

2025

Q1 2025 Compliance Audit Report

DOMAIN:

PREPARED BY: COMPLIANCE AUDIT TEAM

DATE: MAY 2025 | AUDIT PERIOD: January- April 2025

Table of Contents

Abstract:	2
Overview	2
Summary of Section Findings	2
Section 1: Data Cleaning & Processing	2
Section 2: Data Storage, Security & Privacy	2
Section 3: Compliance & Accountability Measures	2
Section 4: Continuous Improvement & Compliance Culture.....	2
Final Score Summary	3
Recommendations- Quick Guide	4
Final Acknowledgements	5
Sign-Off and Approval	5
Appendix	6
A. Interview Questions.....	6
B. Preliminary (Self-Check) Form	9
C. Compliance Frameworks Referenced.....	9

Abstract:

Overview

Summary of Section Findings

Section 1: Data Cleaning & Processing

Score:

Compliance Status/Rating:

- **Strengths:**
- **Weaknesses**




Section 2: Data Storage, Security & Privacy

Section 3: Compliance & Accountability Measures

Section 4: Continuous Improvement & Compliance Culture

Final Score Summary

Section	Max	Achieved	Status
Data Cleaning & Processing			
Data Storage, Security & Privacy			
Compliance & Accountability			
Continuous Improvement & Compliance Culture			
Total			

Compliance Score (%)	Final Rating
90 - 100%	 Compliant – No major risks, minor improvements suggested.
70 - 89%	 Partially Compliant – Some risks identified; action needed.
Below 70%	 Non-Compliant – Does not meet requirements, immediate action required.

Recommendations- Quick Guide

***See notes below

Audit Finding	Recommended Action	Priority	Owner

Final Acknowledgements

This report was prepared by the Compliance Audit Team following structured interviews, documentation reviews, and collaborative input from the Data Cleaning domain. The team acknowledges the effort and cooperation of all domain members throughout the process.

Sign-Off and Approval

Name	Role	Signature	Date
[Audit Lead]	Compliance Audit Team Lead		
[Compliance Lead]	Compliance Team Lead		
[Reviewer Name]	Domain Representative		

Appendix

A. Interview Questions

Section 1 (PART 2): Data Cleaning & Processing (To be answered by Data Cleaning ONLY)

Data Integrity & Quality Control

1. Is there a structured data cleaning process that is version controlled or documented for reproducibility?

☐ Yes/ ☐ No

Comments

2. Are scripts or automated tools used to check data quality (e.g., duplicates, missing values, or formatting issues)?

☐ Yes/ ☐ No

3. How is missing data handled? Are nulls, blanks, and duplicates properly identified and managed?

4. After data cleaning, is the output reviewed manually or validated using tools to ensure accuracy before use?

☐ Yes/ ☐ No

5. How is potentially compromised or illegal data handled during cleaning (e.g., flagged, quarantined, discarded)?

6. Are cleaning rules reassessed regularly based on feedback, new patterns, or issues found?

☐ Yes/ ☐ No

7. Are there performance bottlenecks or known limitations in the current cleaning workflow?

☐ Yes/ ☐ No

Section 2: Data Storage, Security & Privacy

Security & Risk Awareness

1. If your team handles compromised or leaked data, how is risk managed during acquisition and storage. (3 pts max)

2. Are regular vulnerability assessments conducted? (3pts max)

☐ Yes/ ☐
No

3. Is there a centralized repository for finalized scripts and collected information or datasets? How is version control managed? (3 pts max)

☐ Yes/ ☐
No

Comments

4. Are backup systems in place for scripts, scraped information or datasets? Are they encrypted and stored offsite or in a secure cloud location? (4 pts max)	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>
5. Is there a process for revoking access when a team member leaves or changes roles? (2 pts max)	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>
6. Are there clear policies for retention and secure disposal? (3 pts max)	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>
7. If datasets are stored across different platforms (e.g., Teams, GitHub, local machines), how is cross platform consistency ensured, so people are not working on outdated information? (3 pts max)		<hr/>
8. Are you aware of whether members have standard protections in place? Multi-Factor Authentication (MFA), etc.? (4 pts max)	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>

Section 3: Compliance & Accountability Measures

Breach & Incident Reporting

1. Are formal data breach reporting processes in place?	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	Comments <hr/>
2. Any compliance violations or incidents before this audit?	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>
3. Is there a documented incident response plan in case of a data breach or unauthorized access? If yes, who is responsible for executing it?		<hr/>
4. Has your team encountered any challenges in storing or organizing data securely (e.g., decentralized files, missing logs, lost local data)?	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>
5. Is there a dedicated person responsible for ensuring your team remains up to date on compliance obligations?	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>

Section 4: Continuous Improvement & Compliance Culture

Transparency

1. Has your team finalized a document outlining the roles and responsibilities of each subgroup or team member?	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	Comments <hr/>
2. What specific improvements (if any) has your team made in the past 3–6 months to strengthen data practices and compliance?		<hr/>
3. Do you conduct internal reviews or debriefs after completing major collection or cleaning cycles?	<input type="checkbox"/> Yes/ <input type="checkbox"/> No	<hr/>

4. When was the last time your team reviewed or discussed compliance expectations in a meeting or formal setting?

5. What tools or support do you feel would help your team become more compliant or secure?

B. Preliminary (Self-Check) Form

Preliminary self-check forms completed by both domains. Responses informed about the focus areas of the interviews and scoring methods. It covered topics such as team responsibilities, data sensitivity, access controls, and compliance awareness. The full form can be viewed at the following link:

<https://forms.office.com/r/KzA5nxSAAG>

C. Compliance Frameworks Referenced

Barbados Data Protection Act- <https://www.privacylaws.com/media/4517/data-protection-act-2019-29.pdf>

EU AI Act- <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

GDPR- <https://gdpr-info.eu/>

NIST AI RMF- <https://www.nist.gov/itl/ai-risk-management-framework>