to sensitive visual data.</li> </ul>	<ul style="list-style-type: none"> <li>Reduced risk of data leaks by securing access to sensitive visual data.</li> </ul>	Access control policy	Ensures sensitive visual data is protected from unauthorized viewers.

Stage	Security data management activities	Data governance consequences	Relevant Policy	Rationale for Policy Inclusion
<b>Archiving</b>	<ul style="list-style-type: none"> <li>• Encrypt archived data.</li> <li>• Store archived data in accordance with legal and regulatory requirements.</li> </ul>	<ul style="list-style-type: none"> <li>• Archived data remains secure.</li> <li>• Compliance with retention schedules to mitigate legal risks.</li> </ul>	Data archiving, retention, and disposal policy; Data encryption policy	Secures long-term storage and complies with legal retention requirements.
<b>Transmission</b>	<ul style="list-style-type: none"> <li>• Encrypt data during transmission to ensure confidentiality.</li> <li>• Establish standards for secure communication protocols and network configurations.</li> <li>• Conduct integrity checks to verify that data remains unchanged during transmission.</li> </ul>	<ul style="list-style-type: none"> <li>• Secure data during transmission to prevent unauthorized access.</li> <li>• Safeguard data while it is in transit.</li> <li>• Implement data integrity to minimize the risk of tampering.</li> </ul>	Data encryption policy; Third-party and vendor security policy	Protects data in transit with encryption and secure communication protocols, especially when shared with vendors.
<b>Sharing</b>	<ul style="list-style-type: none"> <li>• Establish agreements for sharing data with external parties.</li> <li>• Use anonymization or masking to safeguard sensitive data.</li> <li>• Continuously monitor and review data access and sharing practices.</li> </ul>	<ul style="list-style-type: none"> <li>• Establish and enforce regulations, roles, and obligations for sharing data.</li> <li>• Ensure the protection of data privacy when sharing with external parties.</li> <li>• Adhere to regulations and security measures when sharing data.</li> </ul>	Third-party and vendor security policy; Privacy policy; Data management policy	Formalizes external sharing practices, ensures anonymity where needed, and reinforces oversight responsibilities
<b>Applications</b>	<ul style="list-style-type: none"> <li>• Control access to data-driven applications.</li> </ul>	<ul style="list-style-type: none"> <li>• Enhanced application security by preventing unauthorized access.</li> </ul>	Access control policy; Data management policy	Ensures only authorized users access sensitive data through apps.
<b>Destruction</b>	<ul style="list-style-type: none"> <li>• Develop protocols for securely deleting data to ensure complete removal.</li> <li>• Establish guidelines for data retention and secure archiving prior to deletion.</li> <li>• Maintain audit trails to verify compliance and uphold data privacy</li> </ul>	<ul style="list-style-type: none"> <li>• Ensure appropriate disposal of data to prevent leaks or breaches.</li> <li>• Adhere to regulations governing data retention.</li> <li>• Maintain accessible audit trails for inspection.</li> </ul>	Data archiving, retention, and disposal policy; Privacy policy; Data management policy	Ensures secure deletion, retention compliance, and verification of proper disposal through documentation and auditing.

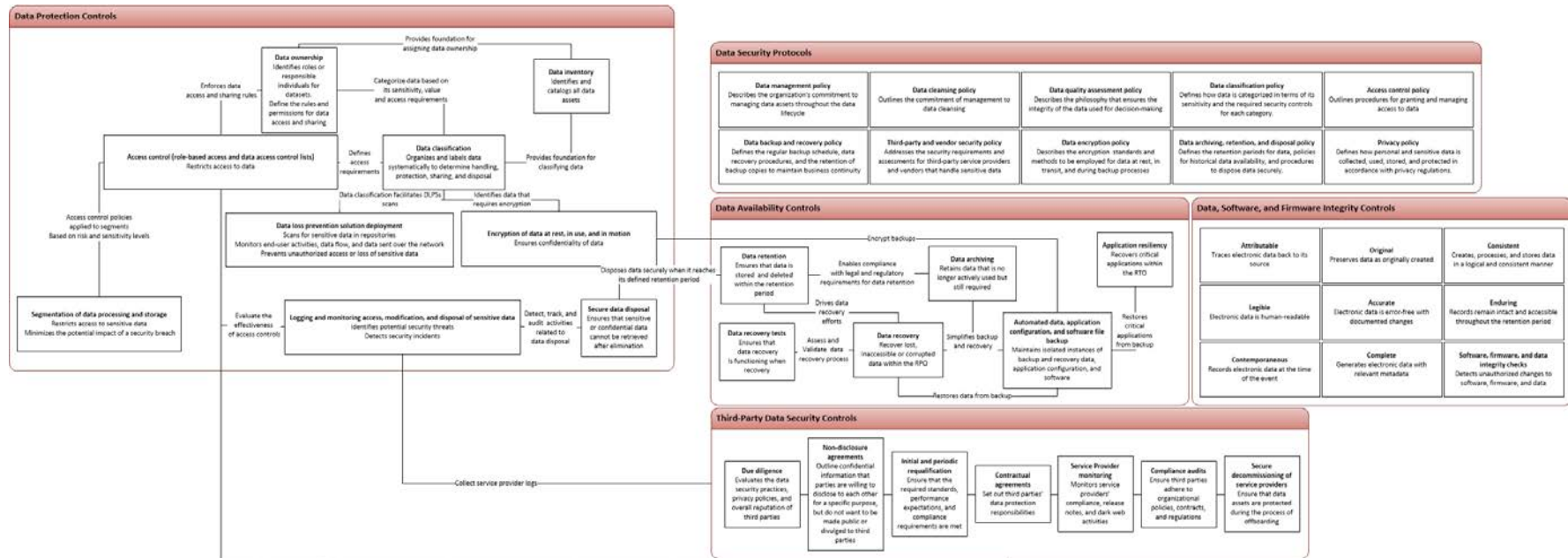
**Figure 44***Topic-specific Policies for Secure Data Management*

Data Security Protocols		
<b>Data management policy</b> Describes the organization's commitment to managing data assets throughout the data lifecycle	<b>Data cleansing policy</b> Outlines the commitment of management to data cleansing	<b>Third-party and vendor security policy</b> Addresses the security requirements and assessments for third-party service providers and vendors that handle sensitive data
<b>Data backup and recovery policy</b> Defines the regular backup schedule, data recovery procedures, and the retention of backup copies to maintain business continuity	<b>Access control policy</b> Outlines procedures for granting and managing access to data	<b>Data quality assessment policy</b> Describes the philosophy that ensures the integrity of the data used for decision-making
<b>Data encryption policy</b> Describes the encryption standards and methods to be employed for data at rest, in transit, and during backup processes	<b>Data archiving, retention, and disposal policy</b> Defines the retention periods for data, policies for historical data availability, and procedures to dispose data securely.	<b>Privacy policy</b> Defines how personal and sensitive data is collected, used, stored, and protected in accordance with privacy regulations.
<b>Data classification policy</b> Defines how data is categorized in terms of its sensitivity and the required security controls for each category.		



Figure 45

## The PhIDS Model



Consequently, the PhIDS model recommends using integrity verification tools to identify unauthorized changes to firmware and software. This understanding indicates that data quality assessments should encompass software and firmware integrity checks. As presented in Table 14, this domain reinforces data authenticity and system trustworthiness through integrity verification technologies.

**Figure 46**

*Data, Software, and Integrity Controls of the PhIDS Model*

Data, Software, and Firmware Integrity Controls		
<b>Attributable</b> Traces electronic data back to its source	<b>Original</b> Preserves data as originally created	<b>Consistent</b> Creates, processes, and stores data in a logical and consistent manner
<b>Legible</b> Electronic data is human-readable	<b>Accurate</b> Electronic data is error-free with documented changes	<b>Enduring</b> Records remain intact and accessible throughout the retention period
<b>Contemporaneous</b> Records electronic data at the time of the event	<b>Complete</b> Generates electronic data with relevant metadata	<b>Software, firmware, and data integrity checks</b> Detects unauthorized changes to software, firmware, and data

At a higher level, a data quality assessment policy (ISACA, 2018a), as illustrated in Figure 44, defines the organization's overarching approach to ensuring data quality, with the goal of maintaining the integrity of data used in decision-making processes that affect the organization. The policy also identifies the methods, solutions, and tools available to ensure data integrity. Integrity verification tools play a crucial role in enhancing data quality assessment within the technological infrastructure. Tools like parity checks, cryptographic hashes, and cyclical redundancy checks support data quality assessments by examining changes or tampering with software components (e.g., applications, middleware, and key internal elements such as kernels and drivers within operating systems) and firmware like Basic Input Output System (BIOS) (Cybersecurity Audit Program, n.d.). These tools act as vigilant

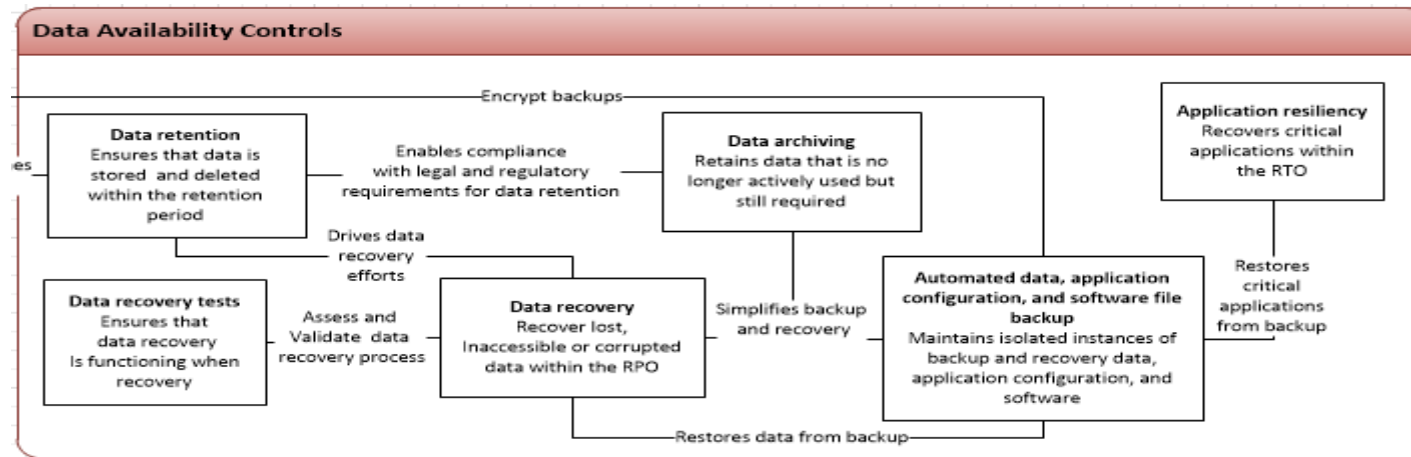
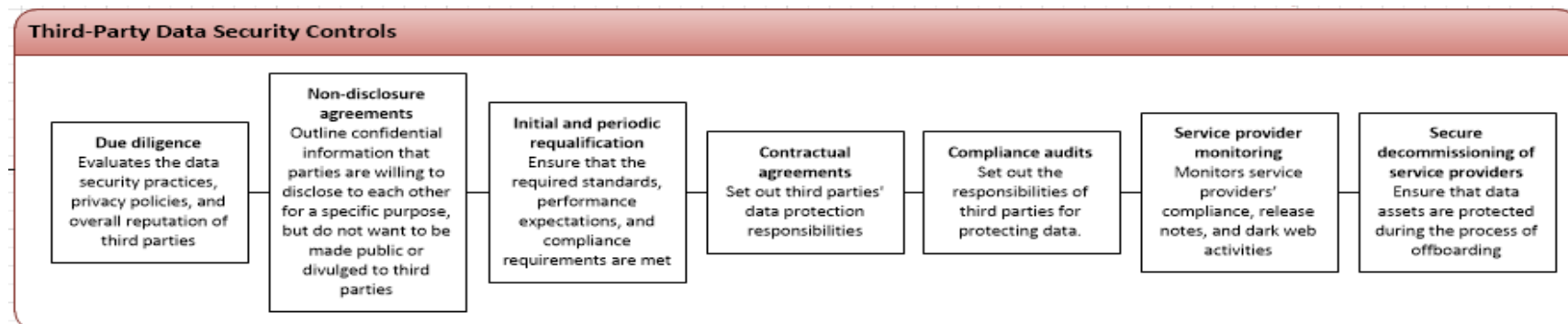
guardians against unauthorized tampering and alterations across various layers of hardware, software, and systems. Moreover, their importance transcends software or hardware scrutiny, extending to the detection of unauthorized access to critical information and metadata. Integrity verification tools also evaluate security attributes associated with sensitive data and other vital metadata (Cybersecurity Audit Program, n. d.). By closely monitoring these layers, integrity verification tools serve as sentinels, identifying any irregularities or unauthorized modifications that could jeopardize the integrity and authenticity of the system and the data it hosts. This comprehensive coverage of various layers and components within technological systems ensures a holistic approach to data protection, facilitating the prompt detection of unauthorized alterations. Through their continuous vigilance and verification mechanisms across multiple layers, integrity verification tools provide assurance regarding the integrity of stored data. Implementing such robust measures enables drug manufacturing organizations to bolster their defenses against unauthorized data modifications, thus enhancing their overall security posture and bolstering trust in the data ecosystem.

**Data Availability Controls.** This control domain, illustrated in Figure 47, isolate and expand upon the availability attributes of ALCOA+, integrating concepts such as data backups, retention, archiving, recovery, and recovery tests. It ensures resilience, recovery, and uninterrupted access to data and applications during outages or disasters. To ensure uninterrupted access to application data in the event of a disaster, we included the backup of application configuration and software files as part of our data availability controls. These backups are vital to application resiliency, ensuring that critical application elements are restored within the RTO, thereby minimizing downtime and maintaining access to application data. Consequently, a data backup and recovery policy, as depicted in Figure 44, should govern the regular backup schedule, recovery procedures, and retention of backup copies of data, along with application configuration, software files, and related data to reinforce data resilience.

Additionally, an isolated instance of recovery data, along with the application configuration and software files, should be created, maintained, and safeguarded with equivalent controls to the original data for successful recovery. Furthermore, a data archiving, retention, and disposal policy, also shown in Figure 44, ensures compliance with legal and regulatory requirements for retaining, archiving, and disposing of historical data. This policy governs the duration of data retention, the procedures for archiving data, and the protocols for securely disposing of data when it is no longer necessary.

**Third-Party Data Security Controls.** This control domain address the data risks associated with vendors, outsourced IT providers, and contract manufacturers. This domain, as illustrated in Figure 48, incorporates policies and activities designed to minimize risks related to third-party access to drug manufacturers' data assets. The third-party and vendor security policy governs the security requirements and assessments for third-party service providers and vendors handling sensitive data from drug manufacturers. This policy, depicted in Figure 44, fosters sustainable relationships where risks are managed and directs activities involving third parties and vendors, including due diligence, initial and periodic requalification assessments, compliance audits, service provider monitoring, and secure decommissioning of service providers.

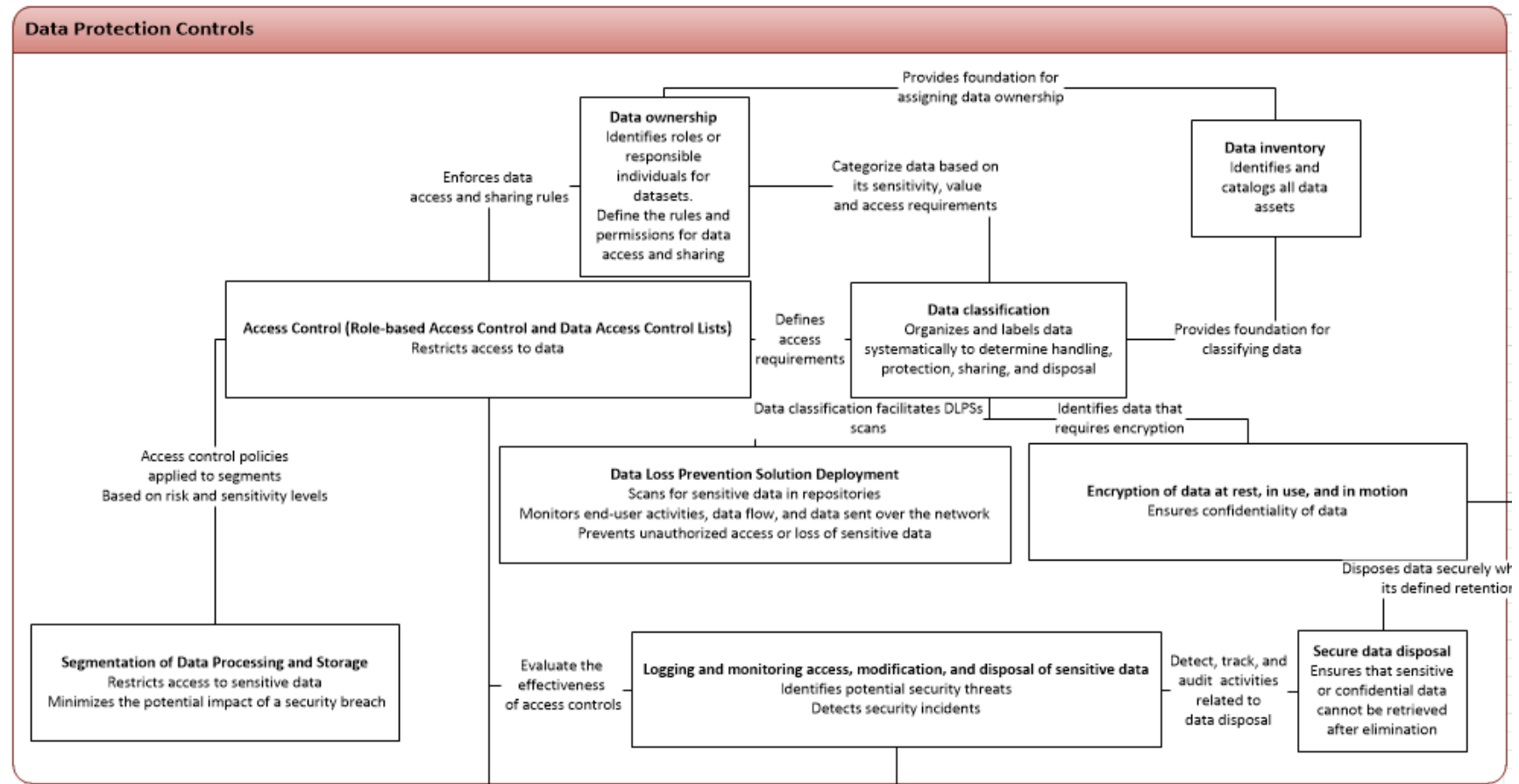
Due diligence is the first step in evaluating and selecting a third-party provider. It entails researching and assessing a potential provider's capabilities, compliance with security standards, and overall reputation (ISACA, 2014; Daley et al., 2023). This comprehensive examination allows drug manufacturers to mitigate risks, ensure alignment with their operational needs, and create a reliable partnership. To protect sensitive data during discussions and negotiations, NDAs are established (ISACA, 2019) after due diligence and prior to further engagement. NDAs establish confidential relationships between drug manufacturers and third parties, detailing the information that must remain confidential and secured.

**Figure 47***Data Availability Controls of the PhIDS Model***Figure 48***Third-Party Data Controls of the PhIDS Model*

The initial and periodic requalification process involves evaluating the qualifications, capabilities, and security measures of third-party providers. Initial requalification occurs before engagement, while periodic requalification ensures ongoing compliance and security. After completing due diligence and requalification, the drafting and signing of contractual agreements takes place. These agreements define the responsibilities, security requirements, and terms of the relationship. Conducting compliance audits ensures that third-party providers meet contractual security and regulatory requirements, with these audits occurring periodically or as necessary. Furthermore, monitoring the activities and security practices of third-party providers and vendors should be carried out throughout the relationship. Service provider monitoring ensures consistent maintenance of security measures and prompt resolution of any issues. In addition to periodic reassessment, monitoring activities should include reviewing service provider release notes and checking the dark web (CIS Critical Security Controls Version 8, n.d.). When the engagement with a third-party provider ends, safe and proper handling of data and assets is facilitated through secure decommissioning procedures. The chronological order of third-party data security controls presented by the PhIDS Model illustrates the typical sequence of activities in managing third-party relationships while emphasizing data security and compliance considerations in drug manufacturing. Such a structured approach is essential for drug manufacturing organizations to effectively oversee and mitigate vulnerabilities arising from vendor partnerships.

**Data Protection Controls.** Data protection is a fundamental aspect of the PhIDS Model, and this control domain, illustrated in Figure 49, encompasses both management practices and technical solutions to safeguard data. This domain focuses on protecting sensitive data throughout its life cycle—from creation to destruction. Central to this domain is data inventory, which offers a comprehensive overview of enterprise data assets (CIS Critical

Security Controls Version 8, n. d.), serves as the basis for assigning ownership and classifying data (ISACA, 2019), and facilitates the creation and maintenance of a data management policy. A data management policy, depicted in Figure 44, is developed from the insights derived from the data inventory. This policy articulates the organization's commitment to managing data assets throughout their life cycle (ISACA, 2018a). It is put into operation through the data management process, which encompasses data ownership, handling, sensitivity, retention limits, and disposal requirements based on sensitivity and retention standards for the enterprise. Data ownership identifies who is responsible for datasets, and data owners classify data according to its sensitivity, value, and access requirements (ISACA, 2019). The categorization defined by a data classification policy, also shown in Figure 44, helps to establish access requirements, identify data needing encryption, and enable the implementation of DLPSs. Beyond the main functions of DLPSs—scanning for sensitive data in repositories, monitoring end-user activities, tracking data flow, and overseeing data transmitted over the network, as well as preventing unauthorized access or loss of sensitive data—DLPSs that manage data in storage enforce data encryption policies by encrypting entire file systems (Alneyadi et al., 2016). The data encryption policy, depicted in Figure 44, establishes the standards and methods for encrypting data at rest, in use, in transit, and during the backup process. Data encryption methods enforce privacy policies by keeping data confidential throughout its life cycle. Furthermore, data ownership defines the rules and permissions for accessing and sharing data. Access controls, such as role-based access controls and data access control lists, restrict access and sharing permissions to authorized individuals by enforcing data access requirements and sharing rules for both users and third parties. The access control policy, depicted in Figure 44, outlines the procedures for granting and managing data access.

**Figure 49***Data Protection Controls of the PhIDS Model*



Moreover, segmenting data processing and storage facilitates the application of access control policies to segments based on risk and sensitivity levels, thereby restricting access to sensitive data and minimizing the potential impact of security breaches. Logging and monitoring mechanisms further assess the effectiveness of access controls, as well as track data-related activities. Collecting service provider logs, along with logging and monitoring access, modification, and disposal of sensitive data, helps to identify potential security threats, detect security incidents, and track, audit, and monitor data disposal activities. Also, data processing and storage segmentation reduces the potential impact of security breaches.

### **5.2.3 Standards-Based Validation and Scalability of the PhIDS Model**

The PhIDS Model policies and data security controls demonstrate strong alignment with the ISO/IEC 27002:2022 standard (ISO, 2022b), which provides guidelines for information security, cybersecurity, and privacy protection. Also, the CIS Controls IGs offer a scalable framework, tailoring cybersecurity safeguards to organizations with differing risk profiles and resources (CIS Critical Security Controls Version 8, n. d.). We assigned IGs to PhIDS controls lacking IGs to ensure comprehensive scalability. The detailed validation and scalability analysis of the PhIDS Model, outlined below and illustrated in Table 16, guarantees that organizations of all sizes, from small businesses to large enterprises, can effectively secure their data environments. The data management policy in the model aligns with ISO/IEC 27002 Section 5.9, which emphasizes the importance of maintaining an accurate inventory of information assets and ownership (ISO, 2022b). This policy requires drug manufacturing organizations to systematically record and monitor data assets, providing them with a clear view of their data environment to support effective management and enhance security. This control apply across all implementation groups (IG1, IG2, and IG3) (CIS Critical Security Controls Version 8, n. d.) as they form the foundation for effective data security.

The data classification policy of the model aligns with Sections 5.12 and 5.13 of ISO/IEC 27002. These sections emphasize the classification and labeling of information (ISO, 2022b). This policy requires organizations to provide a comprehensive data classification scheme that allows them to identify, classify, and label information based on sensitivity and significance. It ensure that data is properly protected throughout its life cycle. This control is essential for drug manufacturing organizations in IG2 and IG3 (CIS Critical Security Controls Version 8, n.d.), which manage moderately sensitive to highly sensitive data.

The access control policy of the model aligns with Sections 5.15 and 8.3 of ISO/IEC 27002 (ISO, 2022b), which emphasize restricting access to information based on roles and responsibilities. This policy requires drug manufacturing organizations to implement RBAC, data access control lists, and data segmentation to minimize unauthorized access and impact of data breaches. Data access control lists apply to all IG levels, while data segmentation is critical for drug manufacturing organizations in IG2 and IG3 (CIS Critical Security Controls Version 8, n. d.). RBAC is particularly relevant for drug manufacturing organizations in IG3 (CIS Critical Security Controls Version 8, n. d.).

In managing third-party relationships, the third-party and vendor security policy of the model aligns with Sections 5.19, 5.20, and 5.22 of ISO/IEC 27002. These sections highlight the significance of due diligence, contractual agreements, and ongoing monitoring of supplier services (ISO, 2022b). This policy ensures that vendor relationships are governed by clear security expectations, making this policy especially critical for IG2 and IG3 drug manufacturing organizations, which often collaborate with external service providers (CIS Critical Security Controls Version 8, n. d.).

The data archiving, retention, and disposal policy of the model aligns with Sections 7.10, 7.14, and 8.10 of ISO/IEC 27002 (ISO, 2022b), which address the secure retention and disposal of data. This policy specifies strict controls to retain data only as long as necessary

and mandates secure disposal to prevent unauthorized recovery. These control apply across all IG levels (CIS Critical Security Controls Version 8, n.d.), ensuring compliance with data protection regulations while minimizing risks associated with obsolete data.

PhIDS Model addresses data resilience through its data backup and recovery policy, which aligns with Section 8.13 of ISO/IEC 27002. This section emphasizes the importance of regular backups, testing, and recovery of essential information, systems, and software to meet security requirements (ISO, 2022b). Automated backups, recovery, and application resiliency practices ensure that critical data remains accessible and intact during disruptions. This control is fundamental for all drug manufacturing organizations (IG1, IG2, and IG3), with recovery tests being particularly crucial for IG3 organizations (CIS Critical Security Controls Version 8, n. d.).

The data encryption policy of the PhIDS Model is validated by Section 8.24 of ISO/IEC 27002, which specifies the use of cryptography to protect data confidentiality (ISO, 2022b). This policy ensures the encryption of data at rest, in use, and in motion, offering robust protection against data breaches. This control is particularly relevant for IG2 and IG3 drug manufacturing organizations (CIS Critical Security Controls Version 8, n. d.), which handle sensitive or regulated data that requires advanced encryption.

The PhIDS Model incorporates software, firmware, and data integrity checks, aligning with ISO/IEC 27002 Sections 8.7, 8.19, and 8.26 (ISO, 2022b). These controls protect against malware infections, system integrity breaches, and unauthorized software exploitation that could compromise data. The data quality assessment policy of the model, acting as an overarching policy for these integrity checks, ensures data integrity by preventing unauthorized modifications from various sources. These controls are applicable to all drug manufacturing organizations (IG1, IG2, and IG3).

The PhIDS Model ensures privacy through its privacy policy, which aligns with ISO/IEC 27002 Section 5.34 (ISO, 2022b). This policy ensures compliance with regulations regarding privacy and the protection of PII. This control is pertinent to all drug manufacturing organizations (IG1, IG2, and IG3) for privacy compliance.

The PhIDS Model incorporates DLPSs to monitor, detect, and prevent unauthorized data transfers. Aligned with ISO/IEC 27002 Section 8.12 (ISO, 2022b), this control ensures that sensitive data stays within designated security perimeters, mitigating the risks of exfiltration. The deployment of DLPS primarily applies to IG3 drug manufacturing organizations that handle highly sensitive or regulated data, ensuring real-time protection and compliance with regulatory requirements.

Lastly, the PhIDS Model includes technological controls for capturing data access and monitoring unauthorized modifications. Logging and monitoring aligns with Sections 8.15 and 8.16 (ISO, 2022b), which emphasize the importance of recording data access and monitoring system activities to identify and respond to potential data security incidents. These controls enable organizations to effectively detect and respond to incidents, making them essential for IG2 and IG3 drug manufacturing organizations facing sophisticated threats (CIS Critical Security Controls Version 8, n. d.).

In summary, the PhIDS Model closely aligns with ISO/IEC 27002:2022, offering a comprehensive framework for securing pharmaceutical data. The distribution of controls across IGs ensures scalability and relevance for pharmaceutical organizations with different maturity levels and resources, while also facilitating a phased approach to implementing safeguards.

#### **5.2.4 Model Validation through Pilot Implementation and Refinement**

To ensure that the proposed PhIDS model is both practically applicable and contextually relevant, a structured validation approach is essential. The following multi-stage strategy was proposed:

**Table 16***PhIDS Model Validation and Scalability*

Topic-Specific Policies	PhIDS Controls	Implementation Groups	Reference Standard	Control classification	Control type
Data management policy	• Data inventory, Data ownership	• IG1, IG2, IG3	ISO/IEC 27002 5.9 Inventory of information and other associated assets	Organizational	Preventive
Data classification policy	• Data classification scheme	• IG2, IG3	ISO/IEC 27002 5.12 Classification of information	Organizational	Preventive
			ISO/IEC 27002 5.13 Labeling of information	Organizational	Preventive
Access control policy	• Role-based access control • Data access control lists • Segmentation of data processing and storage	• IG3 • IG1, IG2, IG3 • IG2, IG3	ISO/IEC 27002 5.15 Access control	Organizational	Preventive
			ISO/IEC 27002 8.3 Information access restriction	Technological	Preventive
Third-party and vendor security policy	• Due diligence • Secure decommissioning of service providers • Contractual agreements, Non-disclosure agreements	• IG3 • IG3 • IG2, IG3	ISO/IEC 27002 5.19 Information security in supplier relationships	Organizational	Preventive
			ISO/IEC 27002 5.20 Addressing information security within supplier agreements	Organizational	Preventive
			ISO/IEC 27002 6.6 Confidentiality or non-disclosure agreements	People	Preventive
	• Initial and periodic requalification • Service provider monitoring • Compliance audits	• IG3	ISO/IEC 27002 5.22 Monitoring, review, and change management of supplier services	Organizational	Preventive
Data archiving, retention, and disposal policy	• Data retention (including retention of data archives) • Secure data disposal	• IG1, IG2, IG3 • IG1, IG2, IG3	ISO/IEC 27002 7.10 Storage media	Physical	Preventive
			ISO/IEC 27002 7.14 Secure disposal or re-use of equipment	Physical	Preventive
			ISO/IEC 27002 8.10 Information deletion	Technological	Preventive
Data backup and recovery policy	• Data recovery (a critical foundation of application resiliency) • Data recovery tests • Automated data, application configuration, and software file backup	• IG1, IG2, IG3 • IG2, IG3 • IG1, IG2, IG3	ISO/IEC 27002 8.13 Information backup	Technological	Corrective
Data encryption policy	• Encryption of data at rest, in use, and in motion	• IG2, IG3	ISO/IEC 27002 8.24 Use of cryptography	Technological	Preventive
Data quality assessment policy	• Software, firmware, and data integrity checks	• IG1, IG2, IG3	ISO/IEC 27002 8.7 Protection against malware	Physical	Preventive/ Detective/ Corrective
			ISO/IEC 27002 8.19 Installation of software on operational systems	Technological	Prevention
			ISO/IEC 27002 8.26 Application security requirements	Technological	Preventive
Privacy policy	• Privacy and protection of PII in compliance with regulations	• IG1, IG2, IG3	ISO/IEC 27002 5.34 Privacy and protection of PII	Organizational	Preventive
	• Data loss prevention solution deployment	• IG3	ISO/IEC 27002 8.12 Data leakage prevention	Technological	Preventive/ Detective
	• Logging access, modification, and disposal of sensitive data	• IG1, IG2, IG3	ISO/IEC 27002 8.15 Logging	Technological	Detective
	• Monitoring of access, modification, and disposal of sensitive data	• IG2, IG3	ISO/IEC 27002 8.16 Monitoring activities		Detective/ Corrective

**Pilot Implementation in a Select Pharmaceutical Organization.** The primary method of validating the PhIDS model will involve deploying it on a pilot basis within a selected pharmaceutical company in Nigeria. This implementation would focus on integrating the model's core components—data protection controls, data availability controls, third-party data security controls, integrity (data, firmware, and software) controls, and policy framework—into the organization's existing data management processes. The objective is to assess how well the model enhances organizational data security posture and supports compliance with regulatory expectations (e.g., NDPR, NAFDAC).

**Simulation of Use-Case Scenarios.** Complementing the pilot, scenario-based simulations will be used to test the model's overall ability to protect sensitive pharmaceutical data and detect security risks under realistic conditions. These simulations will involve scenarios such as attempts to access patient data without authorization, unauthorized efforts to retrieve proprietary formulations, or improper disposal of digital records. The purpose is to evaluate how effectively the model's controls prevent such incidents and detect any attempts that could compromise data security.

**Iterative Refinement and External Consultation.** Insights gathered from the pilot and simulations will guide iterative modifications to the model. To further strengthen validity, feedback will also be solicited from external experts in pharmaceutical compliance, information security, and regulatory policy. This may include academic researchers, regulators, or professional bodies. These contributions will help ensure the model's wider applicability across the Nigerian pharmaceutical sector.

### **5.2.5 PhIDS Model Implementation Strategy**

The implementation of the PhiDS model follows a structured, phased approach to enhance data security in drug manufacturing practices. The model is divided into three implementation phases, illustrated in Table 17, each integrating progressively advanced

safeguards to thoroughly address data security challenges. Systematic execution of these three phases enables the PhiDS model to establish a robust framework for securing data in drug manufacturing, mitigating evolving threats, and ensuring regulatory compliance.

**Table 17**

*Implementation Phases of the PhiDS Model*

<b>Implementation phases</b>	<b>PhiDS controls</b>
Implement IG1 safeguards	Data management policy
	Data inventory
	Data ownership
	Privacy policy
	Access control policy
	Data access control lists
	Data quality assessment policy
	Software, firmware, and data integrity checks
	Data archiving, retention, and disposal policy
	Data retention (including retention of data archives)
	Secure data disposal
	Data backup and recovery policy
	Data recovery (a critical foundation of application resiliency)
	Automated data, application configuration, and software file backup
	Logging access, modification, and disposal of sensitive data
Implement IG2 safeguards (includes IG1)	Data classification policy
	Data classification scheme
	Segmentation of data processing and storage
	Access control policy (updated)
	Third-party and vendor security policy
	Contractual agreements
	Non-disclosure agreements
	Data recovery tests
	Data backup and recovery policy (updated)
	Data encryption policy
Implement IG3 safeguards (includes IG1 and IG2)	Encryption of data at rest, in use, and in motion
	Monitoring of access, modification, and disposal of sensitive data
	Role-based access control
	Access control policy (updated)
	Due diligence
	Secure decommissioning of service providers
	Initial and periodic requalification
	Service provider monitoring
	Compliance audits
	Third-party and vendor security policy (updated)
	Data loss prevention solution deployment

The first phase, Implement IG1 Safeguards, establishes foundational security controls that focus on data governance and integrity. This includes implementing a data management policy, maintaining a comprehensive data inventory, and defining clear data ownership. It also involves a privacy policy and an access control policy supported by data access control lists. A

data quality assessment policy, along with software, firmware, and data integrity checks, ensures that information remains reliable and trustworthy. Also, a data archiving, retention, and disposal policy cover retention requirements, including retention of data archives, and mandate secure data disposal. What's more, a data backup and recovery policy provides a critical foundation for application resiliency, incorporating automated backups of data, application configurations, and software files to support data recovery. In addition, logging mechanisms are implemented to record access, modifications, and disposal of sensitive data.

The second phase, Implement IG2 Safeguards, builds on IG1 by introducing advanced security measures, including data classification policies and schemes, segmentation of data processing and storage, and updated access control policies. It also incorporates security policies for third parties and vendors through contractual agreements and NDAs to bolster external data security. Data recovery processes are enhanced with revised backup and recovery policies and the inclusion of regular data recovery tests to ensure resilience. Encryption policies are applied to protect data at rest, in use, and in motion. Additionally, continuous monitoring of access, modifications, and disposal of sensitive data is implemented to improve security oversight.

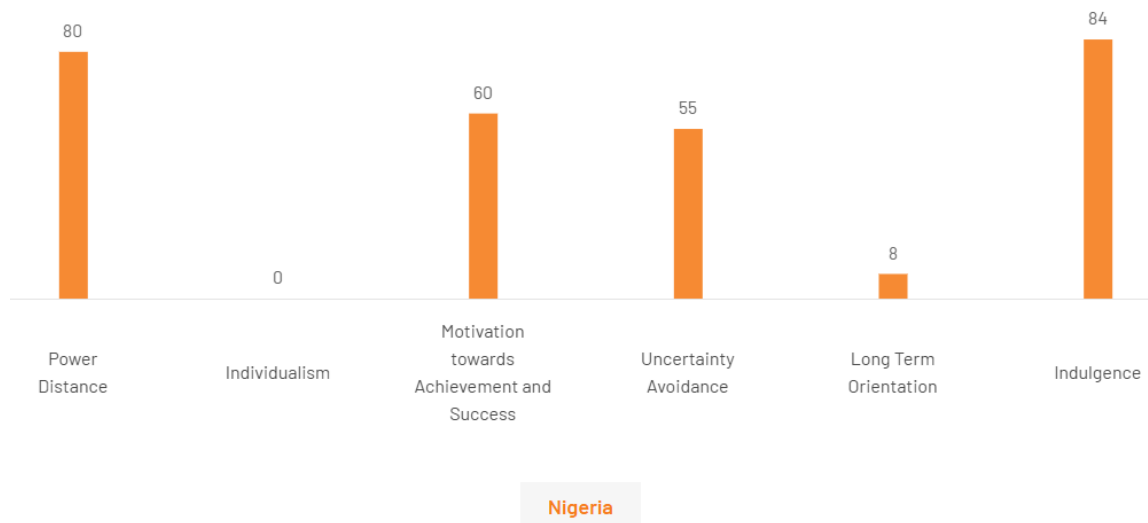
The third and final phase, Implement IG3 Safeguards, expands IG1 and IG2 protections by emphasizing role-based access control supported by an updated access control policy. It introduces due diligence measures, secure decommissioning of service providers, initial and periodic requalification processes, ongoing service provider monitoring, and regular compliance audits. Security in relationships with external providers is further reinforced through an updated third-party and vendor security policy. In addition, a data loss prevention solution is deployed to prevent unauthorized data breaches and ensure comprehensive protection of sensitive information.



### 5.2.6 National Culture and PhIDS Model Implementation

National culture plays a crucial role in shaping security-related policy, influencing the ability of both private and public entities to develop and invest in data security capacity building. It also significantly influences an organization's information security culture by shaping employees' attitudes, behaviors, and perceptions toward security practices (Connolly et al., 2019, Fang et al., 2016). Cultural factors can even impact an individual's ability to make effective cybersecurity decisions (Collier et al., 2023). Therefore, understanding and integrating cultural considerations into the adoption of the PhIDS Model is essential for developing effective and resilient data security strategies. Figure 50 provides an overview of Nigerian culture, based on the Country Comparison Tool (Country comparison tool, n. d.), while Table 14 describes the cultural dimensions.

**Power Distance.** Figure 50 shows that Nigeria scored 80 on the power distance dimension, indicating a high level. In high power distance environments, where authority and hierarchy are deeply respected, decision-making is typically reserved for top-level executives. This cultural trait can significantly affect the implementation of data security measures and the PhIDS model in several ways. The centralized decision-making may delay the adoption of proactive security measures within the PhIDS model. Furthermore, subordinates typically expect clear direction on what to do (Country comparison tool, n. d.). Therefore, employees may be more inclined to adhere to PhIDS policies if those in authority enforce them. However, lower-level employees might strictly follow orders rather than understand the rationale behind certain security protocols. Also, employees may be reluctant to question security protocols, fearing they might challenge authority. These limited feedback loops can hinder the effectiveness of the PhIDS model.

**Figure 50***Overview of Nigerian Culture*

**Note.** Based on content from *Country comparison tool* (n. d.), The Culture Factor.

Retrieved August 09, 2025, from <https://www.theculturefactor.com/country-comparison-tool?countries=nigeria>

**Individual versus Collectivism.** As shown in Figure 50, Nigeria, with a score of 0—the lowest in the Hofstede Insights database—is a highly collectivist society. In such cultures, people belong to strong “in groups,” such as family, extended family, or extended relationships, that take care of them in exchange for loyalty. Loyalty overrides most other societal rules and regulations, and members share a long-term commitment to the well-being of their group. Offenses can lead to shame and loss of face, and employer–employee relationships are often viewed in moral terms, similar to family ties. Hiring and promotion decisions are influenced by an individual’s in-group membership, and management tends to focus on leading groups rather than individuals (Country comparison tool, n. d.). Consequently, employees in Nigeria are likely to feel motivated to adhere to the PhIDS policies, as violations not only have individual consequences but may also cause loss of social standing within their community.

**Table 18***Ranking of Nigeria's Cultural Dimensions*

<b>Dimension</b>	<b>Relative ranking</b>	<b>General belief systems, values, attitudes, and traditions</b>
POWER DISTANCE INDEX (PDI)	HIGH	<ul style="list-style-type: none"> <li>• Acceptance of an established hierarchy where everyone understands their place without questioning.</li> <li>• Subordinates expect directions from superiors regarding responsibilities and tasks</li> <li>• A benevolent yet autocrat figure is seen as the ideal boss</li> </ul>
INDIVIDUALISM VERSUS COLLECTIVISM (IDV)	COLLECTIVISM	<ul style="list-style-type: none"> <li>• Belonging to strong in-groups (family, extended family, extended relationships) that provide mutual support.</li> <li>• Loyalty to the group overrides most other societal rules and regulations.</li> <li>• Close, long-term commitment to the member group's well-being.</li> <li>• Offenses lead to shame and loss of face.</li> <li>• Employer–employee relationships perceived in moral terms, akin to family ties.</li> <li>• Hiring and promotion are influenced by the individual's in-group membership.</li> <li>• Management focuses on leading and supporting groups rather than individuals.</li> </ul>
MASCULINITY VERSUS FEMINITY (MAS)	MASCULINITY	<ul style="list-style-type: none"> <li>• There is a strong emphasis on work as a central aspect of life</li> <li>• Managers are expected to be assertive and decisive</li> <li>• Competition, equity, and performance are emphasized in personal and professional settings</li> <li>• Conflicts are often addressed through fighting</li> </ul>
LONG-TERM ORIENTATION VERSUS SHORT-TERM NORMATIVE ORIENTATION (LTO)	SHORT-TERM NORMATIVE ORIENTATION	<ul style="list-style-type: none"> <li>• Focus on establishing absolute truths</li> <li>• A normative approach to thinking</li> <li>• A deep respect for tradition</li> <li>• Relative strong inclination toward saving for the future</li> <li>• A desire for quick results and immediate success</li> </ul>
INDULGENCE VERSUS RESTRAINT (IVR)	INDULGENCE	<ul style="list-style-type: none"> <li>• Willingness to fulfill their impulses and want to enjoy life and have fun</li> <li>• A positive attitude with a tendency for optimism</li> <li>• Leisure time is considered important, and individuals act as they see fit, spending money freely</li> </ul>
UNCERTAINTY AVOIDANCE INDEX (UAI)	INTERMEDIATE	<ul style="list-style-type: none"> <li>• There is a balanced approach to uncertainty, with no clear preference for either avoiding or accepting it.</li> </ul>

*Note.* Based on content from Country comparison tool (n. d.), *The Culture Factor*. Retrieved

August 09, 2025, from <https://www.theculturefactor.com/country-comparison->

tool?countries=nigeria

**Masculinity versus Femininity.** Figure 50 indicates that Nigeria has a score of 60 in this dimension, suggesting it is a masculine society. The emphasis in a masculine society is on assertiveness, achievement, and material success (Country comparison tool, n. d.).

Therefore, employees are more likely to adhere to PhIDS policies if they allow them to showcase their competency and control over their work environment.

**Uncertainty Avoidance.** Figure 50 shows that Nigeria has an intermediate score of 55 in this dimension. In a culture with an intermediate value, there is no clear preference for avoiding uncertainty (Country comparison tool, n. d.), indicating a more flexible and adaptive attitude toward ambiguous situations. Individuals rely more on informal rules and improvisation. This intermediate position also suggests that the culture may not prioritize or lean towards rigid and formal structures or measures to reduce uncertainty, encouraging a more flexible or moderately regulated approach to complying with PhIDS policies.

**Long-term versus Short-term Orientation.** Figure 50 shows that Nigeria's score in this dimension was quite low (8), indicating that its culture is more normative than pragmatic. A normative culture emphasizes short-term orientations and maintains adherence to established rules, norms, and customs (Country comparison tool, n. d.). This emphasis on tradition and short-term goals may lead to PhIDS policies that align closely with current practices and historical perspectives, rather than policies that prioritize long-term strategic changes or innovations. This focus might also create PhIDS policies that emphasize continuity and stability, potentially favoring incremental changes over radical shifts to ensure compliance with established norms and values within the organization. As a result, employees may be inclined to follow the PhIDS policies if doing so leads to short-term benefits, such as enhanced efficiency, immediate productivity improvements, or lower costs.

**Indulgence versus Restraint.** Figure 50 illustrates that Nigerian culture is characterized by a high indulgence score of 84. Indulgence implies relatively weak control over desires and impulses (Country comparison tool, n. d.). An indulgent culture may present challenges regarding policy compliance, as it can foster behaviors that prioritize personal desires, leisure, and enjoyment over strict adherence to policies. This culture, emphasizing

personal pleasure and freedom and marked by a strong inclination toward gratification, may not align well with policies that stress discipline and compliance with rules and procedures. Such a culture could potentially lead to lax enforcement of policies, especially those related to behavior codes, spending, or regulatory compliance.

These rankings emphasize the importance of considering national cultural contexts when implementing the PhIDS policies. Adapting security strategies to align with cultural values can improve compliance and effectiveness, ensuring that data security measures are both culturally relevant and effective.

### **5.3 Recommendations for Future Research**

The PhIDS Model offers an exciting opportunity for future research within the Nigerian pharmaceutical industry, requiring extensive investigations into its practical application and overall effectiveness. To start, dedicated research efforts should prioritize implementing and evaluating the PhIDS Model within this sector. This focus includes a comprehensive examination of the model's effectiveness in addressing common data security gaps, thereby reducing the risk of data breaches while enhancing regulatory compliance. Conducting real-world case studies and pilot implementations is essential for assessing its adaptability across various organizational structures and measuring the model's tangible impact on improving data security within the pharmaceutical landscape.

Research efforts should also aim to establish a knowledge-sharing platform, consortium, or community network devoted to the PhIDS Model's implementation and sustainability. This collaborative network should support the practical application of the model and help streamline data security practices to align with regulatory requirements. Promoting collaboration and knowledge exchange among industry stakeholders, academia, and regulatory bodies will be crucial in refining the model. This cooperative effort will facilitate the sharing of insights and practical experiences, fostering a collective understanding of data security

challenges and solutions within the pharmaceutical sector. By uniting diverse perspectives, this collaborative approach will enhance the model's applicability and capacity to effectively tackle multifaceted security risks.

Furthermore, research efforts should prioritize developing comprehensive training programs and capacity-building initiatives tailored to different stakeholders within the pharmaceutical ecosystem. These programs will equip participants with the essential skills and knowledge needed to effectively implement and maintain the PhIDS Model. Investing in skills enhancement and awareness campaigns will foster a culture of data security consciousness and ensure that the model is successfully implemented and sustainable across various organizational levels.

In parallel, the research should aim to thoroughly understand the PhIDS Model's adaptability to various organizational structures. This opportunity requires an in-depth examination of the complexities involved in tailoring the model to meet the specific needs and operational dynamics of diverse pharmaceutical organizations. It will also be critical to evaluate the model's capability to navigate multifaceted industry or government security requirements, ensuring its effectiveness and widespread adoption.

Furthermore, research on the PhIDS Model within the Nigerian pharmaceutical industry is closely linked with the emerging field of smart manufacturing systems and Industry 4.0. A vital area for future research lies in addressing the gap between the model's data security controls and the unaddressed data security concerns, such as data loss, IP theft, unauthorized extraction of confidential information, and the collection of sensitive business or personal data unique to smart factories. This study could explore how the model can be customized to mitigate data security risks within smart manufacturing systems.

Furthermore, it is essential to perform a thorough analysis of the PhIDS Model's impact on improving data security measures in the pharmaceutical industry. This analysis includes

evaluating how the implementation of the model affects security culture and resilience against potential cyber threats. Gaining insight into the tangible outcomes and improvements resulting from the model's adoption will offer concrete evidence of its effectiveness and inform future data protection strategies.

The research should also recognize the importance of continuous monitoring and evaluation of the PhIDS Model's implementation. Ongoing assessments and regular reviews are necessary to evaluate the model's adaptability and sustainability in response to evolving security threats, as well as its ongoing compliance with regulatory frameworks. By establishing a structured approach to continuous improvement, the model can preserve its lasting relevance and effectiveness within the ever-changing landscape of the pharmaceutical industry.

Future research could assess the adaptability and effectiveness of DLPSs by simulating diverse scenarios that reflect real-world usage in a manufacturing context. Given the potential for malicious actors to evade DLPS detection mechanisms through file binary manipulation, future studies could explore advanced detection techniques capable of identifying such altered files. Incorporating AI and ML into these research efforts could further enhance DLP technology and strengthen its ability to detect sensitive pharmaceutical data.

Essentially, future research on the PhIDS Model within the Nigerian pharmaceutical industry should take a multifaceted approach that includes practical implementation, economic implications, adaptability, capacity-building initiatives, collaboration, and ongoing evaluation. These research efforts would not only strengthen data security measures but also offer pragmatic insights into aligning data protection strategies at local and smart factories with global security standards, resulting in more resilient and secure drug manufacturing ecosystems.

## **5.4 Conclusions**

This study set out to examine data security gaps in Nigeria's pharmaceutical industry. The research responded to a critical problem: existing regulatory guidelines and organizational practices were insufficient to safeguard sensitive data in a highly regulated sector, leaving drug manufacturing operations vulnerable to cyber threats and operational disruptions. The findings indicate that health authorities' guidance documents, including those from the WHO and the PIC/S, lacked explicit provisions for essential security aspects such as data inventory, classification, segmentation, loss prevention, isolation and protection of data recovery instances, and secure service provider decommissioning. Also, data security controls within the Nigerian pharmaceutical sector were largely insufficient. Critical challenges include underdeveloped data management practices, unclear data ownership structures, governance risks, software integrity issues, inconsistent network security measures, USB vulnerabilities, gaps in supply chain integrity, and inadequate prioritization of data security. In addition, a lack of standardized risk assessment procedures, weak third-party data protection strategies, and poorly defined disaster recovery frameworks compound these shortcomings. Many organizations also struggle with implementing robust encryption methods, establishing effective access controls, and maintaining comprehensive audit trails. Despite widespread recognition of its importance, the study also revealed major gaps in structured and consistent protocols to safeguard data integrity. Weak audit trails, inadequate system validation and control, and the absence of standardized log review processes revealed regulatory non-compliance.

### **5.4.1 Implications for Theory and Practice**

The findings of this study carry important implications for both theory and practice. They inform ongoing discussions on data security and regulatory alignment within pharmaceutical manufacturing. The details of these implications are explored further below.



**Strengthening Data Security and Integrity Pharmaceutical Manufacturing.** Data security gaps leave drug manufacturing organizations exposed to significant risks, including operational disruptions, regulatory non-compliance, and cyber threats. Addressing these vulnerabilities requires a coordinated approach that combines regulatory intervention, enhanced security framework, and the adoption of advanced measures, such as real-time automated monitoring, predictive risk assessments, and updated security policies, tailored to the needs of pharmaceutical operations. By aligning data security practices with recognized best practices, Nigerian drug manufacturing organizations can reduce cyber threats, protect intellectual property, safeguard patient data, ensure regulatory compliance, and build trust within the pharmaceutical supply chain. Equally important, the findings reinforce the critical role of data integrity as a cornerstone of pharmaceutical manufacturing, directly influencing product quality, patient safety, and compliance with local and international regulations. Weak data integrity controls heighten the risk of non-compliance and undermine operational reliability. Fully adopting ALCOA+ principles is essential for building robust data integrity systems, strengthening compliance efforts, and ensuring alignment with evolving industry standards. From a theoretical perspective, these insights highlight significant gaps in data management within a regulated industry context, providing a foundation for refining existing models and developing targeted, long-term strategies that integrate security and integrity considerations. From a practical standpoint, they underscore the need for organizations to move from reactive to proactive security and integrity frameworks to achieve sustainability, reliability, and resilience in an increasingly complex threat landscape.

**Addressing Data Security Gaps in Regulatory Frameworks.** The study reveals key regulatory gaps, underscoring the need for best-practice data security provisions and positioning the PhIDS Model as a practical solution for enhanced compliance and resilience. From a theoretical perspective, these gaps demonstrate that current regulatory guidelines do

not adequately address modern cyber threats and highlight opportunities to expand existing data security frameworks by integrating these overlooked elements. The introduction of the PhIDS Model offers a structured, context-specific framework that integrates data protection, integrity, and governance principles into a cohesive model tailored for the pharmaceutical sector. From a practical perspective, the absence of these provisions in regulatory frameworks leads to inconsistencies in data security implementation across Nigerian pharmaceutical organizations, thereby worsening vulnerabilities. These findings underscore the urgent need for standardized regulations, tighter compliance enforcement, and an industry-wide shift toward more structured data protection practices. Integrating the PhIDS Model into Nigeria's pharmaceutical manufacturing sector represents a transformative step toward establishing robust data protection and regulatory compliance. Strengthening data security will not only protect sensitive pharmaceutical data but also build public trust in the industry's ability to maintain the integrity of medicinal products. Enforcing structured data security measures will further reduce cyber risks and position Nigerian pharmaceutical companies as trusted, resilient players within the global supply chain.

### **Bridging Gaps between Regulatory Guidance and Data Management Practices.**

The study's findings reveal that misalignment between regulatory guidelines and actual data management practices in pharmaceutical organizations creates significant vulnerabilities, carrying important implications for both theory and practice. From a theoretical perspective, the research bridges the gap between data security principles and their real-world application, expanding existing knowledge by demonstrating how deficiencies in regulatory alignment can expose critical weaknesses in pharmaceutical operations. These insights provide a foundation for refining existing frameworks and guiding future research to better integrate regulatory guidance with operational realities. From a practical perspective, the study underscores that such gaps can lead to data breaches that compromise regulatory credibility, medicine security,

and even national security. This highlights the urgent need for policymakers, regulatory agencies, and pharmaceutical organizations to adopt stronger and better-aligned data security measures. By evaluating shortcomings in current data management guidelines and proposing actionable solutions, the study offers concrete guidance to improve data security practices and strengthen resilience within the pharmaceutical industry.

**Bridging Local Challenges with Global Data Security Imperatives.** Although this study primarily examines data security challenges in Nigeria's pharmaceutical sector, its findings have important implications for both theory and practice. Practically, many of the identified security gaps are not unique to Nigeria but are widespread across pharmaceutical markets globally. This underscores the need for pharmaceutical organizations worldwide to proactively enhance their data security frameworks in alignment with best practices and evolving cyber threats. From a theoretical perspective, the study contextualizes data security challenges within a developing-country pharmaceutical setting, an area underrepresented in current scholarship. By situating Nigeria's pharmaceutical industry within a global supply chain context, the research highlights how institutional voids and inconsistent enforcement of data security standards influence system vulnerabilities. As the industry continues to digitize and integrate within interconnected global supply chains, cyber risks are anticipated to rise in scale and complexity. By illustrating how these vulnerabilities appear in a developing market, this study adds to existing literature and offers a strategic roadmap for tackling data security issues at both national and international levels.

#### **5.4.2 Contribution to Knowledge**

This study enhances the existing literature on data governance by providing empirical evidence of data security gaps in pharmaceutical manufacturing. It underscores the necessity of a strong data security framework and highlights the need for industry-specific cybersecurity strategies. Previous research primarily focused on data breaches in developed nations, creating

a gap in understanding how pharmaceutical companies in emerging markets manage data security. This study fills that gap by presenting a case study of Nigeria and offering comparative insights that inform international cybersecurity policies.

A significant contribution of this research is the introduction of the PhIDS Model, a structured framework designed to address data security gaps in Nigeria's pharmaceutical sector. By incorporating provisions based on internationally recognized data security principles, the model offers a comprehensive approach to enhancing data security and regulatory compliance within the pharmaceutical industry. It serves as both a benchmark and a practical guide for pharmaceutical organizations aiming to elevate their data security posture, filling a critical void in existing literature and practice.

#### **5.4.3 Closing Statement**

To sum up, this study demonstrates that addressing data security vulnerabilities in pharmaceutical operations requires more than fragmented controls—it calls for a unified, well-structured approach. By introducing and validating the PhIDS Model, this research not only advances theoretical understanding but also provides practical guidance for organizations and regulators. Strengthening data security is not merely a compliance requirement; it is a strategic imperative for safeguarding IP, protecting patients, and ensuring the future viability of the pharmaceutical industry.

## REFERENCES

- Aamir, M., & Zaidi, S. M. (2019). DDoS attack detection with feature engineering and machine learning: The framework and performance evaluation. *International Journal of Information Security*, 18, 761–785. <https://doi.org/10.1007/s10207-019-00434-1>
- About. (n.d.). NDPC. <https://ndpc.gov.ng/Home/About>
- About us. (n.d.). CordenPharma. <https://www.cordenpharma.com/about-us/>
- About PMG-MAN. (n.d.). PMGMAN. <https://pmgman.com/about/>
- Abraham, R., vom Brocke, J., & Schneider, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49, 424-438. <https://doi.org/10.1016/j.ijinfomgt.2019.07.008>
- Adami, M.F., & Kiger, A. (2005). The use of triangulation for completeness purposes. *Nurse Researcher*, 12(4), 19-29. <https://doi.org/10.7748/nr2005.04.12.4.19.c5956>
- Adenekan, O. A., Ezeigweneme, C., & Chukwurah, E. G. (2023). Strategies for protecting IT supply chains against cybersecurity threats. *International Journal of Management & Entrepreneurship Research*, 5(2), 87–96. <https://doi.org/10.51594/ijmer.v6i5.1125>
- Adeoti, E. (2023). A new era of data protection and privacy; Unveiling innovations & identifying gaps in the Nigeria Data Protection Act of 2023. *SSRN Electronic Journal*. <https://dx.doi.org/10.2139/ssrn.4520238>
- Adeyemi, B. B. (2024). Reliability and validity in quantitative research. In H. P. Bui (Ed.), *Applied linguistics and language education research methods: Fundamentals and innovations* (pp. 86–102). IGI Global. [https://books.google.co.uk/books/about/Applied\\_Linguistics\\_and\\_Language\\_Educational\\_innovations.html?id=xNOa0AEACAAJ&redir\\_esc=y](https://books.google.co.uk/books/about/Applied_Linguistics_and_Language_Educational_innovations.html?id=xNOa0AEACAAJ&redir_esc=y)

- Adigwe, O. P. (2023). Policies and practice in Nigeria's pharmaceutical sector: A mixed methods exploration of stakeholders' perspectives on strategic reforms. *Health Policy OPEN*, 4, 100091. <https://doi.org/10.1016/j.hpopen.2023.100091>
- Adigwe, O. P., & Onavbavba, G. (2024). The role of government in the achievement of medicines' security: A preliminary exploration of stakeholders' views and experience. *Plos One*, 19(6), e0299978. <https://doi.org/10.1371/journal.pone.0299978>
- Aguboshim, F. C., & Ezeasomba, I. N. (2022). Intellectual property rights: The effects on information security and research innovations in Nigeria. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 13(1), 113–129. <https://doi.org/10.7176/ISDE/10-7-06>
- Aguilar-Solano, M. (2020). Triangulation and trustworthiness: Advancing research on public service interpreting through qualitative case study methodologies. *FITISPosInternational Journal*, 7 (1), 31-52. <https://repositori.upf.edu/handle/10230/44595>
- Agwu, M. O. (2014). Organizational culture and employees performance in the National Agency for Food and Drugs Administration and Control (NAFDAC), Nigeria. *Global Journal of Management and Business Research*. [https://globaljournals.org/GJMBR\\_Volume14/1-Organizational-Culture-and-Employees-Performance.pdf](https://globaljournals.org/GJMBR_Volume14/1-Organizational-Culture-and-Employees-Performance.pdf)
- Ahern, D. M., Clouse, A., & Turner, R. (2008). *CMMI distilled: A practical introduction to integrated process improvement*. (3rd ed.). Addison-Wesley Professional. [https://books.google.com.ng/books?id=5-  
oaCyF0fxQC&printsec=frontcover&dq=CMMI+Distilled:+A+Practical+Introduction  
+to+Integrated+Process+Improvement+third+edition&hl=en&sa=X&redir\\_esc=y#v=](https://books.google.com.ng/books?id=5-<br/>oaCyF0fxQC&printsec=frontcover&dq=CMMI+Distilled:+A+Practical+Introduction<br/>+to+Integrated+Process+Improvement+third+edition&hl=en&sa=X&redir_esc=y#v=)

[onepage&q=CMMI%20Distilled%3A%20A%20Practical%20Introduction%20to%20Integrated%20Process%20Improvement%20third%20edition&f=false](#)

Ahmad, S., Mehfuz, S., & Beg, J. (2022). Cloud security framework and key management services collectively for implementing DLP and IRM. *Materials Today: Proceedings*, 62, 4828-4836. doi: 10.1016/j.matpr.2022.03.420

Ahmed, S. K. (2024). The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, 2, 100051. <https://doi.org/10.1016/j.glmedi.2024.100051>

Aibieyi, S., & Eke, A. F. (2022). An Evaluation of Regulatory Policies in Nigeria: A Case Study of National Agency for Food and Drug Administration and Control (NAFDAC) and Federal Character Commission (FCC). *ANSU Journal of Arts and Sciences (ANSUJASS)*, 9 (1): 31-44. <https://www.ansujassng.com/images/vol91/2StanAIBIEYIAmetu.pdf>

Aigbavboa, S., & Mbohwa, C. (2020). The headache of medicines' supply in Nigeria: an exploratory study on the most critical challenges of pharmaceutical outbound value chains. *Procedia Manufacturing*, 43, 336-343. <https://doi.org/10.1016/j.promfg.2020.02.170>

Akinwunmi, A. (2024, August). Nigeria - Data protection overview. DataGuidance. <https://www.dataguidance.com/notes/nigeria-data-protection-overview>

Akinyadenu, O. (2013). Counterfeit drugs in Nigeria: A threat to public health. *African Journal of Pharmacy and Pharmacology*, 7(36), 2571-2576. <https://doi.org/10.5897/AJPP12.343>

Akunyili, D. (2004). Fake and counterfeit drugs in the health sector: The role of medical doctors. *Annals of Ibadan Postgraduate Medicine*, 2(2), 19-23. <https://indexmedicus.afro.who.int/iah/fulltext/counterfeit.pdf>

- Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications*, 7(4), 485-498. <https://doi.org/10.14569/IJACSA.2016.070464>
- Alhassan, I., Sammon, D., & Daly, M. (2019). Critical success factors for data governance: A theory building approach. *Information Systems Management*, 36(2), 98-110. <https://doi.org/10.1080/10580530.2019.1589670>
- Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, 155, 1-8. <https://doi.org/10.1016/j.comcom.2020.03.007>
- Alhindi, H., Traore, I., & Woungang, I. (2021). Preventing data leak through semantic analysis. *Internet of Things*, 14, 100073. <https://doi.org/10.1016/j.iot.2019.100073>
- Aljawarneh, S. A., & Yassein, M. O. B. (2016). A conceptual security framework for cloud computing issues. *International Journal of Intelligent Information Technologies (IJIT)*, 12(2), 12-24. <https://doi.org/10.4018/IJIT.2016040102>
- AlKilani, H., Nasereddin, M., Hadi, A., & Tedmori, S. (2019, December). Data exfiltration techniques and data loss prevention system. In *2019 International Arab Conference on Information Technology (ACIT)* (pp. 124-127). IEEE. <https://doi.org/10.1109/ACIT47987.2019.8991131>
- Alshenqeeti, H. (2014). Interviewing as a data collection method: A critical review. *English Linguistics Research*, 3(1), 39-45. <https://doi.org/10.5430/elr.v3n1p39>
- Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018a). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, 23, 839-859. <https://doi.org/10.1007/s00779-017-1104-3>



- Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018b). Data governance taxonomy: Cloud versus non-cloud. *Sustainability*, 10(1), 1-26. <https://doi.org/10.3390/su10010095>
- Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications*, 62, 137-152. <https://doi.org/10.1016/j.jnca.2016.01.008>
- Amadi, L., & Amadi, M. (2014). Sustainable drug consumption, regulatory dynamics and fake drug repositioning in Nigeria: A case of NAFDAC. *Sci-Afric Journal of Scientific Issues, Research and Essays*, 2, 412-419. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.687.881&rep=rep1&type=pdf>
- Andreu, R., & Ciborra, C. (1996). Organizational learning and core capabilities development: The role of IT. *Journal of Strategic Information Systems*, 5(2), 111-127. [https://doi.org/10.1016/S0963-8687\(96\)80039-4](https://doi.org/10.1016/S0963-8687(96)80039-4)
- Angers, J., & Machtmes, K. (2005). An ethnographic-case study of beliefs, context factors, and practices of teachers integrating technology. *The Qualitative Report*, 10(4), 771-794. <https://doi.org/10.46743/2160-3715/2005.1832>
- Anthony, R. N. (1965). *Planning and control systems: A framework for analysis*. Division of Research, Graduate School of Business Administration, Harvard University. <https://www.amazon.com/Planning-Control-Systems-Framework-Analysis/dp/0875840477>
- Archive collected data, Technique T1560. (n.d.). attack.mitre.org. Retrieved December 7, 2023, from <https://attack.mitre.org/techniques/T1560/#:~:text=Compressing%20the%20data%20can%20help,upon%20inspection%20by%20a%20defender>
- Atkinson, P. A. (1997). Narrative turn or blind alley? *Qualitative Health Research* 7(3), 325-

344.<https://doi.org/10.1177/104973239700700302>

- Atkinson, P. A., & Coffey, A. (1997). Analysing documentary realities. In D. Silverman (Eds.), *Qualitative research: Theory, method and practice* (pp. 45–62). Sage Publications.<https://books.google.com.ng/books?id=-YvRs1O87KkC&printsec=frontcover#v=onepage&q&f=false>
- Atkinson, P., & Delamont, S. (2006). Rescuing narrative from qualitative research. *Narrative Inquiry* 16(1), 164-172.<https://doi.org/10.1075/ni.16.1.21atk>
- Atrinawati, L. H., Ramadhani, E., Fiqar, T. P., Wiranti, Y. T., Abdullah, A. I. N. F., Saputra, H. M. J., & Tandirau, D. B. (2021, February). Assessment of process capability level in University XYZ based on COBIT 2019. *Journal of Physics: Conference Series*, 1803, 1-11. <https://iopscience.iop.org/article/10.1088/1742-6596/1803/1/012033/meta>
- Attride-Stirling, J. (2001). Thematic networks: An analytic tool for qualitative research. *Qualitative Research*, 1(3), 385-405. <https://doi.org/10.1177/146879410100100307>
- Avizienis, A., Laprie, J., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 11–33. <https://doi.org/10.1109/TDSC.2004.2>
- Babalola, O. (2022). Nigeria’s data protection legal and institutional model: An overview. *International Data Privacy Law*, 12(1), 44-52. <https://doi.org/10.1093/idpl/ipab023>
- Ballard, C., Compert, C., Jesionowski, T., Milman, I., Plants, B., Rosen, B., & Smith, H. (2014). *Information governance principles and practices for a big data landscape*. IBM Redbooks.  
[https://books.google.com.ng/books/about/Information\\_Governance\\_Principles\\_and\\_Pr.html?id=-0M5AwAAQBAJ&printsec=frontcover&source=kp\\_read\\_button&hl=en&redir\\_esc=y#v=onepage&q&f=false](https://books.google.com.ng/books/about/Information_Governance_Principles_and_Pr.html?id=-0M5AwAAQBAJ&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false)

- Ballin, M., Di Zio, M., D'Orazio, M., Scanu, M., & Torelli, N. (2008). File concatenation of survey data: Computer intensive approach to sampling weights estimation. *Rivista di statistica ufficiale*, 10(2), 5-12. <http://hdl.handle.net/11368/3314>
- Barbour, R., & Schostak, J. F. (2005). Interviewing and focus groups. In B. Somekh & C. Lewin (Eds.), *Research methods in the Social Sciences* (pp. 41-48). Sage Publications. <https://www.worldcat.org/title/research-methods-in-the-social-sciences/oclc/56654330>
- Barker, J. M. (2016). *Data governance: The missing approach to improving data quality*. University of Phoenix. <https://media.proquest.com/media/hms/ORIG/2/whKIH?s=rv3kQZ1ncDy5mRA3tXuFDFO0vxs%3D>
- Beck, C. T. (2009). Critiquing qualitative research. *AORN Journal*, 90(4), 543-554. <https://doi.org/10.1016/j.aorn.2008.12.023>
- Begg, C., & Cairra, T. (2012). Exploring the SME quandary: Data governance in practise in the small to medium-sized enterprise sector. *The Electronic Journal Information Systems Evaluation*, 15(1), 3-13. <https://academic-publishing.org/index.php/ejise/article/view/237/200>
- Bell, E., & Bryman, A. (2007). The ethics of management research: an exploratory content analysis. *British Journal of Management* 18(1), 63-77. <https://doi.org/10.1111/j.1467-8551.2006.00487.x>
- Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, 2, 8-14. <https://doi.org/10.1016/j.npls.2016.01.001>
- Berg, B. L. (2007). *Qualitative research methods for the social sciences*. Pearson. <https://www.pearson.com/us/higher-education/product/Berg-Qualitative-Research-Methods-for-the-Social-Sciences-6th-Edition/9780205482634.html>

- Bergin, M. (2011). NVivo 8 and consistency in data analysis: reflecting on the use of a qualitative data analysis program. *Nurse Researcher*, 18(3), 6-12.  
<https://doi.org/10.7748/nr2011.04.18.3.6.c8457>
- Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and secure computing*, 2(1), 2-19.  
<https://doi.org/10.1109/TDSC.2005.9>
- BioDermByDesign customer. (n.d.). Navigator Business Solutions. <https://www.nbs-us.com/bioderm-bydesign-customer>
- Borgman, H., Heier, H., Bahli, B., & Boekamp, T. (2016). Dotting the I and crossing (out) the T in IT governance: New challenges for information governance. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4901-4909). IEEE. <https://doi.org/10.1109/HICSS.2016.608>
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27-40. doi:10.3316/QRJ0902027
- Boyd, C.O. (2001). Combining qualitative and quantitative research approaches. In P.L. Munhall (Eds.), *Nursing research: A qualitative perspective* (3rd ed., pp. 579-598). Jones and Bartlett.  
<https://books.google.com.ng/books?id=0drWE2JN1OgC&printsec=frontcover#v=onepage&q&f=false>
- Boynton, A. C., & Zmud, R. W. (1987). Information technology planning in the 1990's: Directions for practice and research. *MIS Quarterly* 11 (1), 58-71.  
<https://doi.org/10.2307/248826>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp063oa>

- Bree, R. T., & Gallagher, G. (2016). Using Microsoft Excel to code and thematically analyse qualitative data: A simple, cost-effective approach. *The All Ireland Journal of Teaching and Learning in Higher Education*, 8, 2811-28114. <https://ojs.aishe.org/index.php/aishe-j/article/view/281/467>
- Brewer, J., & Hunter, A. (1989). *Multimethod research: A synthesis of styles*, Sage Publications.   
[https://books.google.co.uk/books/about/Multimethod\\_Research.html?id=bbAOAQAAMAAJ&redir\\_esc=y#:~:text=Multimethod%20Research%20explains%20how%20a,and%20avoid%20vulnerability%20to%20error](https://books.google.co.uk/books/about/Multimethod_Research.html?id=bbAOAQAAMAAJ&redir_esc=y#:~:text=Multimethod%20Research%20explains%20how%20a,and%20avoid%20vulnerability%20to%20error)
- Britten, N. (1995). Qualitative research: qualitative interviews in research. *British Medical Journal*, 311, 251–253. <https://doi.org/10.1136/bmj.311.6999.251>
- Brous, P., Herder, P., & Janssen, M. (2016a). Governing asset management data infrastructures. *Procedia Computer Science*, 95, 303-310. <https://doi.org/10.1016/j.procs.2016.09.339>
- Brous, P., Janssen, M., & Herder, P. (2016b). Coordinating data-driven decision-making in public asset management organizations: A quasi-experiment for assessing the impact of data governance on asset management decision making. In D. Y. al. (Eds.), *Social media: The good, the bad, and the ugly. I3E 2016. Lecture notes in computer science: 9844* (pp. 573-583). Springer. [https://doi.org/10.1007/978-3-319-45234-0\\_51](https://doi.org/10.1007/978-3-319-45234-0_51)
- Brown, C. V. (1997). Examining the emergence of hybrid IS governance solutions: Evidence from a single case site. *Information Systems Research*, 8(1), 69–94. <http://www.jstor.org/stable/23010934>
- Bruhn, J. (2014). Identifying useful approaches to the governance of indigenous data. *The International Indigenous Policy Journal*, 5(2), 1-32. <https://doi.org/10.18584/iipj.2014.5.2.5>

- Brunswick, D. (2019). Data privacy, data protection and the importance of integration for GDPR compliance. *ISACA Journal*, 3, 14-17. <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/data-privacy-data-protection-and-the-importance-of-integration-for-gdpr-compliance>
- Bryman, A. (2012). *Social research methods*. (4th ed.). Oxford University Press. <https://books.google.com.ng/books?id=vCq5m2hPkOMC&printsec=frontcover#v=onepage&q&f=false>
- Brynjolfsson, E. (1993). The productivity paradox of information technology. *Communications of the ACM* 36(12), 66–77. <https://doi.org/10.1145/163298.163309>
- Burnard, P., Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Analysing and presenting qualitative data. *British Dental Journal*, 204(8), 429-432. <https://doi.org/10.1038/sj.bdj.2008.292>
- Cabinet Office. (2011). *ITIL lifecycle suite*. The Stationery Office. <https://www.amazon.co.uk/ITIL-Lifecycle-Suite-Cabinet-Office/dp/0113313233>
- CardinalStone. (2014). *Fidson Healthcare Plc: Pioneering a new vista*. <https://docplayer.net/41116029-Initiation-of-coverage-fidson-healthcare-plc.html>
- CardinalStone. (2017). *Fidson Healthcare Plc: New plant is delivering enormous value*. <https://www.proshareng.com/news/Stock%20&%20Analyst%20Updates/Fidson-Healthcare-Plc-New-plant-is-Delivering-Enormous-Value/35727>
- Carolan, M. (2003). Reflexivity: A personal journey during data collection. *Nurse Researcher*, 10(3), 7-14. <http://doi.org/10.7748/nr2003.04.10.3.7.c5892>
- Carretero, A. G., Gualo, F., Caballero, I., & Piattini, M. (2017). MAMD 2.0: Environment for data quality processes implantation based on ISO 8000-6X and ISO/IEC 33000. *Computer Standards & Interfaces*, 54(3), 139-151. <https://doi.org/10.1016/j.csi.2016.11.008>
- Casey, D., & Murphy, K. (2009). Issues in using methodological triangulation in research.

Nurse                                      Researcher                                      16(4),                                      40-55.

<https://link.gale.com/apps/doc/A205249299/HRCA?u=anon~cb87e27b&sid=googleScholar&xid=d8f4a270>

- Chan, Y. E., Huff, S. L., Barclay, D. W., & Copeland, D. G. (1997). Business strategic orientation, information systems strategic orientation, and strategic alignment. *Information Systems Research*, 8(2), 125–150. <http://www.jstor.org/stable/23010900>
- Chapple, M., Maymi, D. V., & Gibson, D. (2018). *CISSP (ISC)<sup>2</sup> Certified Information Systems Security Professional Official Study Guide* (8th ed.). Wiley.
- Cheng, G., Li, Y., Gao, Z., & Liu, X. (2017). Cloud data governance maturity model. In *Proceedings of 2017 IEEE 8th International Conference on Software Engineering and Service Science (ICSESS)*, (pp. 517-520). IEEE. <https://doi.org/10.1109/ICSESS.2017.8342968>
- Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), 1-14. <https://doi.org/10.1002/widm.1211>
- Cheong, L. K., & Chang, V. (2007). The need for data governance: A case study. In *ACIS 2007 Proceedings* (pp. 999-1008). <http://aisel.aisnet.org/acis2007/100>
- Cherdantseva Y., & Hilton, J. (2014). Information security and information assurance. The discussion about the meaning, scope and goals. In F. Almeida & I. Portela (Eds.), *Organizational, legal, and technological dimensions of information systems administration* (pp. 167-198). IGI Global Publishing. <https://www.igi-global.com/gateway/chapter/80717>
- Chhetri, S. R., Rashid, N., Faezi, S., & Al Faruque, M. A. (2017). Security trends and advances in manufacturing systems in the era of industry 4.0. In *2017 IEEE/ACM International*

- Conference on Computer-Aided Design (ICCAD)* (pp. 1039-1046). doi: 10.1109/ICCAD.2017.8203896
- Chika, D.M., & Tochukwu, E.S. (2020). An analysis of data protection and compliance in Nigeria. *International Journal of Research and Innovation in Social Science (IJRISS)*, 4(5), 377-382. <https://www.rsisinternational.org/journals/ijriss/Digital-Library/volume-4-issue-5/377-382.pdf>
- Chopra, A. (2021). Cyberattack-intangible damages in a virtual world: Property insurance companies declare war on cyber-attack insurance claims. *Ohio State Law Journal*, 82, 121-162. <http://hdl.handle.net/1811/101097>
- CIS Critical Security Controls Version 8. (n. d). Center for Internet Security. <https://learn.cisecurity.org/e/799323/1-799323-2020-07-22-28vhr/34gng/353120386?h=PFal4bZFIsWyxUZLtapobIQYuJN4rdKfpl2c7F7301o>
- CIS security controls. (2021). Center for Internet Security. <https://www.cisecurity.org/controls/>
- Clarke, C., Reed, J. & Keyes, S. E. (2015). Case study research. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 279-290). John Wiley & Sons. <https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=301>
- Clemmons, S, & Simon, S 2001. Control and coordination in global ERP configuration. *Business Process Management Journal*, 7(3), 205-215. <https://doi.org/10.1108/14637150110392665>
- Cole, J., & Gardner, K. (1979). Topic work with first-year secondary pupils. In E. Lunzer & K. Gardner (Eds.) *The effective use of reading* (pp. 167–192). Heinemann Educational Books. <https://eric.ed.gov/?id=ED174979>
- Collier, H., Morton, C., Alharthi, D., & Kleiner, J. (2023). Cultural influences on information security. University of Colorado Colorado Springs. *Proceedings of the 22nd European*



- Conference on Cyber Warfare and Security (ECCWS)*, 22(1). 143-150.  
<https://doi.org/10.34190/eccws.22.1.1127>
- Committee of Sponsoring Organizations of the Treadway Commission (1992). *Internal control, integrated framework: Framework including executive summary*.  
[https://egrove.olemiss.edu/aicpa\\_assoc/20](https://egrove.olemiss.edu/aicpa_assoc/20)
- Committee on National Security Systems. (2010, April 26). *National Information Assurance (IA) Glossary* (CNSS Instruction No. 4009).  
[https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009\\_National\\_Information\\_Assurance.pdf](https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf)
- Connolly, L. Y., Lang, M., & Wall, D. S. (2019). Information security behavior: A cross-cultural comparison of Irish and US employees. *Information Systems Management*, 36(4), 306–322. <https://doi.org/10.1080/10580530.2019.1651113>
- Constella (n.d). *Pharma sector exposure report: 2018-2021 digital risk findings and trends*.  
<https://info.constellaintelligence.com/pharmaceutical-sector-exposure-report-2021>
- Corbin, J., & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (3rd ed.). Sage Publications.  
<https://dx.doi.org/10.4135/9781452230153>
- CordenPharma adopts CIS Controls as their framework. (n.d.). Center for Internet Security.  
<https://www.cisecurity.org/insights/case-study/corden-pharma-adopts-cis-controls-as-their-framework>
- Country comparison. (n.d.). *Hofstede insights*. Retrieved April 30, 2023, from  
<https://www.hofstede-insights.com/country-comparison/nigeria/>
- Cousins, K. (2016). Health IT legislation in the United States: Guidelines for IS researchers. *Communications of the Association for Information Systems*, 39, 338-366.  
<https://doi.org/10.17705/1CAIS.03917>

- Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches*. Sage Publications.  
<https://books.google.co.uk/books?id=Ykruxor10cYC&printsec=frontcover#v=onepage&q&f=false>
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.  
[https://www.ucg.ac.me/skladiste/blog\\_609332/objava\\_105202/fajlovi/Creswell.pdf](https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf)
- Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, 147(2), 432–448. <https://doi.org/10.1016/j.jfineco.2022.12.002>
- Cybersecurity Audit Program: Based on the NIST Cybersecurity Framework* [Microsoft Excel spreadsheet]. (n.d.). ISACA. <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx>
- Daley, B., Geelen, T., & Green, B. (2023). Due diligence. *Journal of Finance, Forthcoming*.  
<http://dx.doi.org/10.2139/ssrn.3702560>
- Daly, J., Kellehear, A., & Gliksman, M. (1997). *The public health researcher: A methodological approach*. Oxford University Press. <https://nla.gov.au/nla.cat-vn1642016>
- DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd ed.). Technics Publications.  
[https://books.google.co.uk/books/about/DAMA\\_DMBOK.html?id=YjacswEACAAJ&redir\\_esc=y](https://books.google.co.uk/books/about/DAMA_DMBOK.html?id=YjacswEACAAJ&redir_esc=y)
- Dardick, G. S. (2010). Cyber Forensics Assurance. *Australian Digital Forensics Conference Proceedings* (pp.57-64). <https://doi.org/10.4225/75/57b2926c40cda>

- Dahlberg, T., & Nokkala, T. (2015). A framework for the corporate governance of data – Theoretical background and empirical evidence. *Business, Management and Education*, 13(1), 25-45. <https://doi.org/10.3846/bme.2015.254>
- Deepu, T. S., & Ravi, V. (2021). A conceptual framework for supply chain digitalization using integrated systems model approach and DIKW Hierarchy. *Intelligent Systems with Applications*, 10, 1-11. <https://doi.org/10.1016/j.iswa.2021.200048>
- De Abreu Faria, F., Maçada, A. C., & Kumar, K. (2013). Information governance in the banking industry. *Proceedings of the 46th Hawaii International Conference on System Sciences* (pp. 4436-4445). IEEE. <https://doi.org/10.1109/HICSS.2013.270>
- De Haes, S., & Van Grembergen, W. (2008, January). Analysing the relationship between IT governance and business/IT alignment maturity. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 428-428). IEEE. <https://doi.org/10.1109/HICSS.2008.66>
- De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management* 26 (2), 123-137. <https://doi.org/10.1080/10580530902794786>
- De Haes, S., Van Grembergen, W., & Debreceeny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, 27(1), 307-324. <https://doi.org/10.2308/isys-50422>
- De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). COBIT as a framework for enterprise governance of IT. In *Enterprise governance of information technology* (pp. 125-162). Springer. [https://doi.org/10.1007/978-3-030-25918-1\\_5](https://doi.org/10.1007/978-3-030-25918-1_5)
- Denzin, N. K. (1970). *The research act: A theoretical introduction to sociological methods*. McGraw-Hill.
- [https://books.google.com.ng/books/about/The\\_Research\\_Act.html?id=cfoAAAAIA](https://books.google.com.ng/books/about/The_Research_Act.html?id=cfoAAAAIA)

AJ&redir\_esc=y

Denzin, N.K. (1989). *The research act*. (3rd ed.). McGraw-Hill.

<https://www.worldcat.org/title/research-act-a-theoretical-introduction-to-sociological-methods/oclc/17878165>

Dhawan, S. (2014). Information and data security concepts, integrations, limitations and future. *International Journal of Advanced Information Science and Technology (IJAIST)*, 3(9), 9-13. <https://doi.org/10.15693/ijaist/2014.v3i9.9-13>

Dreibelbis, A., Hechler, E., Milman, I., Oberhofer, M., & van Run, P. (2008). *Enterprise master data management: An SOA approach to managing core information*. IBM Press.

[https://www.researchgate.net/profile/Ivan-Milman/publication/235720534\\_Enterprise\\_Master\\_Data\\_Management\\_An\\_SOA\\_A\\_pproach\\_to\\_Managing\\_Core\\_Information/links/58d087fd92851c8841c288a7/Enterprise-Master-Data-Management-An-SOA-Approach-to-Managing-Core-Information.pdf](https://www.researchgate.net/profile/Ivan-Milman/publication/235720534_Enterprise_Master_Data_Management_An_SOA_A_pproach_to_Managing_Core_Information/links/58d087fd92851c8841c288a7/Enterprise-Master-Data-Management-An-SOA-Approach-to-Managing-Core-Information.pdf)

*Drugs & medical devices*. (n. d.). NAFDAC. <https://www.nafdac.gov.ng/drugs/>

Du, D., Yu, L., & Brooks, R. R. (2015). Semantic similarity detection for data leak prevention. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference* (pp. 1-6). <https://doi.org/10.1145/2746266.2746270>

Dyché, J., & Levy, E. (2006). *Customer data integration*. John Wiley & Sons. [https://books.google.com.ng/books/about/Customer\\_Data\\_Integration.html?id=ICR44R1xZY0C&printsec=frontcover&source=kp\\_read\\_button&hl=en&redir\\_esc=y#v=onepage&q&f=false](https://books.google.com.ng/books/about/Customer_Data_Integration.html?id=ICR44R1xZY0C&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false)

Earl, M. J. (1989). *Management strategies for information technology*. Prentice Hall. <https://www.amazon.com/exec/obidos/ASIN/0135516641/acmorg-20>

- Easterby-Smith, M., Thorpe, R. & Jackson, P. (2015). *Management and business research*. (5th ed.). London: Sage Publications. <https://www.worldcat.org/title/management-and-businessresearch/oclc/909223005>
- Education and training*. (n.d.). Pharmacists Council of Nigeria. <https://www.pcn.gov.ng/education-and-training/>
- Ein-Dor, P., & Segev, E. (1982). Organizational context and MIS structure: Some empirical evidence. *MIS Quarterly*, 6(3), 55–68. <https://doi.org/10.2307/248656>
- Eisner, E. W. (1991). *The enlightened eye: Qualitative inquiry and the enhancement of educational practice*. Prentice Hall College. [https://books.google.com.ng/books/about/The\\_Enlightened\\_Eye.html?id=09UcDgAAQBAJ&redir\\_esc=y](https://books.google.com.ng/books/about/The_Enlightened_Eye.html?id=09UcDgAAQBAJ&redir_esc=y)
- Ekhator, O. (2024, January 29). *Nigeria's data protection regulator is investigating 17 data breaches*. Techpoint.africa. <https://techpoint.africa/2024/01/29/nigeria-data-protection-breaches/>
- Elijah, O., Ling, P. A., Rahim, S. K. A., Geok, T. K., Arsad, A., Kadir, E. A., ... & Abdulfatah, M. Y. (2021). A survey on industry 4.0 for the oil and gas industry: Upstream sector. *IEEE Access*, 9, 144438-144468. <https://ieeexplore.ieee.org/iel7/6287639/6514899/09579415.pdf>
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 5(1), 1-4. [https://www.academia.edu/download/55796997/Comparison\\_Convenience\\_and\\_Purposive\\_Sampling-2016\\_4p.pdf](https://www.academia.edu/download/55796997/Comparison_Convenience_and_Purposive_Sampling-2016_4p.pdf)
- Eryurek, E., Gilad, U., Lakshmanan, V., Kibunguchy-Grant, A., & Ashdown, J. (2021). *Data governance: The definitive guide*. O'Reilly Media. <https://books.google.co.uk/books?hl=en&lr=&id=jQYiEAAAQBAJ&oi=fnd&pg=PP>

1&dq=Data+Governance:+The+Definitive+Guide&ots=jIINc\_P5cV&sig=umciBkyu  
 DJIbhB3fX5tCX\_BstvA&redir\_esc=y#v=onepage&q=Data%20Governance%3A%20  
 The%20Definitive%20Guide&f=false.

European Commission. (2011). *Good manufacturing practice medicinal products for human and veterinary use* (EudraLex: Vol. 4). Health and Consumers Directorate-General.

[https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-4/chapter4\\_01-2011\\_en.pdf](https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-4/chapter4_01-2011_en.pdf)

Eze, G. P. (2019). The impact of trade volume on stock market returns of Nigerian pharmaceutical companies. *International Journal of Social Sciences and Management Research*, 5(1), 36-52.

<http://iiardpub.org/get/IJSSMR/VOL.%205%20NO.%201%202019/The%20impact%20of%20trade.pdf>

Fadare, J. O., Oshikoya, K. A., Ogunleye, O. O., Desalu, O. O., Ferrario, A., Enwere, O. O., ... Godman, B. (2018). Drug promotional activities in Nigeria: Impact on the prescribing patterns and practices of medical practitioners and the implications. *Hospital practice*, 46(2), 77-87. <https://doi.org/10.1080/21548331.2018.1437319>

Fagbolu, O., & Nnebue, J. (2019). *Fidson Healthcare Plc - Still set to deliver value to shareholders*. CardinalStone. <https://research.cardinalstone.com/reports>

Fang, X., Lederer, A. L., & Benamati, J. "Skip." (2016). The influence of national culture on information technology development, implementation, and support challenges in China and the United States. *Journal of Global Information Technology Management*, 19(1), 26–43. <https://doi.org/10.1080/1097198X.2016.1134170>

FAQS. (n.d.). Nigerian Data Protection Commission. <https://ndpc.gov.ng/faqs/>

- Federal Republic of Nigeria. (2021, April). National Cybersecurity Policy and Strategy. [https://cert.gov.ng/ngcert/resources/NATIONAL\\_CYBERSECURITY\\_POLICY\\_AND\\_STRATEGY\\_2021.pdf](https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf)
- Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, 5(1), 80-92. <https://doi.org/10.1177/160940690600500107>
- Findley, M. G., Kikuta, K., & Denly, M. (2021). External validity. *Annual Review of Political Science*, 24(1), 365-393. <https://doi.org/10.1146/annurev-polisci-041719-102556>
- Firestone, W. A. (1993). Alternative arguments for generalizing from data as applied to qualitative research. *Educational Researcher*, 22(4), 16–23. <https://doi.org/10.3102/0013189X022004016>
- Flick, U. (2009). *An introduction to qualitative research* (4th ed.). Sage Publications. <https://books.google.com.ng/books?id=sFv1oWX2DoEC&printsec=frontcover#v=onepage&q&f=false>
- Flindon, W. G., & Divya, S. V. (2022). Secured cloud data storage with industrial IoT. In V. Gomathi & V. Kalaivani (Eds.), *AIP Conference Proceedings: Vol. 2444* (p. 050002). <https://doi.org/10.1063/5.0078382>
- FM'tHoen, E., Hogerzeil, H. V., Quick, J. D., & Sillo, H. B. (2014). A quiet revolution in global public health: The World Health Organization's Prequalification of Medicines Programme. *Journal of public health policy*, 35(2), 137-161. <https://doi.org/10.1057/jphp.2013.53>
- Forslund, H. (2010). ERP systems' capabilities for supply chain performance management. *Industrial Management & Data Systems*, 110, 351-367. <https://doi.org/10.1108/02635571011030024>

- Foss, C., & Ellefsen, B. (2002). The value of combining qualitative and quantitative approaches in nursing research by means of method triangulation. *Journal of Advanced Nursing*, 40, 242-248. <https://doi.org/10.1046/j.1365-2648.2002.02366.x>
- Frangie, R. C., Mihalic, A., Chehab, T., Kan, J., Luk, C., & Perinpacumarasamy, S. (2018, April). Smart railways... or not so smart: A cyber security perspective. In *Proceedings of the Conference on Railway Excellence* (pp. 230-239). <https://ndy.com/wp-content/uploads/2019/01/SMART-RAILWAYS...-OR-NOT-SO-SMART-A-CYBER-SECURITY-PERSPECTIVE.pdf>
- Freshwater D., & Holloway, I. (2015). Narrative research. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 225-235). John Wiley & Sons. <https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=247>
- Fu, J. S., Liu, Y., Chao, H. C., Bhargava, B. K., & Zhang, Z. J. (2018). Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics*, 14(10), 4519-4528. <https://doi.org/10.1109/TII.2018.2793350>
- Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408–1416. <https://doi.org/10.46743/2160-3715/2015.2281>
- Gagel, C. (1997). Literacy and technology: Reflections and insights for technological literacy. *Journal of Industrial Teacher Education*, 34(3), 6–34. <https://scholar.lib.vt.edu/ejournals/JITE/v34n3/Gagel.html>
- Gaidarski, I., & Kutinchev, P. (2021). An approach for constructing a simulation model for dynamic analysis of the information security system. In A. Abraham, N. Gandhi, T. Hanne, TP. Hong, T. Nogueira Rios, & W. Ding (Eds.), *21st International Conference*



*on Intelligent Systems Design and Applications (ISDA 2021)* (pp. 518-522). Springer.

[https://doi.org/10.1007/978-3-030-96308-8\\_48](https://doi.org/10.1007/978-3-030-96308-8_48)

Galvin, K. T., & Holloway, I. (2015). Phenomenological research. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 211-223). John Wiley & Sons.  
<https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=233>

Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, 13(117), 1–8. <https://doi.org/10.1186/1471-2288-13-117>

Gasser, L., & Aad, I. (2023). Disk, file, and database encryption. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), *Trends in data protection and encryption technologies* (pp. 201-202). Springer, Cham. [https://doi.org/10.1007/978-3-031-33386-6\\_33](https://doi.org/10.1007/978-3-031-33386-6_33)

Gerrish, K., & Lathlean, J. (2015). *The research process in nursing*. John Wiley & Sons.  
<https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&query=the+research+process+in+nursing#>

Giralt, A. N., Schiavetti, B., Meessen, B., Pouget, C., Caudron, J. M., Marchal, B., ...Ravinetto, R. (2017). Quality assurance of medicines supplied to low-income and middle-income countries: poor products in shiny boxes? *BMJ Global Health*, 2(2), 1-10.  
<https://doi.org/10.1136/bmjgh-2016-000172>

Goldstein, A. E., & Reiboldt, W. (2004). The multiple roles of low income, minority women in the family and community: A qualitative investigation. *The Qualitative Report*, 9(2), 241–265. <https://doi.org/10.46743/2160-3715/2004.1927>

*Global API, excipient, drug product, & packaging CDMO.* (n.d.). CordenPharma.  
<https://www.cordenpharma.com/>

Gong, Y., & Janssen, M. (2019). The value of and myths about enterprise architecture.  
*International Journal of Information Management*, 46, 1-9.  
<https://doi.org/10.1016/j.ijinfomgt.2018.11.006>

Grimstad, T., & Myrseth, P. (2010, October). Information governance and metadata strategies as a basis for cross-sector e-Services. In P. Cunningham, & M. Cunningham (Eds.), *eChallenges e-2010 Conference Proceedings* (pp. 1-8). IEEE.  
[https://www.academia.edu/download/82302899/eChallenges\\_2010\\_Grimstad\\_Metadata.pdf](https://www.academia.edu/download/82302899/eChallenges_2010_Grimstad_Metadata.pdf)

Groš, S. (2021, June). A critical view on CIS controls. In *Proceedings of the 2021 16th International Conference on Telecommunications (ConTEL)* (pp. 122-128).  
<https://arxiv.org/pdf/1910.01721>

Guba, E. G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Communication and Technology*, 29(2), 75-91. <https://doi.org/10.2307/30219811>

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 105-117). Sage Publications.  
<https://eclass.uoa.gr/modules/document/file.php/PPP356/Guba%20%26%20Lincoln%201994.pdf>

Gubrium, J. F., & Holstein, J. A. (2002). *Handbook of interview research: Context and method*. Sage Publications.  
<https://books.google.com.ng/books?id=uQMUMQJZU4gC&printsec=frontcover#v=onepage&q&f=false>

- Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, 18(1), 59–82. <https://doi.org/10.1177/1525822X05279903>
- Guetat, S. B., & Dakhli, S. B. (2015). The architecture facet of information governance: The case of urbanized information systems. *Procedia Computer Science*, 64, 1088-1098. <https://doi.org/10.1016/j.procs.2015.08.564>
- Gugelmann, D., Studerus, P., Lenders, V., & Ager, B. (2015). Can content-based data loss prevention solutions prevent data leakage in web traffic? *IEEE Security & Privacy*, 13(4), 52-59. <https://doi.org/10.1109/MSP.2015.88>
- Guha, A., Samanta, D., Banerjee, A., & Agarwal, D. (2021). A deep learning model for information loss prevention from multi-page digital documents. *IEEE Access*, 9, 80451-80465. doi:10.1109/ACCESS.2021.3084841
- Guillemin, M. and Gillam, L. (2004). Ethics, reflexivity, and “ethically important moments” in research. *Qualitative inquiry* 10(2), 261-280. <https://doi.org/10.1177/1077800403262360>
- Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. *Academy of Business, Engineering and Science, Halmstad University*. <https://hh.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf>
- Halcomb, E., & Andrew, S. (2005). Triangulation as a method for contemporary nursing research. *Nurse Researcher*, 13(2), 71-82. <https://doi.org/10.7748/nr.13.2.71.s8>
- Hagmann, J. (2013). Information governance – Beyond the buzz. *Records Management Journal*, 23(3), 228-240. <https://doi.org/10.1108/RMJ-04-2013-0008>
- Halder, S., & Newe, T. (2022). Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT. *Future Generation Computer Systems*, 133, 351-363. <https://doi.org/10.1016/j.future.2022.03.032>

- Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction*, 31(3), 498-501. <https://doi.org/10.1093/humrep/dev334>
- Han, J., Pei, J., & Tong, H. (2022). *Data mining: Concepts and techniques*. Morgan Kaufmann. <https://books.google.co.uk/books?id=NR1oEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false>
- Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, 4 (4), 27-47. <https://doi.org/10.12821/ijispm040402>
- Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 472-484. <https://doi.org/10.1147/sj.382.0472>
- Hewege, C. R. (2012). A critique of the mainstream management control theory and the way forward. *SAGE open*, 2(4), 1-11. <https://doi.org/10.1177/2158244012470114>
- Hinchliffe, A. (2017). Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. *Computer Fraud & Security*, 2017(5), 5-9. [https://doi.org/10.1016/S1361-3723\(17\)30040-4](https://doi.org/10.1016/S1361-3723(17)30040-4)
- Hinds, P. S. (1989). Method triangulation to index change in clinical phenomena. *Western Journal of Nursing Research*, 11(4), 440-447. <https://doi.org/10.1177/019394598901100406>
- Holloway, I., & Galvin, K. T. (2015a). Ethnography. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 199-210). John Wiley & Sons. <https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=221>

- Holloway, I., & Galvin, K. T. (2015b). Grounded Theory. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 185-197). John Wiley & Sons. <https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=207>
- Holsti, O.R. (1969). *Content analysis for the social sciences and humanities*. Addison-Wesley Publications. <https://www.worldcat.org/title/content-analysis-for-the-social-sciences-and-humanities/oclc/45548>
- Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher* 20(4), 12–17. [https://www.researchgate.net/publication/236072601\\_Rigour\\_in\\_qualitative\\_case-study\\_research](https://www.researchgate.net/publication/236072601_Rigour_in_qualitative_case-study_research)
- Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15 (9), 1277–1288. <https://doi.org/10.1177/1049732305276687>
- Hu, Q., & Huang, C. D. (2006). Using the balanced scorecard to achieve sustained IT-business alignment: A case study. *Communications of the Association for Information Systems* 17(1), 180-205. <https://doi.org/10.17705/1CAIS.01708>
- Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3). 1-13. <https://doi.org/10.1016/j.heliyon.2021.e06522>
- Hunt, K., & Lathlean, J. (2015). Sampling. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 173-184). John Wiley & Sons. <https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=195>

- Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. (2018, January). Answering key global IT management concerns through IT governance and management processes: A COBIT 5 View. In *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 5335-5344). AIS Electronic Library (AISeL).  
<http://hdl.handle.net/10125/50554>
- Huygh, T., Steuperaert, D., De Haes, S., & Joshi, A. (n.d.). The role of compliance requirements in IT governance implementation: An empirical study based on COBIT 2019. In *Proceedings of the 2022 55th Hawaii International Conference on System Sciences* (pp. 1-10).  
[https://www.researchgate.net/publication/354718657\\_The\\_Role\\_of\\_Compliance\\_Requirements\\_in\\_IT\\_Governance\\_Implementation\\_An\\_Empirical\\_Study\\_Based\\_on\\_COBIT\\_2019](https://www.researchgate.net/publication/354718657_The_Role_of_Compliance_Requirements_in_IT_Governance_Implementation_An_Empirical_Study_Based_on_COBIT_2019)
- Hidayat, R. S., Prasetyo, H., Yulianto, A., & Nurhidayati, S. (2023). Analysis of IT governance maturity level in information security sector using COBIT 2019 framework. *Journal LaMultiapp*, 4(2), 1–10.  
<https://newinera.com/index.php/JournalLaMultiapp/article/view/1514/1471>
- IBM Security. (2020). *Cost of data breach report*. Retrieved from  
<https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf>
- IBM Security. (2022). *X-Force Threat Intelligence Index 2022*.  
<https://www.ibm.com/security/data-breach/threat-intelligence/>
- Igbokwe-Ibeto, C. J. (2015). Re-inventing Nigeria's public sector: A review of National Agency for Food, Drug Administration and Control (NAFDAC). *Africa's Public Service Delivery & Performance Review*, 3(2), 183-211.  
<https://doi.org/10.4102/apsdpr.v3i2.85>

- Ikusika, B. (2023). A critical analysis of cybersecurity in Nigeria and the incidents of cyber-attacks on businesses/companies. *Journal of Cybersecurity and Digital Policy*, 4(1), 45–63. <https://ssrn.com/abstract=4165204>
- Imasuen, I. (2021). *The WTO–TRIPS Agreement and the regulation of counterfeit pharmaceutical products in Nigeria* (Doctoral dissertation, University of East London). <https://doi.org/10.15123/uel.89y14>
- Information Systems Audit and Control Association. (2012a). *COBIT 5: A business framework for the governance and management of enterprise IT*. <https://www.worldcat.org/title/cobit-5-a-business-framework-for-the-governance-and-management-of-enterprise-it/oclc/816978353>
- Information Systems Audit and Control Association. (2012b). *COBIT 5: Enabling processes*. <https://www.amazon.com/COBIT-5-Enabling-Processes-Isaca/dp/1604202394>
- Information Systems Audit and Control Association. (2013a). *COBIT 5: Enabling information*. [https://books.google.com.ng/books?id=G2BsAwAAQBAJ&printsec=copyright&redir\\_esc=y#v=onepage&q&f=false](https://books.google.com.ng/books?id=G2BsAwAAQBAJ&printsec=copyright&redir_esc=y#v=onepage&q&f=false)
- Information Systems Audit and Control Association. (2013b). *COBIT 5 for assurance*. <https://www.isaca.org/resources/cobit/cobit-5>
- Information Systems Audit and Control Association. (2014). *Vendor Management: Using COBIT* 5. [https://www.google.co.uk/books/edition/Vendor\\_Management\\_Using\\_COBIT\\_5/M5RiAwAAQBAJ?hl=en&gbpv=1&dq=VENDOR+MANAGEMENT:+USING+COBIT+5&pg=PA9&printsec=frontcover](https://www.google.co.uk/books/edition/Vendor_Management_Using_COBIT_5/M5RiAwAAQBAJ?hl=en&gbpv=1&dq=VENDOR+MANAGEMENT:+USING+COBIT+5&pg=PA9&printsec=frontcover)
- Information Systems Audit and Control Association. (2018a). *COBIT 2019 Framework: Governance and management objectives*. <https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf>

- Information Systems Audit and Control Association. (2018b). *COBIT 2019 Framework: Introduction and methodology*. <https://www.isaca.org/resources/cobit#2>
- Information Systems Audit and Control Association. (2018c). *COBIT 2019 design guide: Designing an information and technology governance solution*. <https://www.isaca.org/resources/cobit#2>
- Information Systems Audit and Control Association. (2019). *CISA review manual* (27th ed.). <https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCbEAK>
- Information Systems Audit and Control Association. (2021). *Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program*. <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx>
- International Organization for Standardization. (2004). *Information technology - Security techniques - Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management*. (ISO/IEC 13335-1:2004). <https://www.iso.org/standard/39066.html>
- International Organization for Standardization. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. (ISO/IEC 27000:2018). <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>
- International Organization for Standardization. (2022a). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. (ISO/IEC 27001:2022). <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>
- International Organization for Standardization. (2022b). *Information security, cybersecurity and privacy protection — Information security controls*. (ISO/IEC 27002:2022). <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en>



- Isola, W. A., & Mesagan, E. P. (2016). Determinants of pharmaceutical industry's performance in Nigeria. *Managing Global Transitions*, 14(3), 267-282. [https://www.fm-kp.si/zalozba/issn/1581-6311/14\\_267-282.pdf](https://www.fm-kp.si/zalozba/issn/1581-6311/14_267-282.pdf)
- IT Governance Institute (ITGI). (2000). *COBIT* (3rd ed.). <https://www.amazon.com/Cobit-Framework-3rd-Edition/dp/1893209148>
- IT Governance Institute (ITGI). (2007). *COBIT 4.1*. [https://www.bauer.uh.edu/parks/cobit\\_4.1.pdf](https://www.bauer.uh.edu/parks/cobit_4.1.pdf)
- Jain, S. K. (2017). Strategy to avoid data integrity issues in pharmaceutical industry. *The Pharma Innovation*, 6(2, Part B), 110-115. <https://www.thepharmajournal.com/archives/2017/vol6issue2/PartB/6-2-6-428.pdf>
- Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, 137, 103611. <https://doi.org/10.1016/j.compind.2022.103611>
- Jarvenpaa S. L., & Ives, B. (1993). Organizing for global competition: The fit of information technology. *Decision Sciences* 24, (3), 547-580. <https://doi.org/10.1111/j.1540-5915.1993.tb01293.x>
- Jiao, J. (2020). Deploying a data security defense. *ISACA Journal*, 4, 1-7. [https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-4/deploying-a-data-security-defense\\_joa\\_eng\\_0720.pdf](https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-4/deploying-a-data-security-defense_joa_eng_0720.pdf)
- Jick, T. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative Science Quarterly*, 24(4), 602-611. <https://doi.org/10.2307/2392366>

- Johansson, K., Paulsson, T., Bergström, E., & Seigerroth, U. (2022). Improving cybersecurity awareness among SMEs in the manufacturing industry. *Advances in Transdisciplinary Engineering*, 21, 209-220. <https://ebooks.iospress.nl/pdf/doi/10.3233/ATDE220140>
- Kamble, S. S., Gunasekaran, A., Ghadge, A., & Raut, R. (2020). A performance measurement system for industry 4.0 enabled smart manufacturing system in SMMEs-A review and empirical investigation. *International journal of production economics*, 229, 107853. <https://doi.org/10.1016/j.ijpe.2020.107853>
- Kamioka, T., Luo, X., & Tapanainen, T. (2016). An empirical investigation of data governance: The role of accountabilities. In *PACIS 2016 Proceedings* (pp. 1-12). <https://aisel.aisnet.org/pacis2016/29>
- Kaplan, R. S., & Norton, D. P. (1996). *The balanced scorecard: Translating strategy into action*. Harvard Business School Press. <https://www.amazon.com/dp/0875846513>
- Katz, P. (2017). *Compliance trends*. Retrieved from <https://www.fda.gov/media/104372/download>
- Kelley, K. B. (2024). The data bare minimum is not enough. *ISACA Journal* 4, 9. <https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2>
- Khan, M. (2016). Managing data protection and cybersecurity-Audit's role. *ISACA Journal*, 1, 1-3. [https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2016/volume-1/managing-data-protection-and-cybersecurity-audit-s-role\\_joa\\_eng\\_0116.pdf](https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2016/volume-1/managing-data-protection-and-cybersecurity-audit-s-role_joa_eng_0116.pdf)
- Khan, M. J. (2018). The methods and costs of data breaches. *ISACA Journal*, 4, 1-5. [https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-3/the-methods-and-costs-of-data-breaches\\_joa\\_eng\\_0618](https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-3/the-methods-and-costs-of-data-breaches_joa_eng_0618)

- Khan, N. A., Saeed, M. R., Hussain, D., Rehan, M., & Dimral, S. R. (2025). Cyber security and privacy safeguarding pharmaceutical innovation in a digital age: Pharmaceutical innovation in a digital age. *Pakistan BioMedical Journal*, 8(4), 2-10. <https://doi.org/10.54393/pbmj.v8i4.1232>
- Khatri, V. (2016). Managerial work in the realm of the digital universe: The role of the data triad. *Business Horizons*, 59, 673-688. <https://doi.org/10.1016/j.bushor.2016.06.001>
- Khatri, V., & Brown, C. V. (2010, January). Designing data governance. *Communications of the ACM*, 53(1), 148-152. <https://doi.org/10.1145/1629175.1629210>
- Kim, H. Y., & Cho, J. S. (2017). Data governance framework for big data implementation with a case of Korea. In *Proceedings of 2017IEEE 6th International Congress on Big Data* (pp. 384-391). <https://doi.org/10.1109/BigDataCongress.2017.56>
- King, N. (2004). Using templates in the thematic analysis of text. In C. Cassell & G. Symon (Eds.), *Essential guide to qualitative methods* (2nd ed., pp. 118–134). Sage Publications. <http://dx.doi.org/10.4135/9781446280119.n21>
- Kirk, J., & Miller, M. L. (1986). *Reliability and validity in qualitative research*. SAGE Publications. <https://doi.org/10.4135/9781412985659>
- Knafil, K.A, & Gallo, A. M, (1995). Triangulation in nursing research. In L. Talbot (Eds.), *Principles and practice of nursing research*. (pp. 492-507). Morsby. [https://archive.org/details/principlespracti0000talb\\_v5t4/page/n5/mode/2up](https://archive.org/details/principlespracti0000talb_v5t4/page/n5/mode/2up)
- Knafl, K., & Breitmayer, B. (1991). Triangulation in qualitative research: Issues of conceptual clarity and purpose. In J. M. Morse (Eds.), *Qualitative nursing research: A contemporary dialogue* (pp. 226-239). Sage Publications. <https://doi.org/10.1046/j.1365-2648.1998.00716.x>
- Kobezak, P., Marchany, R., Raymond, D., & Tront, J. (2018, January). Host inventory controls and systems survey: Evaluating the CIS Critical Security Control One in higher

- education networks. In *Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 4742-4751).  
<https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1661&context=hicss-51>
- Kooper, M., Maes, R., & Lindgreen, E. R. (2011, June). On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*, 31(3), 195-200.  
<https://doi.org/10.1016/j.ijinfomgt.2010.05.009>
- Korac-Kakabadse, N., & Kakabadse, A. (2001). IS/IT governance: Need for an integrated model. *Corporate Governance*, 1(4), 9-11.  
<https://doi.org/10.1108/EUM00000000005974>
- Koutsourelis, D., & Katsikas, S. K. (2014). Designing and developing a free data loss prevention system. In *Proceedings of the 18th Panhellenic Conference on Informatics* (pp. 1-5). ACM. <http://doi.org/10.1145/2645791.2645833>
- Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, 125, 691-697.  
<https://doi.org/10.1016/j.procs.2017.12.089>
- Krauss, S. E. (2005). Research paradigms and meaning making: A primer. *The qualitative report*, 10(4), 758-770. <https://doi.org/10.46743/2160-3715/2005.1831>
- Krippendorff, K. (1980). *Content analysis: An introduction to its methodology*. Sage Publications.  
<https://books.google.com.ng/books?id=q657o3M3C8cC&printsec=frontcover#v=onepage&q&f=false>
- Kvale, S., & Brinkmann, S. (2009). *Interviews. Learning the craft of qualitative research interviewing* (2nd ed.). Sage Publications.

<https://books.google.com.ng/books?id=bZGvwsP1BRwC&printsec=frontcover#v=onepage&q&f=false>

- Lacey, A., & Luff, D. (2009). *Qualitative data analysis: The NIHR research design service for Yorkshire and the Humber*. National Institute for Health Research. [https://www.academia.edu/download/61606002/9\\_Qualitative\\_Data\\_Analysis\\_Revisi\\_on\\_200920191225-129738-301p8i.pdf](https://www.academia.edu/download/61606002/9_Qualitative_Data_Analysis_Revisi_on_200920191225-129738-301p8i.pdf)
- Lacey, A. (2015). The research process. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 15—27). New York, NY: John Wiley & Sons, Incorporated
- Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. *META group research note*, 6(70), 1-4. <https://studylib.net/download/8647594>
- La Pelle, N. (2004). Simplifying qualitative data analysis using general purpose software tools. *Field Methods*, 16(1), 85-108. <https://doi.org/10.1177/1525822X03259227>
- Lathlean, J. (1997). *Lecturer practitioners in action*. Butterworth-Heinemann. <https://www.goodreads.com/book/show/2853500-lecturer-practitioners-in-action>
- Leal, F., Chis, A. E., Caton, S., González-Vélez, H., García-Gómez, J. M., Durá, M., ... Mier, M. (2021). Smart pharmaceutical manufacturing: Ensuring end-to-end traceability and data integrity in medicine production. *Big Data Research*, 24, 1-11. <https://doi.org/10.1016/j.bdr.2020.100172>
- Lee, S.U., Zhu, L., & Jeffery, D.R. (2017). Data governance for platform ecosystems: Critical factors and the state of practice. In *Twenty First Pacific Asia Conference on Information Systems Proceedings* (pp. 1-12). <https://doi.org/10.48550/arXiv.1705.03509>
- Lee, Y., Madnick, S., Wang, R., Wang, F., & Zhang, H. (2014). A cubic framework for the Chief Data Officer: Succeeding in a world of big Data. *MIS Quarterly Executive*, 13(1), 1-13.

[https://dspace.mit.edu/bitstream/handle/1721.1/98915/Madnick\\_A%20cubic.pdf?sequence=1&isAllowed=y](https://dspace.mit.edu/bitstream/handle/1721.1/98915/Madnick_A%20cubic.pdf?sequence=1&isAllowed=y)

Legard, R., Keegan, J., & Ward, K. (2003). In-depth interviews. In J. Ritchie & J. Lewis (Eds.), *Qualitative research practice: A guide for Social Science students and researchers* (pp. 138–169). Sage Publishing.

[https://books.google.co.uk/books/about/Qualitative\\_Research\\_Practice.html?id=e6EO83ZKGYoC&redir\\_esc=y](https://books.google.co.uk/books/about/Qualitative_Research_Practice.html?id=e6EO83ZKGYoC&redir_esc=y)

Lincoln, Y.S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

[https://books.google.co.uk/books/about/Naturalistic\\_Inquiry.html?id=2oA9aWlNeooC](https://books.google.co.uk/books/about/Naturalistic_Inquiry.html?id=2oA9aWlNeooC)

Lincoln, Y., & Guba, E. (1989). *Fourth generation evaluation*. Sage.

[https://books.google.co.uk/books/about/Fourth\\_Generation\\_Evaluation.html?id=k\\_zxEUst46UC&redir\\_esc=y](https://books.google.co.uk/books/about/Fourth_Generation_Evaluation.html?id=k_zxEUst46UC&redir_esc=y)

Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journal*, 20(2), 182-198.

<https://doi.org/10.1108/09565691011064322>

Luftman, J. N. (1996). *Competing in the information age: Strategic alignment in practice*. Oxford University Press.

<https://books.google.com.ng/books?id=LxwjXmR2pIEC&printsec=frontcover#v=onepage&q&f=false>

Maennel, K., Mäses, S., Maennel, O. (2018). Cyber hygiene: The big picture. In N. Gruschka, (Eds.), *Secure IT systems. NordSec 2018. Lecture notes in computer science: Vol. 11252* (pp. 225–240). Springer. [https://doi.org/10.1007/978-3-030-03638-6\\_18](https://doi.org/10.1007/978-3-030-03638-6_18)

Mahrer, A. R. (1988). Discovery-oriented psychotherapy research: Rationale, aims, and methods. *American Psychologist*, 43(9), 694-702. <https://doi.org/10.1037/0003->

[066X.43.9.694](#)

- Major data breach: Sensitive government data of Nigerian citizens available online for just 100 Naira* (2024, June 20). Paradigm Initiative. <https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/>
- Malik, P. (2013). Governing big data: Principles and practices. *IBM Journal of Research and Development*, 57(3/4), 1-13. <https://doi.org/10.1147/JRD.2013.2241359>
- Malik, V. R., Gobinath, K., Khadsare, S., Lakra, A., & Akulwar, S. V. (2021). Security challenges in industry 4.0 SCADA systems—A digital forensic prospective. In *2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)* (pp. 229-233). Yogyakarta, Indonesia. IEEE. <https://doi.org/10.1109/ICAICST53116.2021.9497829>
- Marchionini G., & Teague, J. (1987). Elementary students' use of electronic information services: An exploratory study, *Journal of Research on Computing in Education*, 20, 139–155. <https://doi.org/10.1080/08886504.1987.10781830>
- Mason, J. (2002) *Qualitative researching*, (2nd ed.). Sage. [https://books.google.co.uk/books/about/Qualitative\\_Researching.html?id=gW5su96QHL0C&redir\\_esc=y](https://books.google.co.uk/books/about/Qualitative_Researching.html?id=gW5su96QHL0C&redir_esc=y)
- Mahmoodpour, M., Lobov, A., Lanz, M., Mäkelä, P., & Rundas, N. (2018). Role-based visualization of industrial IoT-based systems. *2018 14th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA)*, 1-8. <https://doi.org/10.1109/MESA.2018.8449183>
- Massacci, F., & Pashchenko, I. (2021). Technical leverage in a software ecosystem: Development opportunities and security risks. *Empirical Software Engineering*, 27(6), 1–26. <https://doi.org/10.48550/arXiv.2103.03317>

- Matney, D., & Larson, D. (2004, Summer). The four components of BI governance. *Business Intelligence Journal*, 9, 29-36. <https://www.proquest.com/magazines/four-components-bi-governance/docview/222639258/se-2?accountid=188730>
- Maxwell, J. (1997). Designing a qualitative study. In L. Bickman & D. J. Rog (Eds.), *Handbook of applied social research methods* (pp. 69-100). Sage Publications. [https://www.researchgate.net/publication/255579877\\_Designing\\_a\\_Qualitative\\_Study/link/00b7d53bd591a421db000000/download](https://www.researchgate.net/publication/255579877_Designing_a_Qualitative_Study/link/00b7d53bd591a421db000000/download)
- Mays, N. (2000). Assessing quality in qualitative research. *British Medical Journal* 320, 50–52. <https://doi.org/10.1136/bmj.320.7226.50>
- Medicines and Healthcare Products Regulatory Agency. (2015). *MHRA GMP data integrity definitions and guidance for industry* (Version 2) [Withdrawn PDF]. Retrieved from [https://assets.publishing.service.gov.uk/media/5ac4a6cc40f0b60a4be86d80/Data\\_integrity\\_definitions\\_and\\_guidance\\_v2\\_Withdrawn.pdf](https://assets.publishing.service.gov.uk/media/5ac4a6cc40f0b60a4be86d80/Data_integrity_definitions_and_guidance_v2_Withdrawn.pdf)
- Medicine security* (n. d.) Americares. <https://www.americares.org/what-we-do/medicine-security/#:~:text=Medicine%20security%20means%20that%20every,a%20goal%20worth%20striving%20for.>
- Members*. (n.d.). PMG-MAN. (2022). <https://pmgman.com/members/>
- Merriam, S. B. (1988). *Case study research in education: A qualitative approach*. Jossey-Bass. <https://www.worldcat.org/title/case-study-research-in-education-a-qualitative-approach/oclc/18049207>
- Merriam, S. B. (1998). *Qualitative research and case study applications in education*. Jossey-Bass. [https://books.google.co.uk/books/about/Qualitative\\_Research\\_and\\_Case\\_Study\\_Approach/html?id=kYMtQgAACAAJ&redir\\_esc=y](https://books.google.co.uk/books/about/Qualitative_Research_and_Case_Study_Approach/html?id=kYMtQgAACAAJ&redir_esc=y)



- Merriam-Webster. (n.d.). Auditing. In *Merriam-Webster.com dictionary*. Retrieved July 12, 2022, from <https://www.merriam-webster.com/dictionary/auditing>
- Meyer, D. Z., & Avery, L. M. (2009). Excel as a qualitative data analysis tool. *Field Methods*, 21(1), 91-112. <https://doi.org/10.1177/1525822X08323985>
- Mikalef, P., Krogstie, J., Van de Wetering, R., Pappas, I. O., & Giannakos, M. N. (2018). Information governance in the big data era: Aligning organizational capabilities. In *Proceedings of the 51<sup>st</sup> Hawaii International Conference on System Sciences* (pp. 4911-4920). <https://doi.org/10.24251/hicss.2018.615>
- Miles, M. B. & Huberman, M. A. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Sage. [https://books.google.co.uk/books/about/Qualitative\\_Data\\_Analysis.html?id=U4IU - wJ5QEC&redir\\_esc=y](https://books.google.co.uk/books/about/Qualitative_Data_Analysis.html?id=U4IU-wJ5QEC&redir_esc=y)
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis* (3rd ed.). Sage Publications. <https://books.google.co.id/books?id=p0wXBAAQBAJ&printsec=frontcover&hl=id#v=onepage&q&f=false>
- Mims, L. C., & Perelman, M. (2021, April 17). *Pharmaceutical trade secrets: Protecting IP*. BioProcess International. <https://www.bioprocessintl.com/intellectual-property/trade-secret-vulnerabilities-recent-hacking-schemes-highlight-the-need-to-protect-proprietary-pharmaceutical-information>
- Moghaddasi, H., Sajjadi, S., & Kamkarhaghighi, M. (2016). Reasons in support of data security and data security management as two independent concepts: a new model. *The Open Medical Informatics Journal*, 10, 4-10. <https://doi.org/10.2174/1874431101610010004>
- Mohanta, A., & Saldanha, A. (2020). *Malware analysis and detection engineering: A comprehensive approach to detect and analyze modern malware* (1st ed.). Apress.

[https://learning.oreilly.com/library/view/malware-analysis-and/9781484261934/html/491809\\_1\\_En\\_3\\_Chapter.xhtml#Sec4](https://learning.oreilly.com/library/view/malware-analysis-and/9781484261934/html/491809_1_En_3_Chapter.xhtml#Sec4)

Morabito, V. (2015). *Big data and analytics: Strategic and organizational impacts*. Springer International Publishing.

[https://books.google.com.ng/books/about/Big\\_Data\\_and\\_Analytics.html?id=9lx0BgAAQBAJ&printsec=frontcover&source=kp\\_read\\_button&hl=en&redir\\_esc=y#v=onepage&q&f=false](https://books.google.com.ng/books/about/Big_Data_and_Analytics.html?id=9lx0BgAAQBAJ&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false)

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods*, 1(2), 13-22. <https://doi.org/10.1177/160940690200100202>

Mosely, M., Brackett, M., Earley, P. S., & Henderson, D. (Eds.). (2009). *The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK Guide)*. Technics Publications.

[https://www.academia.edu/19992490/The\\_DAMA\\_Guide\\_to\\_the\\_Data\\_Management\\_Body\\_of\\_Knowledge\\_First\\_Edition](https://www.academia.edu/19992490/The_DAMA_Guide_to_the_Data_Management_Body_of_Knowledge_First_Edition)

Murphy, E., Dingwall, R., Greatbatch, D., Parker S., & Watson, P. (1998.) Qualitative research methods in health technology assessments: A review of the literature. *Health Technology Assessment* 2(16), 1–274. <https://doi.org/10.3310/hta2160>

NAFDAC. (2022, April 4). *WHO certifies NAFDAC as ML3 Regulatory Authority* [Press release]. <https://nafdac.gov.ng/who-certifies-nafdac-as-ml3-regulatory-authority/>

*NAFDAC Strategic Plan (2018 – 2023)*. (n.d.). NAFDAC. <https://www.nafdac.gov.ng/wp-content/uploads/Files/Resources/APPROVED-NAFDAC-SP-2018-2023.pdf>

Nassaji, H. (2020). Good qualitative research. *Language Teaching Research*, 24(4), 427-431. <https://doi.org/10.1177/1362168820941288>

- National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). Department of Commerce, Washington, D.C. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. <https://doi.org/10.1177/1609406917733847>
- Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, 17-31. <https://doi.org/10.1016/j.adhoc.2015.01.006>
- Nigerian Data Protection Act, No. 37. (2023). [https://ndpc.gov.ng/resources/#flipbook-df\\_2442/7/](https://ndpc.gov.ng/resources/#flipbook-df_2442/7/)
- Nigeria Data Protection Regulation. (2019). <https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf>
- Niemi, E., & Laine, S. (2016). Designing information governance with a focus on competence management in a knowledge-intensive project organization. In *Proceedings of 21st International Conference on Information Quality (ICIQ)* (pp. 1-12). [http://alarcos.esi.uclm.es/iciq2016/documents/camera\\_ready/1-niemi-laine\\_information-governance\\_submitted.pdf](http://alarcos.esi.uclm.es/iciq2016/documents/camera_ready/1-niemi-laine_information-governance_submitted.pdf)
- Notes to industry. (n.d.). NAFDAC. <https://www.nafdac.gov.ng/our-services/notes-to-industry/>
- Nwosu, N. (2023a). *Enhancing data security in smart manufacturing: Evaluating the effectiveness of open-source and commercial data loss prevention solutions in detecting sensitive data at rest* [Unpublished master's dissertation]. Glasgow Caledonian University.

- Nwosu, F. P. (2023b). NAFDAC and its structural defects in Nigeria, 1993-2002. *Akwa Journal of History (AJOH)*, 1(1).  
<https://www.nigerianjournalsonline.com/index.php/AJOH/article/view/3730>
- Nye, J. (2015). Cloud computing: Are your data secure in the Cloud? *ISACA Journal*, 1, 12-15.  
<https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/cloud-computing-are-your-data-secure-in-the-cloud>
- Obukohwo, E. O., Olele, E. H., & Buzugbe, P. N. (2018). Assessing efficiency in the pharmaceutical sector of Nigeria. *CBN Journal of Applied Statistics*, 9(2), 131-148.  
<https://doi.org/10.33429/Cjas.09218.6/6>
- Oguejiofor, B. B., Omotosho, A., Abioye, K. M., Alabi, A. M., Oguntinyinbo, F. N., Daraojimba, A. I., & Daraojimba, C. (2023). A review on data-driven regulatory compliance in Nigeria. *International Journal of Applied Research in Social Sciences*, 5(8), 231-243. <https://fepbl.com/index.php/ijarss/article/view/571/730>
- Ogaji, J. I., Alawode, A. O., & Iranloye, T. A. (2014). Pharmaceutical industry capacity utilization in Nigeria. *African Journal of Pharmacy and Pharmacology*, 8(21), 579-585. <https://doi.org/10.5897/AJPP2014.4029>
- Ojo, T. (2014). *Fidson Healthcare Plc: Pioneering a new vista*. CardinalStone.  
<https://research.cardinalstone.com/reports>
- Okereafor, K., & Adebola, O. (2021). Healthcare cybersecurity lessons from COVID. *International Journal in IT and Engineering*, 9(4), 1-11.  
<https://doi.org/10.6084/m9.figshare.14559969.v1>
- Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers & Security*, 117, 102697.  
<https://doi.org/10.1016/j.cose.2022.102697>
- Olasupo, S., Adeyeye, M., Akinyemi, A., Kayode, J., & Sonny-Afoekelu, U. (2024). Impact of

- digitalization in strengthening the regulatory functions of NAFDAC: Opportunities and challenges for other national regulatory authorities. *Journal of Regulatory Science*, 12(1). <https://regsci-ojs-tamu.tdl.org/regsci/article/view/284>
- Oppermann, M. (2000). Triangulation – A methodological discussion. *International Journal of Tourism Research* 2(2), 141-145. [https://doi.org/10.1002/\(SICI\)1522-1970\(200003/04\)2:2<141::AID-JTR217>3.0.CO;2-U](https://doi.org/10.1002/(SICI)1522-1970(200003/04)2:2<141::AID-JTR217>3.0.CO;2-U)
- Ose, S. O. (2016). Using Excel and Word to structure qualitative data. *Journal of Applied Social Science*, 10(2), 147-162. <https://doi.org/10.1177/1936724416664948>
- Oseni, Y. O. (2019). Evaluation of pharmacy practice regulations in Nigeria: The pharmaceutical inspectors' perspective. *Tropical Journal of Pharmaceutical Research*, 18(6), 1353-1360. <https://doi.org/10.4314/tjpr.v18i6.29>
- Otto, B. (2011a). Data governance. *Business & Information Systems Engineering*, 3(4), 241-244. <https://aisel.aisnet.org/bise/vol3/iss4/6>
- Otto, B. (2011b). Organizing data governance: Findings from the telecommunications industry and consequences for large service providers. *Communications of the Association for Information Systems*, 29(1), 45-66. <https://doi.org/10.17705/1CAIS.02903>
- Otto, B. (2011c). A morphology of the organisation of data governance. In *Proceedings of the 19<sup>th</sup> European Conference on Information Systems (ECIS)* (pp. 1-12). <https://aisel.aisnet.org/ecis2011/272>
- Otto, B. (2012). Managing the business benefits of product data management: The case of Festo. *Journal of Enterprise Information Management*, 25(3), 272-297. <https://doi.org/10.1108/17410391211224426>
- O'Connor, H., Madge, C., Shaw, R., & Wellens, J. (2008). Internet-based interviewing. In N. Fielding, R.M. Lee & G. Blank (Eds), *The Sage Handbook of online research methods* (pp. 271–289). Sage Publications.

[https://books.google.com.ng/books?id=EeMKURpicCgC&printsec=frontcover&source=gbs\\_ge\\_summary\\_r&cad=0#v=onepage&q&f=false](https://books.google.com.ng/books?id=EeMKURpicCgC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)

Palczewska, A., Fu, X., Trundle, P., Yang, L., Neagu, D., Ridley, M., & Travis, K. (2013). Towards model governance in predictive toxicology. *International Journal of Information Management*, 33, 567-582.

<https://doi.org/10.1016/j.ijinfomgt.2013.02.005>

Pashchenko, I., Plate, H., Ponta, S. E., Sabetta, A., & Massacci, F. (2018). Vulnerable open source dependencies: Counting those that matter. *Empirical Software Engineering*, 27(1), 1–33. <https://doi.org/10.48550/arXiv.1808.09753>

Patton, M. Q. (1987). *How to use qualitative methods in evaluation*. Sage Publications. [https://books.google.com.ng/books/about/How to Use Qualitative Methods in Evaluation.html?id=IQ1HAAAAMAAJ&redir\\_esc=y](https://books.google.com.ng/books/about/How_to_Use_Qualitative_Methods_in_Evaluation.html?id=IQ1HAAAAMAAJ&redir_esc=y)

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). Sage Publications. <https://doi.org/10.1002/nur.4770140111>

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage Publications. <https://books.google.com.ng/books?id=FjBw2oi8El4C&printsec=frontcover#v=onepage&q&f=false>

Pearce, G. (2017). Boosting cyber security with data governance and enterprise data management. *ISACA Journal*, 3, 1-6. <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/boosting-cyber-security-with-data-governance-and-enterprise-data-management>

Pearce, G. (2024). Data interoperability: Addressing the challenges placing quality healthcare at risk. *ISACA Journal* 4, 15. <https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2>

- Peterson, R. (2004). Crafting information technology governance. *Information systems management*, 21(4), 7-22. <https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2>
- Peterson, R., Parker, M. M., & Ribbers, P. (2002). Information technology governance processes under environmental dynamism: Investigating competing theories of decision making and knowledge sharing. In *Proceedings of the 23th International Conference on Information Systems* (pp. 562-572). <http://aisel.aisnet.org/icis2002/52>
- Pharmacy Practice*. (n.d.). Pharmacists Council of Nigeria. <https://www.pcn.gov.ng/pharmacy-practice/>
- Pharmaceutical Inspection Co-Operation Scheme. (2019). *PIC/S brochure* [Brochure]. <https://picscheme.org/docview/2146>
- Pharmaceutical Inspection Convention Pharmaceutical Inspection Co-Operation Scheme. (2021, July 1). *Good practices for data management and Integrity in regulated GMP/GDP environments*. <https://picscheme.org/docview/4234>
- Polkinghorne, D. E. (2007). Validity issues in narrative research. *Qualitative inquiry*, 13(4), 471-486. <https://doi.org/10.1177/1077800406297670>
- Ponemon Institute. (n. d.). 2022 *Cost of insider threats: Global report*. Retrieved from <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-uk-tr-the-cost-of-insider-threats-ponemon-report.pdf>
- Poorman, P. B. (2002). Perceptions of thriving by women who have experienced abuse or status-related oppression. *Psychology of Women Quarterly*, 26(1), 51-62. <https://doi.org/10.1111/1471-6402.00043>
- Pope, C., & Ziebland, S., & Mays, N. (2000). Qualitative research in health care: Analysing qualitative data. *British Medical Journal*, 320(7227), 114-116. <https://doi.org/10.1136/bmj.320.7227.114>

- Prasad, M. (2024). Addressing the privacy, security, risk, and operations of the data ecosystem. *ISACA Journal* 4, 35. <https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2>
- Pujeri, U., Shamla Mantri, D. H. P., & Gupta, P. (2023). Data loss prevention techniques. *European Chemical Bulletin*, 12(3), 5054-5060. <https://www.eurchembull.com/uploads/paper/b5d0433ee5f46b21da56c4a1d3ceb810.pdf>
- Putrus, R. (2017). A risk-based management approach to third-party data security, risk and compliance. *ISACA Journal*, 6, 33-41. [https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2017/volume-6/a-risk-based-management-approach\\_joa\\_eng\\_1117.pdf](https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2017/volume-6/a-risk-based-management-approach_joa_eng_1117.pdf)
- PricewaterhouseCoopers. (2016). *Turnaround and transformation in cybersecurity: Pharmaceuticals and life sciences*. Retrieved from <https://www.pwc.com/gx/en/consultingservices/information-security-survey/assets/2016-pharmaceuticals.pdf>
- Rahman, M. H., Wuest, T., & Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. *Journal of Manufacturing Systems*, 68, 196-208. <https://doi.org/10.1016/j.jmsy.2023.03.009>
- Rahul, K., & Banyal, R. K. (2020). Data life cycle management in big data analytics. *Procedia Computer Science*, 173, 364-371. <https://doi.org/10.1016/j.procs.2020.06.042>
- Rasouli, M. R., Trienekens, J. J., Kusters, R. J., & Grefen, P. W. (2016c). Information governance requirements in dynamic business networking. *Industrial Management & Data Systems*, 116(7), 1356-1379. <https://doi.org/10.1108/IMDS-06-2015-0260>
- Regulations*. (n.d.). NITDA. <https://nitda.gov.ng/regulations/>



- Rice, P., & Ezzy, D. (1999). *Qualitative research methods: A health focus*. Oxford University Press. [https://www.researchgate.net/profile/William-Pickett/publication/12246119\\_Estimation\\_of\\_youth\\_smoking\\_behaviours\\_in\\_Canada/links/5494e07b0cf29b94482102c5/Estimation-of-youth-smoking-behaviours-in-Canada.pdf#page=47](https://www.researchgate.net/profile/William-Pickett/publication/12246119_Estimation_of_youth_smoking_behaviours_in_Canada/links/5494e07b0cf29b94482102c5/Estimation-of-youth-smoking-behaviours-in-Canada.pdf#page=47)
- Ritchie, J., & Lewis, J. (2003). *Qualitative research practice: A guide for social science students and researchers*. Sage Publications. [https://books.google.com.ng/books/about/Qualitative\\_Research\\_Practice.html?id=CHhMorWjDv0C&printsec=frontcover&source=kp\\_read\\_button&hl=en&redir\\_esc=y#v=onepage&q&f=false](https://books.google.com.ng/books/about/Qualitative_Research_Practice.html?id=CHhMorWjDv0C&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false)
- Richie, J. & Spencer, L. (1994). Qualitative data analysis for applied policy research. In A. Bryman & B. Burgess (Eds.), *Analysing qualitative data* (1st ed., pp.173-194). Routledge. <https://doi.org/10.4324/9780203413081>
- Rifaie, M., Alhajj, R., & Ridley, M. (2009, December). Data governance strategy: A key issue in building enterprise data warehouse. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services* (pp. 587-591). <https://doi.org/10.1145/1806338.1806449>
- Roberts, S. J. (2014). The necessity of information security in the vulnerable pharmaceutical industry. *Journal of Information Security*, 5(4), 147-153. <https://doi.org/10.4236/jis.2014.54014>
- Robertson, A. S., Malone, H., Bisordi, F., Fitton, H., Garner, C., Holdsworth, S., Honig, P., .... Wegner, M. (2020). Cloud-based data systems in drug regulation: An industry perspective. *Nature Reviews Drug Discovery*, 19(6), 365-366. <https://doi.org/10.1038/d41573-019-00193-7>
- Robson, C. (2011). *Real world research* (3rd ed.). Blackwell. <https://www.wiley.com/en->

lk/Real+World+Research,+3rd+Edition-p-9781405182416

- Rossman, G. B. & Wilson, B. L. (1985). Numbers and words: Combining quantitative and qualitative methods in a single large-scale evaluation study. *Evaluation Review*, 9(5), 627–643. <https://doi.org/10.1177/0193841X8500900505>
- Rowley, J. (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science*, 33(2), 163–180. <https://doi.org/10.1177/0165551506070706>
- Rubin, H. J, & Rubin, I. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). Sage Publications. <https://us.sagepub.com/en-us/nam/qualitative-interviewing/book234196#contents>
- Rust-Nguyen, N., Sharma, S., & Stamp, M. (2023). Darknet traffic classification and adversarial attacks using machine learning. *Computers & Security*, 127, 103098. <https://doi.org/10.1016/j.cose.2023.103098>
- Ryan, G. W. (2004). Using a Word Processor to Tag and Retrieve Blocks of Text. *Field Methods*, 16(1), 109-130. <https://doi.org/10.1177/1525822X03261269>
- Saa, P., Costales, A. C., Moscoso-Zea, O., & Luján-Mora, S. (2017). Moving ERP systems to the Cloud-Data security issues. *Journal of Information Systems Engineering and Management*, 2(4), 21. <https://doi.org/10.20897/jisem.201721>
- Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: Global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, 5(5), 67-81. <https://www.proquest.com/scholarly-journals/national-cyber-security-strategies-global-trends/docview/1868264400/se-2?accountid=188730>
- Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C*. John Wiley & Sons. [https://books.google.co.uk/books/about/Applied\\_Cryptography.html?id=01vfjgEACA&redir\\_esc=y](https://books.google.co.uk/books/about/Applied_Cryptography.html?id=01vfjgEACA&redir_esc=y)

- Saez, M., Maturana, F. P., Barton, K., & Tilbury, D. M. (2018). Real-time manufacturing machine and system performance monitoring using internet of things. *IEEE Transactions on Automation Science and Engineering*, 15(4), 1735-1748. <https://ieeexplore.ieee.org/ielam/8856/8481716/8283835-aam.pdf>
- Sagonowsky, E. (2021, Nov 24). *Pfizer says former employee stole trade secrets on megablockbuster COVID-19 vaccine*. Fierce Pharma. <https://www.fiercepharma.com/pharma/pfizer-says-former-employee-stole-trade-secrets-megablockbuster-covid-19-vaccine>
- Sai, N. R., & Kumar, G. S. C. (2021). An approach to secured cloud data storage with industrial IoT. *International Research Journal of Modernization in Engineering Technology and Science*, 3(8), 956-964. [https://www.academia.edu/download/69189464/fin\\_irjmets1630224746.pdf](https://www.academia.edu/download/69189464/fin_irjmets1630224746.pdf).
- Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly*, 23(2), 261–290. <https://doi.org/10.2307/249754>
- Sample DPIA Template*. (n.d.). GDPR.eu. <https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf>
- Schwandt, T. (1997). *Qualitative inquiry: A dictionary of terms*. Sage. [https://books.google.co.uk/books/about/Qualitative\\_Inquiry.html?id=6jrAAAAMAAJ&redir\\_esc=y](https://books.google.co.uk/books/about/Qualitative_Inquiry.html?id=6jrAAAAMAAJ&redir_esc=y)
- Scott, J. (1999). The FoxMeyer Drugs' bankruptcy: Was it a failure of ERP? In *AMCIS 1999 Proceedings* (pp. 223-225). <https://aisel.aisnet.org/amcis1999/80>
- Scott, J. E., & Vessey, I. (2002). Managing risks in enterprise systems implementations. *Communications of the ACM*, 5(4), 74-81. <https://doi.org/10.1145/505248.505249>

- Scott, J. E. (2003). FoxMeyer Case: A failure of large ERP implementation. *European Journal of Operation Research*, 146(3), 241-257.  
[https://www.academia.edu/4823665/FOXMEYER\\_CASE\\_A\\_FAILURE\\_OF\\_LARGE\\_ERP\\_IMPLEMENTATION](https://www.academia.edu/4823665/FOXMEYER_CASE_A_FAILURE_OF_LARGE_ERP_IMPLEMENTATION)
- Senyo, P. K., Liu, K., & Effah, J. (2019). Digital business ecosystem: Literature review and a framework for future research. *International Journal of Information Management*, 47, 52-64. <https://doi.org/10.1016/j.ijinfomgt.2019.01.002>
- SFIA 8 Summary Chart. (n.d.). SFIA. <https://sfia-online.org/en/sfia-8/documentation>
- Shawa, L. (2017). Ethics in Educational Research. In L. Ramrathan, L. Le Grange, & P. Higgs (Eds.), *Education studies for initial teacher development* (pp. 432–443). Juta Legal and Academic Publishers.  
[https://www.researchgate.net/publication/312069857\\_Ethics\\_in\\_educational\\_research](https://www.researchgate.net/publication/312069857_Ethics_in_educational_research)
- Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, 22, 63-75. <https://doi.org/10.3233/EFI-2004-22201>
- Shou, Y., Sellbom, M., & Chen, H. (2022). Fundamentals of measurement in Clinical Psychology. In G. Asmundson (Eds.), *Comprehensive Clinical Psychology* (2nd ed., 13-35). <https://doi.org/10.1016/B978-0-12-818697-8.00110-2>
- Significant changes to DAMA-DMBOK2 revised edition. (n.d.). DAMA INTERNATIONAL.  
<https://www.dama.org/cpages/changes-to-dama-dmbok-2>
- Sihotang, H. T., Zarlis, M., Efendi, S., & Jollyta, D. (2019, August). Evaluation of maturity level of information and communication technology (ICT) governance with CobIT 5.0 case study: STMIK Pelita Nusantara Medan. *Journal of Physics: Conference Series*, 1255(1), 1-6. <https://doi.org/10.1088/1742-6596/1255/1/012046>
- Simons, R. (1990). The role of management control systems in creating competitive advantage:

- New perspectives. *Accounting, Organizations and Society*, 15 (1/2), 127-143.  
[https://doi.org/10.1016/0361-3682\(90\)90018-P](https://doi.org/10.1016/0361-3682(90)90018-P)
- Simons, R. (2000). *Performance measurement and control systems for implementing strategy*. Prentice Hall. <https://www.hbs.edu/faculty/Pages/item.aspx?num=256>
- Smith, J., & Firth, J. (2011). Qualitative data analysis: The framework approach. *Nurse Researcher*, 18(2), 52-62. <https://doi.org/10.7748/nr2011.01.18.2.52.c8284>
- Sohan, M. F. A. A., Khan, S. R., Anannya, N. J., & Ahad, M. T. (2022). Towards a secured smart IoT using light weight blockchain: An aim to secure Pharmacy Products. arXiv. <https://arxiv.org/pdf/2206.06925>
- Souza, C. (2018, Nov 15). *What has pharma learned from the Merck cyber attack*. PharmaExec.com. <https://www.pharmexec.com/view/what-has-pharma-learned-merck-cyber-attack>
- Spooner, D., Silowash, G., Costa, D., & Albrethsen, M. (2018, May). Navigating the insider threat tool landscape: Low cost technical solutions to jump start an insider threat program. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 247-257). IEEE. <https://doi.org/10.1109/SPW.2018.00040>
- Stolfo, S. J. (2019). Cost of a data breach: Time to detection saves real money. *ISACA Journal*, 1, 1-4. <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/cost-of-a-data-breach-time-to-detection-saves-real-money>
- Soares, S. (2013). *IBM InfoSphere: A platform for big data governance and process data governance* (1st ed.). MC Press. <https://idoc.pub/documents/ibm-infosphere-a-platform-for-big-data-governance-and-process-data-governance-pon2ep1gv3n0>
- Sprake, A., & Palmer, C. A. (2022). Understanding the interpretive paradigm: a guide for sports students learning through qualitative research. *Journal of Qualitative Research in Sports Studies*, 16(1), 45-68. <https://clouk.uclan.ac.uk/48569/>

- Stake, R. E. (1995). *The art of case study research*. Sage Publications.  
[https://books.google.com.ng/books?id=ApGdBx76b9kC&printsec=frontcover&redir\\_esc=y#v=onepage&q&f=false](https://books.google.com.ng/books?id=ApGdBx76b9kC&printsec=frontcover&redir_esc=y#v=onepage&q&f=false)
- Stamp, M. (2011). *Information security: Principles and practice*. John Wiley & Sons.  
<https://books.google.co.uk/books?id=P1BDEAAAQBAJ&printsec=frontcover#v=onepage&q&f=false>
- Stemler, S. (2000). An overview of content analysis. *Practical Assessment, Research & Evaluation*, 7(17), 1-6. <https://doi.org/10.7275/z6fm-2e34>
- Stemler, S., & Bebell, D. (1998). *An empirical approach to understanding and analyzing the mission statements of selected educational institutions* [Conference presentation]. Annual Conference of the New England Educational Research Organization (NEERO), Portsmouth, New Hampshire. <https://files.eric.ed.gov/fulltext/ED442202.pdf>
- Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. (2nd ed.). Sage Publications.  
[https://resv.hums.ac.ir/uploads/22\\_288\\_57\\_1qualitative.pdf](https://resv.hums.ac.ir/uploads/22_288_57_1qualitative.pdf)
- Strengtholt, P. (2020). *Data Management at scale* (2nd ed.). O'Reilly Media.  
[https://www.oreilly.com/library/view/data-management-at/9781098138851/?\\_gl=1\\*9py8yp\\*\\_ga\\*ODk2MzI4MTY4LjE3MTMyMDI0MTY.\\*\\_ga\\_092EL089CH\\*MTcxMzU0ODI5My4xMC4xLjE3MTM1NTA3NzEuNjAuMC4w](https://www.oreilly.com/library/view/data-management-at/9781098138851/?_gl=1*9py8yp*_ga*ODk2MzI4MTY4LjE3MTMyMDI0MTY.*_ga_092EL089CH*MTcxMzU0ODI5My4xMC4xLjE3MTM1NTA3NzEuNjAuMC4w)
- Strewig, F., & Stead, G. (2001). *Planning, reporting and designing research*. Pearson.  
<https://books.google.com.ng/books?id=XgO6yEj6xqAC&printsec=frontcover#v=onepage&q&f=false>

*Substandard and falsified medical products*. (2018, January 31). World Health Organization.

<https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>

Sukiasyan, A., Badikyan, H., Pedrosa, T., & Leitao, P. (2022). Secure data exchange in Industrial Internet of Things. *Neurocomputing*, 484, 183-195.  
<https://doi.org/10.1016/j.neucom.2021.07.101>

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, 10(7), 190903.  
<https://doi.org/10.1155/2014/190903>

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal*, 11, 63-75. <https://doi.org/10.3316/QRJ1102063>

Susilowati, M., Kurniawan, Y., Prasetya, H. P., Beatrix, R., Dewa, W. A., & Ahsan, M. (2021). How to manage scope, time and cost of project management plan to develop manufacture information system. *IOP Conference Series: Materials Science and Engineering*, 1098(6), 1-5. <https://doi.org/10.1088/1757-899X/1098/6/062006>

Tabersky, D., Woelfle, M., Ruess, J. A., Brem, S., & Brombacher, S. (2018). Recent regulatory trends in pharmaceutical manufacturing and their impact on the industry. *CHIMIA International Journal for Chemistry*, 72(3), 146-150.  
<https://doi.org/10.2533/chimia.2018.146>

Tallon, P. P. (2013). Corporate governance of big data: Perspectives on value, risk, and cost. *Computer*, 26(6), 32-38. <https://doi.org/10.1109/MC.2013.155>

Tallon, P. P., Ramirez, R. V., & Short, J. E. (2014). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, 30(3), 141-178. <https://doi.org/10.2753/MIS0742-1222300306>

- Tallon, P. P., Short, J. E., & Harkins, M. W. (2013). The evolution of information governance at Intel. *MIS Quarterly Executive*, 12(4), 189-198.  
<https://aisel.aisnet.org/misqe/vol12/iss4/5>
- Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of Manufacturing Systems*, 48, 157-169. <https://doi.org/10.1016/j.jmsy.2018.01.006>
- Tarozzi, M. (2020). *What is grounded theory?* Bloomsbury publishing.  
[https://books.google.co.uk/books?hl=en&lr=&id=-kTqDwAAQBAJ&oi=fnd&pg=PR3&dq=grounded+theory+presupposes+that+no+hypothesis+or+theoretical+framework+exists+prior+to+data+collection&ots=-iIxj4Uo\\_N&sig=INMNdrVOIa2SdwS\\_6d3yg\\_HvgJQ&redir\\_esc=y#v=onepage&q&f=false](https://books.google.co.uk/books?hl=en&lr=&id=-kTqDwAAQBAJ&oi=fnd&pg=PR3&dq=grounded+theory+presupposes+that+no+hypothesis+or+theoretical+framework+exists+prior+to+data+collection&ots=-iIxj4Uo_N&sig=INMNdrVOIa2SdwS_6d3yg_HvgJQ&redir_esc=y#v=onepage&q&f=false)
- Tashakkori, A., & Teddlie, C. (Eds.). (2003). *Handbook of mixed methods in social & behavioral research*. Sage Publications.  
<https://books.google.com.ng/books?id=F8BFOM8DCKoC&printsec=frontcover#v=onepage&q&f=false>
- Teddlie, C., & Yu, F. (2007). Mixed methods sampling: A typology with examples. *Journal of mixed methods research*, 1(1), 77-100. <https://doi.org/10.1177/1558689806292430>
- Template for data protection impact assessment (DPIA). (n.d.). iapp.  
<https://www.icrc.org/en/download/file/18149/dpia-template.pdf>
- Thomas, G. (2006a). *Alpha males and data disasters: The case for data governance*. Brass Cannon Press.  
[https://books.google.com.ng/books/about/Alpha\\_Males\\_and\\_Data\\_Disasters.html?id=3pm8MAAACA AJ&redir\\_esc=y](https://books.google.com.ng/books/about/Alpha_Males_and_Data_Disasters.html?id=3pm8MAAACA AJ&redir_esc=y)
- Thomas, G. (2006b). *The DGI Data Governance Framework*. The Data Governance Institute.  
[https://www.datasqlvisionary.com/wp-content/uploads/2018/06/dgi\\_framework.pdf](https://www.datasqlvisionary.com/wp-content/uploads/2018/06/dgi_framework.pdf)



- Thombre, S. (2020). Freeware solution for preventing data leakage by insider for Windows framework. In *2020 International Conference on Computational Performance Evaluation (ComPE)* (pp. 044-047). IEEE.  
<https://doi.org/10.1109/ComPE49325.2020.9200160>
- Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly*, 32, 316-322. <https://doi.org/10.1016/j.giq.2015.05.001>
- Thorp, J. (2003). *The information paradox*. McGraw-Hill Ryerson.  
[https://openlibrary.org/books/OL32107984M/The\\_information\\_paradox](https://openlibrary.org/books/OL32107984M/The_information_paradox)
- Thurmond, V. A. (2001). The point of triangulation. *Journal of Nursing Scholarship*, 33(3), 253-258. <https://doi.org/10.1111/j.1547-5069.2001.00253.x>
- Tiwana, A., Konsynski, B., & Venkatraman, N. (2014). Special issue: Information technology and organizational governance: The IT governance cube. *Journal of Management Information Systems*, 30(3), 7-12. <http://www.jstor.org/stable/43590140>
- Tod, A. (2015). Interviewing. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 225-235). John Wiley & Sons.  
<https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=409>
- Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): A 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care*, 19(6), 349-357.  
<https://doi.org/10.1093/intqhc/mzm042>
- Topping, A. (2015). The Quantitative–Qualitative Continuum. In K. Gerrish & J. Lathlean (Eds.), *The research process in nursing* (pp. 159-172). John Wiley & Sons.  
<https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1936761&ppg=>

- Tracy, S. J. (2013). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. Wiley-Blackwell.  
[https://edisciplinas.usp.br/pluginfile.php/5569087/mod\\_folder/content/0/Textos/Tracy%2C%20Qualitative%20Research%20Methods-%20Collecting%20Evidence%2C%20Crafting%20Analysis%2C%20Communicating%20Impact.pdf?forcedownload=1](https://edisciplinas.usp.br/pluginfile.php/5569087/mod_folder/content/0/Textos/Tracy%2C%20Qualitative%20Research%20Methods-%20Collecting%20Evidence%2C%20Crafting%20Analysis%2C%20Communicating%20Impact.pdf?forcedownload=1)
- Treacy, C., & McCaffery, F. (2016). Data security overview for medical mobile apps. *International Journal on Advances in Security*, 9, 146-157.  
[http://www.iariajournals.org/security/sec\\_v9\\_n34\\_2016\\_paged.pdf](http://www.iariajournals.org/security/sec_v9_n34_2016_paged.pdf)
- TriRx success story. (n.d.). Navigator Business Solutions. <https://www.nbs-us.com/case-studies/sap-bydesign-case-study-trirx-pharmaceutical-services>
- Tunji, S. (n.d.). NDPC investigating 17 major cases of data breaches in Nigeria, earns N400 million. Nairametrics. <https://nairametrics.com/2024/01/29/ndpc-investigating-17-major-cases-of-data-breach-in-nigeria-earns-n400-million/>
- Turner, S. (2023, June 5). *Cybersecurity in pharma: Securing the future*. Pharmaceutical Technology. <https://www.pharmaceutical-technology.com/features/cybersecurity-in-pharma-securing-the-future/?cf-view>
- Turab, N., & Kharma, Q. (2019). Secure Medical Internet of Things Framework based on Parkerian Hexad Model. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 10(6). 54-62. <https://doi.org/10.14569/IJACSA.2019.0100608>
- Udo Udoma & Belo-Osagie (2023, September 29). *Data breaches: Compliance obligations under the Nigerian Data Protection Act 2023*. MONDAQ. <https://www.mondaq.com/nigeria/data-protection/1371660/data-breaches-compliance-obligations-under-the-nigerian-data-protection-act-2023>

- Urbinati, A., Chiaroni, D., Chiesa, V., & Frattini, F. (2020). The role of digital technologies in open innovation processes: an exploratory multiple case study analysis. *R&D Management*, 50(1), 136-160. <https://doi.org/10.1111/radm.12313>
- Urciuoli, L., Mannisto, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security - potential threat. *Information & Security*, 29(1), 51-68. <https://search.proquest.com/docview/1398483200?accountid=188730>
- U.S. Food and Drug Administration. (2003, August). *Guidance for industry: Part 11, electronic records; electronic signatures—scope and application* (Guidance Document No. 75414). U.S. Department of Health and Human Services. Retrieved from <https://www.fda.gov/media/75414/download>
- U. S. Food and Drug Administration. (2018). *Data integrity and compliance with drug CGMP: Questions and answers; Guidance for industry*. [https://www.gmp-compliance.org/files/guidemgr/7883441\\_DataIntegrity.pdf](https://www.gmp-compliance.org/files/guidemgr/7883441_DataIntegrity.pdf)
- Van Grembergen, W. (2001). Introduction to the Minitrack: IT Governance and its mechanisms. In *Proceedings of the 35<sup>th</sup> Hawaii International Conference on System Sciences (HICSS)* (pp. 3097-3097). <https://doi.org/10.1109/HICSS.2002.994349>
- Van Grembergen, W., De Haes, S., & Guldentops, E. (2003a). Structures, processes and relational mechanisms for IT governance. In W. Van Grembergen (Eds.), *Strategies for information technology governance*. Idea Group Publishing. <https://doi.org/10.4018/978-1-59140-140-7.CH001>
- Van Grembergen, W., Saull, R., & De Haes, S. J. (2003b). Linking the IT balanced scorecard to the business objectives at a major Canadian financial group. *Journal for Information Technology Case and Application Research*, 5(1), 23-50. <https://doi.org/10.1080/15228053.2003.10856015>

- Van Grembergen, W., & De Haes, S. (2009). *Enterprise governance of information technology: achieving strategic alignment and value*. Springer.  
<https://books.google.com.ng/books?id=zNgRBwAAQBAJ&printsec=frontcover#v=onepage&q&f=false>
- Van Stone, M., & Halpert, B. (2018). Mistakes happen: Mitigating unintentional data loss. *ISACA Journal*, 1, 23-29. <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/mistakes-happenmitigating-unintentional-data-loss>
- Venkatesh, V. (2018). Design of cybersecurity risk assessment tool for small and medium sized businesses using the NIST Cybersecurity Framework. In 2018 KSU Proceedings on Cybersecurity Education, Research and Practice (pp. 1-10).  
[https://www.researchgate.net/profile/Vishnu-Venkatesh-2/publication/328410028\\_Design\\_of\\_Cybersecurity\\_Risk\\_Assessment\\_Tool\\_for\\_Small\\_and\\_Medium\\_Sized\\_Businesses\\_using\\_the\\_NIST\\_Cybersecurity\\_Framework/links/5d25e774299bf1547ca7c2ba/Design-of-Cybersecurity-Risk-Assessment-Tool-for-Small-and-Medium-Sized-Businesses-using-the-NIST-Cybersecurity-Framework.pdf](https://www.researchgate.net/profile/Vishnu-Venkatesh-2/publication/328410028_Design_of_Cybersecurity_Risk_Assessment_Tool_for_Small_and_Medium_Sized_Businesses_using_the_NIST_Cybersecurity_Framework/links/5d25e774299bf1547ca7c2ba/Design-of-Cybersecurity-Risk-Assessment-Tool-for-Small-and-Medium-Sized-Businesses-using-the-NIST-Cybersecurity-Framework.pdf)
- Venkatraman, N., Henderson, J. C., & Oldach, S. (1993). Continuous strategic alignment: Exploiting information technology capabilities for competitive success. *European Management Journal*, 11(2), 139-149. [https://doi.org/10.1016/0263-2373\(93\)90037-I](https://doi.org/10.1016/0263-2373(93)90037-I)
- Verizon (n. d.). 2022 Data breach investigations report. Retrieved from <https://www.verizon.com/business/en-gb/resources/reports/dbir/2022/dbir-report/>
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.  
<https://doi.org/10.1016/j.cose.2013.04.004>

- Vu, T. T. N. (2021). Understanding validity and reliability from qualitative and quantitative research traditions. *VNU Journal of Foreign Studies*, 37(3).  
<https://doi.org/10.25073/2525-2445/vnufs.4672>
- Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, 62, 100415.  
<https://doi.org/10.1016/j.ijlcj.2020.100415>
- Waters, M., Waszczuk, P., Ayre, R., Dreze, A., McGlinchey, D., Alkali, B., & Morison, G. (2022). Open source IIoT solution for gas waste monitoring in smart factory. *Sensors*, 22(8), 2972. <https://doi.org/10.3390/s22082972>
- Watson, H. J., Fuller, C., & Ariyachandra, T. (2004). Data warehouse governance: Best practices at Blue Cross and Blue Shield of North Carolina. *Decision Support Systems*, 38, 435-450. <https://doi.org/10.1016/j.dss.2003.06.001>
- Waziri, K. M. (2020). Intellectual property piracy and counterfeiting in Nigeria: The impending economic and social conundrum. *Bayero Journal of Interdisciplinary Studies*, 3(1), 55–68. <https://doi.org/10.5539/jpl.v4n2p196>
- Weber, R. P. (1990). *Basic content analysis* (2nd ed.). Sage Publications.  
<https://dx.doi.org/10.4135/9781412983488>
- Weber, K., Otto, B., & Österle, H. (2009). One size does not fit all-A contingency approach to data governance. *Journal of Data and Information Quality*, 1(1), 1-27.  
<https://doi.org/10.1145/1515693.1515696>
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a Literature Review. *MIS Quarterly*, 26(2), xiii-xxiii.  
[https://web.njit.edu/~egan/Writing\\_A\\_Literature\\_Review.pdf](https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf)
- Weill, P. (1990). Strategic investment in information technology: An empirical study. *Information Age*, 12(3), 141-147. <https://dl.acm.org/doi/10.5555/81240.81242>

- Weill, P. (1992). The relationship between investment in information technology and firm performance: A study of the value-manufacturing sector. *Information Systems Research*, 3(4), 307-333. <https://doi.org/10.1287/ISRE.3.4.307>
- Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive*, 3(1), 1-17. <https://aisel.aisnet.org/misqe/vol3/iss1/3>
- Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press. <https://books.google.com.ng/books?id=xI5KdR21QTAC&printsec=frontcover#v=onepage&q&f=false>
- Weill, P., & Ross, J. (2005). A matrixed approach to designing IT governance. *MIT Sloan Management Review*, 46(2), 25-34. [https://sloanreview.mit.edu/article/a-matrixed-approach-to-designing-it-governance/?switch\\_view=PDF](https://sloanreview.mit.edu/article/a-matrixed-approach-to-designing-it-governance/?switch_view=PDF)
- Weill, P., & Ross, J. W. (2009). *IT savvy: What top executives must know to go from pain to gain*. Harvard Business School Press. <https://books.google.com.ng/books?id=4psb688KSskC&printsec=frontcover#v=onepage&q&f=false>
- Weller, A. (2008). Data governance: Supporting datacentric risk management. *Journal of Securities Operations & Custody*, 1(3), 250-262. <https://hstalks.com/article/873/data-governance-supporting-datacentric-risk-manage/?business&noaccess=1>
- Welsh, E. (2002). Dealing with data: Using NVivo in the qualitative data analysis process. *Forum: Qualitative Social Research*, 3(2). <https://doi.org/10.17169/fqs-3.2.865>
- Wende, K. (2007). A model for data governance – Organising accountabilities for data quality management. In *ACIS 2007 Proceedings* (pp. 416-425). <https://aisel.aisnet.org/acis2007/80>

- Wende, K., & Otto, B. (2007). A contingency approach to data governance. In M. A. Robert, R. O'Hare, L. M. Markus, & B. Klein (Eds.), *Proceedings of 12th International Conference on Information Quality* (pp. 1-14).  
<https://www.alexandria.unisg.ch/213308/1/ICIQ%2520FP%2520Data%2520Governance%2520Contingency%252002%2520kwe.pdf>
- Were, V., & Moturi, C. (2017). Toward a data governance model for the Kenya health professional regulatory authorities. *The TQM Journal*, 29(4), 579-589.  
<https://doi.org/10.1108/TQM-10-2016-0092>
- WHO Global Benchmarking & Quality Management Program. (n.d.). NAFDAC.  
<https://nafdac.gov.ng/about-nafdac/nafdac-programs/who-global-benchmarking-quality-management-program/>
- Wild, P. J., McMahon, C., Darlington, M., Liu, S., & Culley, S. (2009). *A diary study of information needs and document usage in the engineering domain*. Design Studies.  
<http://dx.doi.org/10.1016/j.destud.2009.06.002>
- Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, 24(2), 107-146.  
<https://doi.org/10.2308/jis.2010.24.2.107>
- Winter, J. S., & Davidson, E. (2018). Big data governance of personal health information and challenges to contextual integrity. *The Information Society*, 35(1), 36-51.  
<https://doi.org/10.1080/01972243.2018.1542648>
- Wlosinski, L. G. (2018). Data loss prevention—Next steps. *ISACA Journal* 1, 1-11.  
<https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/data-loss-preventionnext-steps>

- World Health Organization. (2006). *WHO Technical Report Series, No. 937: Supplementary guidelines on good manufacturing practices: Validation (Annex 4)* [PDF]. Author.  
[https://apps.who.int/iris/bitstream/handle/10665/43443/WHO\\_TRS\\_937\\_eng.pdf](https://apps.who.int/iris/bitstream/handle/10665/43443/WHO_TRS_937_eng.pdf)
- World Health Organization. (2014). WHO prequalification: Building quality-assured manufacturing capacity in Nigeria. *WHO Drug Information*, 28(4), 425-430. <https://apps.who.int/iris/handle/10665/331090>
- World Health Organization. (2016). *Guidance on good data and record management practices*. (WHO TRS 996: Annex 5). [https://www.gmp-compliance.org/files/guidemgr/WHO\\_TRS\\_996\\_annex05.pdf](https://www.gmp-compliance.org/files/guidemgr/WHO_TRS_996_annex05.pdf)
- World Health Organization. (2021). *Guidance on data integrity*. (WHO TRS 1033: Annex 4). <https://www.who.int/publications/i/item/55th-report-of-the-who-expert-committee-on-specifications-for-pharmaceutical-preparations>
- Xu, K., Li, Y., Liu, C., Liu, X., Hao, X., Gao, J., & Maropoulos, P. G. (2020). Advanced data collection and analysis in data-driven manufacturing process. *Chinese Journal of Mechanical Engineering*, 33, 1-21. <https://doi.org/10.1186/s10033-020-00459-x>
- Yin, R. K. (1994). *Case study research: Design and methods* (2nd ed.). Sage Publications.  
[https://books.google.com.ng/books/about/Case\\_Study\\_Research.html?id=AvYOAQAAMAAJ&redir\\_esc=y](https://books.google.com.ng/books/about/Case_Study_Research.html?id=AvYOAQAAMAAJ&redir_esc=y)
- Yin, R. K. (2003). *Case study research: Design and methods* (4th ed.). Sage Publications.  
[https://books.google.co.uk/books?id=BWea\\_9ZGQMwC&printsec=frontcover#v=onepage&q&f=false](https://books.google.co.uk/books?id=BWea_9ZGQMwC&printsec=frontcover#v=onepage&q&f=false)
- Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Sage Publications.  
[https://books.google.com.ng/books/about/Case\\_Study\\_Research.html?id=Cdk5DQAQBAJ&redir\\_esc=y](https://books.google.com.ng/books/about/Case_Study_Research.html?id=Cdk5DQAQBAJ&redir_esc=y)



- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications. <https://uk.sagepub.com/en-gb/eur/case-study-research-and-applications/book250150>
- Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, 27(1), 13–15. <https://doi.org/10.4314/mmj.v27i1.4>
- Zhao, D., & Gao, Y. (2024). Information security and privacy protection strategies in the process of electronic archiving. *Journal of Electrical Systems*, 20(6s), 374-380. [https://media.proquest.com/media/hms/PFT/1/Fje1Z?\\_s=PuviwHLdUYgbjp0vQeJmas28rKs%3D](https://media.proquest.com/media/hms/PFT/1/Fje1Z?_s=PuviwHLdUYgbjp0vQeJmas28rKs%3D)

## APPENDICES

### Appendix A: Questionnaire Template for Demographic Information

Please complete all questions and make sure you follow the instructions for each question.

1. **What gender do you identify as? Choose one option.**
  - A. Male
  - B. Female
  - C. Prefer not to answer
  
2. **What is your age? Choose one option.**
  - A. Below 20
  - B. 21-30
  - C. 31-40
  - D. 41-50
  - E. Above 50
  - D. Prefer not to answer
  
3. **What is the highest degree or level of education you have completed? Choose one option.**
  - A. High School/ General Certificate in Education/ Senior Secondary School Certificate
  - B. Ordinary National Diploma
  - C. Higher National Diploma
  - D. Bachelor's Degree
  - E. Post-Graduate Diploma
  - F. Master's Degree
  - G. Ph.D. or higher
  - H. Trade School
  - I. Prefer not to say
  
4. **What is your current role in your organization?**
  - A. System Administration
  - B. Information/Cybersecurity
  - C. Data Protection
  - D. \_\_\_\_\_ (Short Answer Space)
  
5. **What is years of experience**
  - A. Below 2 years
  - B. 2-5 years
  - C. 5-10 years
  - D. Above 10 years
  
6. **What is your current employment status? Choose one option.**
  - A. Employed Full-Time
  - B. Employed Part-Time
  - C. Seeking opportunities
  - D. Retired
  - E. Prefer not to say
  
7. **How long have you been in the organization? Choose one option.**
  - A. Below 2 years
  - B. 2-5 years
  - C. 5-10 years
  - D. Above 10 years
  - E. Prefer not to answer
  
8. **Position in organization. Choose one option.**
  - A. Junior level
  - B. Middle level
  - C. Senior level
  - D. Prefer not to answer

### Appendix B: Interview Guide with a Proposed Sequence

Interview Sequence	Interview Procedure and Question Items
Introduction	<ul style="list-style-type: none"> <li>• Commence the interview with an introduction of the study.</li> <li>• Explain the purpose of the interview.</li> <li>• Ask the following opening questions: <ul style="list-style-type: none"> <li>▪ Do you understand the purpose and nature of this study?</li> <li>▪ Do you consent to be interviewed?</li> </ul> </li> <li>• Engage in a conversation with the participant to promote a relaxed atmosphere</li> </ul>
Warm-up	<ul style="list-style-type: none"> <li>• Administer a short questionnaire eliciting demographic information.</li> <li>• Ask for factual background information and expansion if necessary <ul style="list-style-type: none"> <li>▪ What roles have you played in your organization?</li> <li>▪ Can you elaborate more on your background, qualifications, experience, training, and qualifications?</li> </ul> </li> </ul>
Main interview questions	<ul style="list-style-type: none"> <li>▪ Can you tell me about your data management process? How do you maintain this process?</li> <li>▪ Can you tell me about the flow of data within and outside the enterprise?</li> <li>▪ Have you established a data inventory? On what basis was this inventory established? How do you maintain this inventory? How do you ensure the accuracy of the data inventory? Can you tell me about your data inventory process?</li> <li>▪ How do you identify confidential or sensitive data on the organization's network? Can you tell me about your data classification scheme? How do you maintain this scheme?</li> <li>▪ Can you tell me about your access control? Do you maintain a data access control lists (access permission)? On what basis was this list configured?</li> <li>▪ How do you determine the criticality, vulnerability, and risk of data (including metadata) generated by computerized systems and software? What is the scope of this evaluation? What is the focus and scope of your data risk assessments?</li> <li>▪ How do you minimize potential risk to data security from contract acceptors, supply chain partners, and outsourced activities?</li> <li>▪ How does your qualification of supply chain partners and outsourced activities address data integrity risks?</li> <li>▪ How do you get service providers and vendor of systems to understand GMP and effectively implement data integrity requirements?</li> <li>▪ Can you tell me about the strategies for assessing data integrity in the supply chain?</li> <li>▪ What measures are in place to monitor subcontracting organizations and service providers?</li> <li>▪ How do you securely decommission service providers?</li> <li>▪ How do you protect sensitive data at rest? How do you ensure that third parties storing confidential data have in place appropriate security controls for sensitive data at rest?</li> <li>▪ How do you protect sensitive data on end-user devices?</li> <li>▪ How do you protect sensitive data on removable media?</li> <li>▪ How do you prevent vulnerabilities and security breaches from the use of USB memory sticks and storage devices on computer server and clients hosting GMP/GDP critical data?</li> <li>▪ How do you protect sensitive data in transit? How do you ensure that third parties transmitting confidential data have in place appropriate security controls for transmission of sensitive data?</li> <li>▪ How do you protect sensitive or confidential data transmitted via email?</li> <li>▪ What measures are in place to ensure that employees transmit data securely?</li> <li>▪ What measures are in place for correct and complete transfer of data?</li> <li>▪ How do you block potential unauthorized or unintentional transmission or removal of confidential data?</li> </ul>

Interview Sequence	Interview Procedure and Question Items
	<ul style="list-style-type: none"> <li>▪ Can you tell me about your strategies and efforts to prevent data loss or exfiltration of confidential data?</li> <li>▪ What measures are in place to prohibit unauthorized access to, changes to and deletion of data? What measures are in place to prevent, detect, and correct lapses in data security resulting from employee behavior? How do you ensure appropriate changes and modifications to data? How do you handle data security lapses?</li> <li>▪ How do you detect actions and entries relating to the acquisition, creation, access, deletion, overwriting of, changes to, and disposal of sensitive or confidential electronic data</li> <li>▪ Have you established audit trail functionality in all computerized system, including those of contracted organization? How do you ensure the correct management and configuration of audit trails? What mechanisms are in place to prevent audit trail functionalities from deactivation, deletion or modification? How do you verify the audit trail functionality?</li> <li>▪ How do you determine the data that is required in audit trails?</li> <li>▪ Can you tell me about your process for the review of audit trails? How do you determine which specific trails and which entries within trails are of significance for review? How do you determine the frequency of reviews? Does your review include audit trails held by contracted organization's computerized systems?</li> <li>▪ What measures are in place to ensure data availability in terms of capacity?</li> <li>▪ How do you address distributed denial-of-service (DDoS)?</li> <li>▪ How do you determine requirements for on-site and off-site storage of backup data?</li> <li>▪ What is the scope of your backups? How often do you backup and archive data? How do you determine the frequency of your backups? How physically close are archive copies to backup and original data storage?</li> <li>▪ Can you tell me about your data recovery process? How do you maintain this process? How do you maintain recovery data? How would you describe the strength of your recovery data controls?</li> <li>▪ What is the scope of the test for data recovery? How often do you test data recovery? How often do you test the restoration of archived data?</li> <li>▪ Can you tell me about your data retention process? How do you enforce data retention? How do you ensure ownership, access, and retrieval of data if data retention is contracted to a third party? What measures are in place for the maintenance of data access in the event of business closure or bankruptcy of the third party? What measures are in place to minimize the impact of laws on data held in applicable geographical locations?</li> <li>▪ How do you maintain accessibility, readability, and integrity of data for all the period of archiving? Are there provisions for the access of archived data in case an investigation is needed?</li> <li>▪ What measures are in place to protect records in an archiving facility from deliberate or inadvertent alteration or loss? What provisions are made for continued readability of the data archived when a system in the facility has to be retired?</li> <li>▪ What measures are in place to satisfy legal and regulatory requirements for historical data availability?</li> <li>▪ What measures are in place for new software to read existing and archived data? How do you ensure data access when legacy systems software can no longer be supported?</li> <li>▪ What measures are in place to incorporate data security controls in new systems and legacy systems (existing systems in use) /or software? How is the integrity of software and firmware verified?</li> <li>▪ What measures are in place for the correct capture of data acquired through automated means? How do you ensure that sensitive data is processed securely? What measures are in place to ensure test data are not processed by production</li> </ul>

Interview Sequence	Interview Procedure and Question Items
	<p>systems? How is the integrity of electronic data verified? Can you tell me about the process for the review of electronic data?</p> <ul style="list-style-type: none"> <li>▪ How do you securely dispose of electronically stored and/or confidential data?</li> <li>▪ Can you tell me about the network system security measure to detect and prevent potential threats to data?</li> <li>▪ Can you tell me about your system validation process? What measures are in place to prevent unauthorized changes to validated systems settings that may affect data integrity</li> <li>▪ How do you determine the effectiveness of data security control measures in computerized systems?</li> <li>▪ Can you tell me about your resource allocation for the support and sustenance of data security? What informs the allocation of resources?</li> </ul>
Wind-down	<ul style="list-style-type: none"> <li>▪ How long has the company been in operation?</li> <li>▪ Has the organization implemented a quality management system?</li> <li>▪ Is the organization ISO 9001 Certified?</li> <li>▪ Has the organization implemented an information security management system?</li> <li>▪ Is the organization ISO 27001 Certified?</li> <li>▪ To finish with this interview session, is there is anything else you would like to add?</li> </ul>
Close of interview	<ul style="list-style-type: none"> <li>▪ Is there nothing else you want to add?</li> <li>▪ Do you know and remember what happens to the interview data?</li> <li>• Show appreciation to the interviewee for his/her participation</li> </ul>

*Note.* This table provides the sequence of the schedule of interview questions.

## Appendix C: University Research Ethics Committee Provisional Approval



REAF\_DSPA - Version 1.0 AP

### UNICAF UNIVERSITY RESEARCH ETHICS APPLICATION FORM DOCTORAL STUDIES PROVISIONAL APPROVAL

The Provisional Approval - Research Ethics Application Form (REAF) should be completed by Doctoral level candidates enrolled on Dissertation stage 1.

This form is a **provisional approval** which means that the UREC committee has accepted the initial description of the project but this is conditional as changes may have to be implemented following Dissertation Stage 2 and piloting in Dissertation Stage 3.

**This is a conditional offer and acceptance of the project needs to be verified and confirmed upon completion of the Research Ethics Application Form in Dissertation Stage 3.**

#### Important Notes:

- An electronic version of the completed form should be uploaded by the student to the relevant submission link in the VLE. Student's supervisor will then review the form and provide feedback commentary. Once supervisor's initial approval is given then the supervisor will forward this to [doctoral.studies-aa@unicaf.org](mailto:doctoral.studies-aa@unicaf.org), for provisional approval by the Unicaf University Research Ethics Committee (UREC).
- Please type your answers and **do not** submit paper copy scans. Only *PDF* format documents should be submitted to the committee.
- If you need to supply any supplementary material, not specifically requested by the application form, please do so in a separate file. Any additional document(s) should be clearly labelled and uploaded in the relevant VLE link.
- If you have any queries about the form, please address them to your dissertation or project supervisor.



REAF\_DSPA - Version 1.0



**UNICAF UNIVERSITY**  
**RESEARCH ETHICS APPLICATION FORM**  
**DOCTORAL STUDIES PROVISIONAL APPROVAL**

UREC USE ONLY:

Application No: Date Received: **Student's Name:** Nnamdi Nwosu**Student's E-mail Address:** nwosu.nnamdi@gmail.com**Student's ID #:** R1903D8089259**Supervisor's Name:** Hatem Trabelsi**University Campus:** Unicaf University Zambia (UUZ)**Program of Study:** UUZ: PhD Doctorate of Philosophy**Research Project Title:** Toward a new framework for data security and compliance for drug GMP in pharmaceutical industry: A case study of Nigeria**1. Please state the timelines involved in the proposed research project:**

Estimated Start Date: 27-Sep-2020

Estimated End Date: 30-Jun-2021

**2. The research project****a. Project Summary:**

In this section please fully describe the purpose and underlying rationale for the proposed research project. Ensure that you pose the research questions to be examined, state the hypotheses, and discuss the expected results of your research and their potential.

It is important in your description to use plain language so it can be understood by all members of the UREC, especially those who are not necessarily experts in the particular discipline. To that effect please ensure that you fully explain / define any technical terms or discipline-specific terminology (maximum 300 words +/- 10%).

Pharmaceutical organizations have been the target of sophisticated cybercriminals and their operations reported with data integrity failings. Firstly, a security survey revealed a 78% increase in security incidents and a 50% rise in the theft of intellectual property (IP) in the life science and pharmaceutical industry. More so, governments such as that of the UK, suffered damages estimated at £1.8b resulting from cyber-theft of pharmaceutical IPs. Furthermore, findings show that most organizations, including indigenous drug manufacturing companies, were ill-prepared to respond to threats to information security despite an estimated cost of \$550 million due to cybercrime in Nigeria. Secondly, the US Food and Drug Administration (FDA) reported an increase in data integrity violations, globally, during GMP (Good Manufacturing Practices) inspections. Health authorities provided guidance on data management following these trends. Nonetheless, expert validation confirmed the existence of vulnerabilities that could be exploited by malicious individuals to steal pharmaceutical IPs and perform other malicious activities. The aim of this study is to investigate the data security gaps in drug current GMP and explore the application of best-practice frameworks in addressing identified gaps. Three research questions emerged to these investigate gaps: What are the gaps between drug current GMP specified by health authorities' guidance and drug manufacturing operations, in terms of data security? To what extent is data security emphasized in health authorities' guidance? What are the data security gaps in the guidance provided by health authorities? An expected outcome of this study is the identification of gaps in data security between health authorities' guidance and drug manufacturing operations. Another expected outcome is the identification and provision for gaps in health authorities' guidance and drug manufacturing operations in terms of good data security practices underscored by best-practice frameworks. The resulting data security framework informs GMP inspections and initiate other post-research interventions.

**b. Significance of the Proposed Research Study and Potential Benefits:**

Outline the potential significance and/or benefits of the research (maximum 200 words).

This study extends previous research efforts on enterprise governance and management of information and technology (EGIT), incorporating new insights from best-practice frameworks and standards, such as COBIT, ITIL, etc., in data management, tailored to the specific needs of pharmaceutical organizations. By proposing an approach based on such frameworks, this study will improve the security of data and systems that process and store intellectual properties of drug manufacturers. This study also responds to the call by an earlier study for further research in the area of data security, which in turn will enrich knowledge in data governance by the introduction of a data security framework. Furthermore, the study will provide governments with a framework for improving the critical cybersecurity infrastructure for pharmaceutical industries. More so, this study will inform the assessment of data integrity, which is a crucial aspect of cGMP (current good manufacturing practices) inspections. In addition, this study will address the needs of health authorities for modern control strategies for data management in the pharmaceutical industry.

**3. Project execution:**

**a. Type of project. The following study is an:**

- ☒ experimental study (primary research)
- ☐ desktop study (secondary research)
- ☐ desktop study using existing databases involving information of human/animal subjects
- ☐ Other

If you have chosen 'Other' please Explain:





**b. Methods. The following study will involve the use of:**

Method	Materials / Tools
<input checked="" type="checkbox"/> Qualitative	<input checked="" type="checkbox"/> Face to Face Interviews <input type="checkbox"/> Phone Interviews <input type="checkbox"/> Face to Face Focus Groups <input type="checkbox"/> Online Focus Groups <input type="checkbox"/> Other*
<input type="checkbox"/> Quantitative	<input type="checkbox"/> Self-administered Questionnaires <input type="checkbox"/> Online Questionnaires <input type="checkbox"/> Experiments <input type="checkbox"/> Tests <input type="checkbox"/> Other *

\*If you have chosen 'Other' please Explain:

**4. Participants**

**a. Does the Project involve the recruitment of participants?**

☒ YES    **If YES, please complete all following sections.**  
☐ NO    **If NO, please directly proceed to [Question 5](#).**

**Note:** The definition of "participation" includes active participation, such as when participants knowingly take part in an interview or complete a questionnaire.



### b. Relevant Participant Details of the Proposed Research

Please state the number of participants you plan to recruit, and describe important characteristics such as: demographics (e.g. age, gender, location, affiliation, level of fitness, intellectual ability etc). It is also important that you specify any inclusion and exclusion criteria that will be applied (e.g. eligibility criteria for participants).

Number of participants

Age range From  To

Gender ☒ Female  
☒ Male

Eligibility Criteria:

- Inclusion criteria 

Experts involved in qualifying and validating computerized systems and electronic data including data protection officers, system auditors, information security managers, and quality assurance managers.
- Exclusion criteria 

Participants whose profile does not indicate a minimum of 5 years experience in cGMP standards, as it relates to computer systems and data integrity in the pharmaceutical industry, are excluded from this study.

Disabilities 

Participants with disabilities are excluded from this study

Other relevant information (maximum 100 words):

The study involves the selection of experts playing the roles of data protection officer, system auditor, information security manager, and quality assurance manager from each of the ten Nigerian drug manufacturers that qualified or undergoing World Health Organization cGMP prequalification and certification. The selection of the four roles per organization results in 40 experts participating in this study.

**c. Recruitment Process for Human Research Participants:**

Please clearly describe how the potential participants will be identified, approached and recruited (maximum 200 words).

Potential participants will be identified from professional networking platforms. The principal investigator will engage each potential participants associated the organizations understudy and request for their email account, if not provided on the selected platform. The investigator will send research participants an information sheet to the email account provided that describes the study's purpose, procedures involved, rights to withdraw participation, how findings will be reported, etc., in lay terms, to obtain informed consent. The email account of an authorized individual, acting as gatekeeper for each organization understudy, will also be requested from the research participant to send an access proposal to conduct research at each site.

**d. Relationship between the principal investigator and participants:**

Is there any relationship between the principal investigator (student), co-investigators(s), (supervisor) and participant(s)? For example, if you are conducting research in a school environment on students in your classroom (e.g. instructor-student).

☐

YES

☒

NO

If YES, please specify (maximum 100 words).

**5. Further Approvals**

**Are there any other approvals required (in addition to ethics clearance from UREC) in order to carry out the proposed research study?**

☐

YES

☒

NO

If YES, please specify (maximum 100 words).

## 6. Potential Risks of the Proposed Research Study

**Are there any potential risks, psychological harm and/or ethical issues associated with the proposed research study, other than risks pertaining to everyday life events (such as the risk of an accident when travelling to a remote location for data collection)?**

☐ YES ☒ NO

If YES, please specify (maximum 150 words):

## 7. Application Checklist

Please mark ✓ if the study involves any of the following:

- ☐ Children and young people under 18 years of age, vulnerable population such as children with special educational needs (SEN), racial or ethnic minorities, socioeconomically disadvantaged, pregnant women, elderly, malnourished people, and ill people.
- ☐ Research that foresees risks and disadvantages that would affect any participant of the study such as anxiety, stress, pain or physical discomfort, harm risk (which is more than is expected from everyday life) or any other act that participants might believe is detrimental to their wellbeing and / or has the potential to / will infringe on their human rights / fundamental rights.
- ☐ Risk to the well-being and personal safety of the researcher.
- ☐ Administration of any substance (food / drink / chemicals / pharmaceuticals / supplements / chemical agent or vaccines or other substances (including vitamins or food substances) to human participants.
- ☐ Results that may have an adverse impact on the natural or built environment.

### 8. Final Declaration by Applicants:

- (a) I declare that this application is submitted on the basis that the information it contains is confidential and will only be used by Unicaf University and Unicaf University Research Ethics Committee (UREC) for the explicit purpose of ethical review and monitoring of the conduct of the research proposed project as described in the preceding pages.
- (b) I understand that this information will not be used for any other purpose without my prior consent, excluding use intended to satisfy reporting requirements to relevant regulatory bodies.
- (c) The information in this form, together with any accompanying information, is complete and correct to the best of my knowledge and belief and I take full responsibility for it.
- (d) I undertake to abide by the highest possible international ethical standards governing the Code of Practice for Research Involving Human Participants, as published by the UN WHO Research Ethics Review Committee (ERC) on <http://www.who.int/ethics/research/en/> and to which Unicaf University aspires to.
- (e) In addition to respect any and all relevant professional bodies' codes of conduct and/or ethical guidelines, where applicable, while in pursuit of this research project.
- (f) I understand it is my responsibility to submit a full REAF application during Dissertation Stage 3 to UREC. If a REAF application is not submitted my project is not approved by UREC.
- (g) I fully acknowledge that this form does not constitute approval of the proposed project but it is only a provisional approval.



I agree with all points listed under Question 8

Student's Name: Nnamdi Nwosu

Supervisor's Name: Hatem Trabelsi

Date of Application: 10-Sep-2020

### Important Note:

Please now save your completed form (we suggest you also print a copy for your records) and then submit it to your UU Dissertation/project supervisor (tutor). **In the case of student projects, the responsibility lies with the Faculty Dissertation/Project Supervisor.** If this is a student application, then it should be submitted via the relevant link in the VLE. Please submit only electronically filled in copies; **do not** hand fill and submit scanned paper copies of this application.



**Before submitting your application, please tick this box to confirm that all relevant sections have been filled in and the information contained is accurate to the best of your knowledge.**

## Appendix D: University Research Ethics Committee Final Approval



UREC Decision, Version 2.0



### Unicaf University Research Ethics Committee Decision

**Student's Name:** Nnamdi Nwosu

**Student's ID #:** R1903D8089259

**Supervisor's Name:** Dr Hatem Trabelsi

**Program of Study:** UU-DOC-900-3-ZM

**Offer ID /Group ID:** O30638G31853

**Dissertation Stage:** DS 3

**Research Project Title:** Leveraging COBIT 2019 in Cyber-Risk Management: A Model for GMP  
Data Security Requirements

Toward a new framework for data security and compliance for drug  
GMP in the pharmaceutical industry: A case study of Nigeria


**Comments:** No comments

**Decision\*:** A. Approved without revision or comments

**Date:** 03-Mar-2022

\*Provisional approval provided at the Dissertation Stage 1, whereas the final approval is provided at the Dissertation stage 3. The student is allowed to proceed to data collection following the final approval.

## Appendix E: Gatekeeper Letter Template



UU\_GL - Version 2.0  
☐

**Gatekeeper letter**

**Address:**

**Date:**

**Subject:**

Dear XXXX,

I am an/a [undergraduate, postgraduate, doctoral] student at Unicaf University [insert the name of the University, e.g. Malawi / Zambia].

As part of my degree I am carrying out a study on [insert project / research topic and area].

I am writing to enquire whether you would be interested in/willing to [insert request for assistance, participation, permission to recruit etc.] in this research.

Subject to approval by Unicaf Research Ethics Committee (UREC) this study will be using [mention the research activity / activities].

[Describe the project briefly and state its title and the name of your supervisor.]

[Describe what would be required of the person, for example, sending an e-mail on your behalf, allowing you to recruit on their premises, giving you access to personal data after participants have consented, allow children to complete experiments during school hours etc. Include the estimated time for the engagement of this person.]

Thank you in advance for your time and for your consideration of this project. Kindly please let me know if you require any further information or need any further clarifications.

Yours Sincerely,

Student's Name:

Student's E-mail:


Student's Address and Telephone:

Supervisor's Title and Name:

Supervisor's Position:

Supervisor's E-mail:

## Appendix F: Informed Consent Form Template



UU IC: Version 2.1  
☐

**Informed Consent Form**

**Part 1: Debriefing of Participants**

**Student's Name:**

**Student's E-mail Address:**

**Student ID #:**

**Supervisor's Name:**

**University Campus:**

**Program of Study:**

**Research Project Title:**

**Date:**

**Provide a short description (purpose, aim and significance) of the research project, and explain why and how you have chosen this person to participate in this research (maximum 150 words).**


The above named Student is committed in ensuring participant's voluntarily participation in the research project and guaranteeing there are no potential risks and/or harms to the participants.

Participants have the right to withdraw at any stage (prior or post the completion) of the research without any consequences and without providing any explanation. In these cases, data collected will be deleted.

All data and information collected will be coded and will not be accessible to anyone outside this research. Data described and included in dissemination activities will only refer to coded information ensuring beyond the bounds of possibility participant identification.

I,  ensure that all information stated above is true and that all conditions have been met:

**Student's Signature:**







UU\_IC - Version 2.1

## Informed Consent Form

## Part 2: Certificate of Consent

**This section is mandatory and should to be signed by the participant(s)**

Student's Name:	<input type="text"/>
Student's E-mail Address:	<input type="text"/>
Student ID #:	<input type="text"/>
Supervisor's Name:	<input type="text"/>
University Campus:	<input type="text" value="Choose from the list"/>
Program of Study:	<input type="text"/>
Research Project Title:	<input type="text"/>

I have read the foregoing information about this study, or it has been read to me. I have had the opportunity to ask questions and discuss about it. I have received satisfactory answers to all my questions and I have received enough information about this study. I understand that I am free to withdraw from this study at any time without giving a reason for withdrawing and without negative consequences. I consent to the use of multimedia (e.g. audio recordings, video recordings) for the purposes of my participation to this study. I understand that my data will remain anonymous and confidential, unless stated otherwise. I consent voluntarily to be a participant in this study.

Participant's Print name:

Participant's Signature:

Date:

**If the Participant is Illiterate:**

I have witnessed the accurate reading of the consent form to the potential participant, and the individual has had an opportunity to ask questions. I confirm that the aforementioned individual has given consent freely.

Witness's Print name:

Witness's Signature:

Date: