Federal Board of Revenue
Revenue Division – Government of Pakistan

Federal Board of Revenue

Data Governance Policy

Approved on 04 July 2024

Team Members

Zain Sahi , Chief IT, FBR
Akbar Mayo, Tax Lead, REMIT
Dr Fareed Zafar, Cyber Security Expert , REMIT
Muhammad Faizan Ghani, Cyber Security Expert, REMIT

1. Table of Contents

1. TABLE OF CONTENTS 2
2. DOCUMENT DETAILS 4
3. REVISION HISTORY 4
4. APPROVAL 5
5. DEFINITIONS AND KEY TERMS 6
6. INTRODUCTION 9
6.1. Purpose of the Document 9
6.2. Scope and Applicability 9
7. PRINCIPLES OF DATA GOVERNANCE 10
8. DATA GOVERNANCE FRAMEWORK 11
8.1. Data Governance Operating Model 11
8.2. Roles and Responsibilities 15
8.3. Reporting and Escalation Procedure 24
9. CORE DATA POLICIES 26
9.1. Data Quality Management Policy 26
9.2. Master and Reference Data Management Policy 28
9.3. Metadata Management Policy 29
9.4. BI and Data Warehousing Policy 31
9.5. Document and Content Management Policy 33
9.6. Data Integration and Interoperability Policy 34
9.7. Data Security Policy 35
9.8. Data Privacy and Protection Policy 41
9.9. Data Storage and Operations Policy 43
9.10. Data Modeling and Design Policy 44
9.11. Data Usage Policy 45
9.12. Data Access and Control Policy 47
9.13. Data Destruction Policy 50
9.14. Third-Party Data Access and Sharing Policy 51
9.15. Incident Response Policy 53
9.16. Data Providers Engagement Policy 54
9.17. Data Classification Policy 55
9.18. Data Backup, Retention and Recovery Policy 56
9.19. Change Management Policy 58
9.20. Data Architecture Policy 59
9.21. Data Management Maturity Policy 61
10. COMMUNICATION AND TRAINING 63
10.1. Communication 63
10.2. Training 63
11. PROCEDURAL FLOWS FOR CRITICAL DATA PROCESSES 64
11.1. VPN Access 64
11.2. Application Creation and Modification 65
11.3. Database Access 66

11.4. Data Sharing 67
11.5. Database Backup 68
11.6. Jurisdiction Change 69
11.7. ETL Pipeline 70
11.8. Server Virtualization 71
12. POLICY REVIEW AND MODIFICATION 72
12.1. Review Schedule 72
12.2. Procedures for Policy Amendments 72
12.3. Feedback Mechanism 72
13. POLICY COMPLIANCE, ESCALATION AND EXCEPTIONS 73
13.1. Compliance 73
13.2. Non-Compliance 73
13.3. Escalations 73
13.4. Compliance Exceptions 73
ANNEX I: ALIGNMENT OF DATA GOVERNANCE POLICY WITH DAMA DMBOK V2 75
ANNEX II: DATA GOVERNANCE POLICY IMPLEMENTATION MATRIX 76
ANNEX III: FBR INFORMATION & CYBER SECURITY GRC FRAMEWORK 78
ANNEX IV: FBR INCIDENT RESPONSE PROCEDURE 79

2. Document Details

Document Title	Data Governance Policy
Document Version	Version 1.0
Effective Date	
Approved By	
Approved Date	

3. Revision History

Version	Date	Author	Comments
Version 1.0			Initial Issue

4. Approval

This Data Governance Policy represents FBR's commitment to the highest standards of data management. It has been developed through a collaborative process, incorporating insights and expertise from various departments to ensure its relevance and effectiveness. By endorsing this policy, the senior leadership commits to its principles and guidelines, recognizing the critical role of data governance in achieving our organizational goals. The policy's approval marks a significant step in our ongoing journey to leverage data responsibly and effectively.

Approved by:

Signature: _____

Date:

5. Definitions and Key Terms

business data glossary is an inventory of business terms, their definitions, and their organized structure within a particular data domain. It acts like a dictionary for business-related terms in data management.

Chief Data Governance and Management (CDGM) is an FBR Officer in charge of overseeing the data governance strategy and its implementation within the Federal Board of Revenue (FBR).

critical data is data essential for risk management, regulatory compliance, and financial reporting, or data crucial for supporting business growth and senior leadership decision-making.

data is a collection of facts, figures, and statistics, either in raw or processed form, used for reference, analysis, or as the basis for decision-making. It forms the foundation for information creation.

data access is the ability to reach, modify, or delete data elements stored in places like databases.

data culture is the collective behaviors and beliefs of people in an organization who value and actively use data to enhance decision-making.

Custodian refers to operational staff responsible for the technical aspects of data management, including the security, storage, and maintenance of data systems.

data element means a fundamental unit of data within a data processing system, which has a specific and clear meaning, like the name of a certified organization or the size of a land area.

data governance is the comprehensive management of data's availability, usability, integrity, and security within an organization.

data governance framework is a collection of operating model, roles, and responsibilities that ensure the integrity, security, and compliance of enterprise data management in an organization.

data governance program is a structured set of standards and procedures as well as a plan implemented to govern and manage data within an organization effectively.

data identifier is a unique label, sign, or token that distinctly identifies an object within an identification scheme, independent of language.

data inventory is a complete listing of all data assets within a tax administration, including details about their scope, source, provider, and storage locations.

data lifecycle encompasses the stages through which data travels, from its initial creation or capture to its final archiving or deletion. This includes phases like creation, usage, storage, sharing, and destruction.

data lineage is the tracing of data's movements and transformations from its original source or point of derivation to its final use or consumption.

data process or processing means any operation or set of operations performed on data, such as collection, recording, organization, storage, adaptation, alteration, retrieval, use, disclosure, dissemination, erasure, or destruction.

data provider is the entity that discloses data for processing and/or use by a data recipient.

data quality represents the measure of data's fitness for use, characterized by accuracy, completeness, reliability, and relevance, ensuring the data is suitable for its intended purpose.

data quality dimensions include aspects such as completeness, validity, precision, uniqueness, integrity, timeliness, and accuracy, which define the overall quality of data.

data quality rule is a specific criterion used to assess the quality of data, like requiring a year to be in a four-digit format.

data quality threshold is the minimum acceptable level or pass rate for data quality as defined by specific rules.

data security incident is an event, either accidental or deliberate, that leads to or poses a risk of unauthorized access, loss, disclosure, modification, disruption, or destruction of data, particularly personal data.

Steward is an individual tasked with the responsibility of managing data assets in a specific area, focusing on maintaining data quality, consistency, and security.

data stewardship involves managing and overseeing the care, quality, and control of data, ensuring it is accurately maintained, securely stored, and appropriately utilized within an organization.

data taxonomy is a hierarchical structure that classifies data into specific categories based on common characteristics.

disclosure means the act of sharing data voluntarily, either publicly or with a specific third party.

evaluation data is data used to compare actual results and impacts against predefined plans or objectives, examining aspects like efficiency and effectiveness.

Federal Board of Revenue (FBR) is the government body responsible for tax administration, data management, and regulatory compliance.

full backup means creating a complete copy of the entire database system, including transaction logs, to ensure data recovery in case of system failure.

identifiable data is any information that can be used to distinguish or trace an individual or entity's identity, or any data linkable to an individual or entity.

incremental backup is a backup process where only the data changes made since the last backup are copied, saving time and storage space.

information means knowledge about objects such as facts, events, processes, ideas, or concepts, which is meaningful in a specific context.

metadata is data about data, describing characteristics like content, quality, format, location, and contact information, ensuring data discoverability and usability.

monitoring data is ongoing measurement of specific indicators over time, focusing on the use of inputs, activities, outputs, and short-term outcomes.

payload is the carrying capacity of a data packet or transmission unit, referring to the actual data being transmitted.

personal data is information in any format that relates to an identified or identifiable living person, identifiable through various means such as a name, identification number, or other specific factors.

project is a temporary effort undertaken to create a unique service or result, characterized by its temporary and unique nature.

program is a group of related projects managed in a coordinated manner to achieve benefits and control not possible from managing them individually.

raw data is the original data as it is first captured, whether recorded on paper or electronically, also known as source data.

record is information created, received, and maintained as evidence and an asset by an organization or person, in pursuit of legal obligations or business transactions.

retention is the specified duration for which an organization agrees to keep different types of records, guided by retention schedules for compliance.

sensitive personal data typically includes bank account numbers, national identification card numbers, tax records, income details, and financial transaction data. This information is crucial for accurate tax processing and requires secure handling to protect taxpayer privacy and confidentiality.

service provider is any individual or entity contracted to process data or to develop, maintain, or update systems for an organization.

system is any information or data system designed to collect, process, store, and distribute data, encompassing technology platforms, databases, data warehouses, websites, applications, and hardware equipment.

6. Introduction

6.1. Purpose of the Document

This Data Governance Policy is established to define and mandate the Federal Board of Revenue's strategic direction in managing its critical data assets. It encapsulates the guiding principles, governance operating model, core data policies, and procedural flows for critical processes that collectively ensure the ethical stewardship, security, and optimal use of data. By transitioning from isolated data handling to a unified governance model, this policy underlines FBR's dedication to reinforcing data integrity, security, and availability across all functions. The comprehensive nature of this policy, with its inclusion of high-level procedural flows for critical processes and execution strategies, underscores FBR's commitment to fostering an accountable and data-centric organizational culture. Upon approval by the **Chairman FBR/Board-in-Council**, this policy will serve as the authoritative blueprint for driving FBR's data governance initiatives forward.

6.2. Scope and Applicability

6.2.1. Data in Scope

This Policy is exhaustive in its reach, encompassing all data and information owned by the Federal Board of Revenue (FBR), irrespective of its form or mode of communication. It pertains to, but is not limited to, the following categories:

6.2.1.1. Verbal communications, whether conducted in person, over the telephone, or through any existing or future technologies.

6.2.1.2. Physical records, encompassing printed materials and handwritten documents.

6.2.1.3. Transmissions via postal or courier services, fax, electronic mail, messaging services, chat, and similar platforms.

6.2.1.4. Data stored, processed, or transmitted through servers, personal computers, laptops, tables, mobile devices, and similar technologies.

6.2.1.5. Data stored on any type of internal, external, or removable media, as well as data housed in cloud-based services.

6.2.2. Applicability

The provisions of this policy apply to all FBR officers/officials, departments, and units, including third-party contractors and IT suppliers such as Pakistan Revenue Automation Ltd (PRAL) who are engaged in the creation, handling, processing, storage, and dissemination of FBR data and/or are provided with access to FBR's data and systems. The requirements laid out in this policy are binding upon all entities that interact with FBR's data, ensuring a standardized approach to data governance that aligns with the organization's commitment to data integrity, security, and regulatory compliance.

7. Principles of Data Governance

The principles outlined below establish the standards for how data should be managed within the Federal Board of Revenue (FBR). They provide a foundation for the consistent development of data governance policies, standards and procedures across the organization.

7.1. Data as an Asset: Recognizing the vital role of data in ensuring compliance and offering tailored services, there is a strong focus on maintaining high-quality standards throughout the data lifecycle. This involves establishing quantifiable measures for data quality and conducting regular assessments. The process encompasses managing data from its creation to its eventual archiving or disposal, ensuring its integrity and value are upheld.

7.2. Privacy and Data Protection: With a firm commitment to protecting taxpayer data, practices are aligned with international privacy standards. The approach to managing personal and sensitive information is grounded in ethics and respect for taxpayer confidentiality. Regular privacy assessments are conducted to mitigate risks in data processing, reinforcing the responsible and lawful handling of data.

7.3. Transparency in Data Management: Emphasizing transparent practices, the approach to data management involves comprehensive documentation of data handling, including its lineage and processing activities. This transparency extends to engaging stakeholders through clear communication and detailed reporting, instilling confidence in the FBR's data management practices.

7.4. Control and Auditability in Data Management: Highlighting the importance of oversight, data management includes rigorous audit trails and control mechanisms like access controls and encryption. The adoption of automated tools for continuous monitoring and compliance verification underscores a commitment to upholding stringent governance standards.

7.5. Responsibility and Data Stewardship: The responsibility for data governance is clearly delineated across FBR. This includes defining roles and ensuring data management is an integral part of the organizational structure. Emphasizing the importance of training and awareness, a culture of accountability and stewardship is fostered, ensuring data is handled with the highest level of care and responsibility.

8. Data Governance Framework

8.1. Data Governance Operating Model

The Federal Board of Revenue (FBR) will adopt a centralized Data Governance Operating Model, emphasizing stringent control over data governance and information security, particularly in FBR's relationship with the IT Supplier/PRAL. This model ensures centralized oversight and effective implementation of FBR's data governance strategies in which Chairman FBR, as primary data owner, holds ultimate accountability for data governance. The Chairman FBR is responsible for approving all overarching data governance and information security policies.

Chairman FBR delegates the responsibility for implementing the Data Governance Policy to Member IT, who maintains accountability for its execution. The Member IT, in turn, entrusts the day-to-day management to the Chief Data Governance and Management (CDGM).

At the core of this model are the key IT Managers/Executives of IT Supplier/PRAL as Stewards. Their role is primarily focused on adherence to the established governance standards and procedures. Their direct reporting to the CDGM ensures that the FBR's Data Governance Policy is effectively implemented and monitored, strictly aligning the operations of IT Supplier/PRAL with the policies set forth by FBR.

The centralized Data Governance Operating Model is anchored by a key entity:

8.1.1. Data Governance Office

The Data Governance Office (DGO) serves as the central unit for implementing, managing, and overseeing the data governance and information security policies within FBR and IT Supplier/PRAL. Headed by the Chief Data Governance and Management (CDGM), the DGO ensures the translation of high-level policies approved by the Chairman FBR/Board-in-Council into operational procedures, maintaining strict adherence to governance standards. Its key functions include monitoring compliance, coordinating with the IT Supplier/PRAL, and reporting on policy implementation progress. The DGO also plays a vital role in training FBR staff and IT Supplier/PRAL personnel to enhance awareness and understanding of data governance issues. Moreover, it oversees the activities of key IT Managers/Executives of IT Supplier/PRAL, who act as Stewards, ensuring their strict alignment with FBR's data governance standards and procedures.

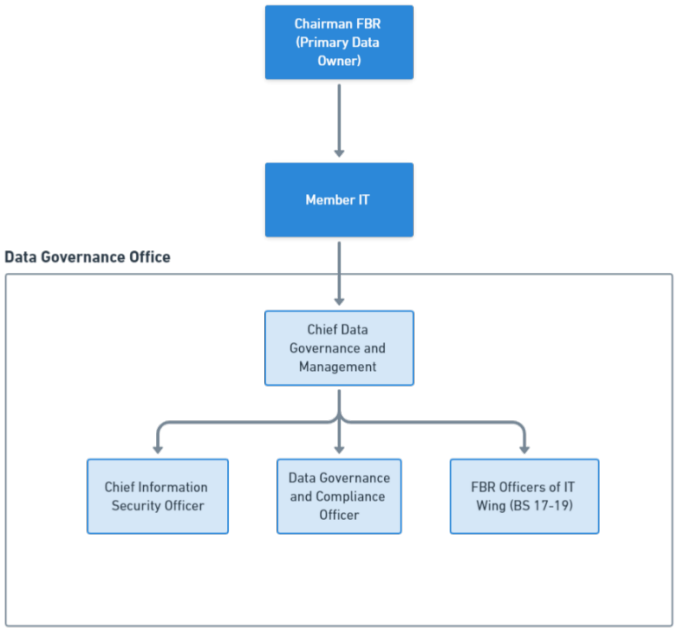


Figure 1. Composition of Data Governance Office.

8.1.2. Creation of the Data Governance Office:

8.1.2.1. Chairman FBR/Board-in-Council shall give approval for the establishment of the Data Governance Office (DGO) as part of the data governance framework.

8.1.2.2. Chairman FBR shall appoint an officer of the IT wing as the Chief Data Governance and Management (CDGM) on recommendation of the Member IT.

8.1.2.3. Chief Data Governance and Management (CDGM) shall head the Data Governance Office.

8.1.2.4. Member IT, upon recommendation of the Chief Data Governance and Management (CDGM), shall appoint BS 17-19 officers of the IT Wing to the Data Governance Office.

8.1.2.5. Member IT, upon recommendation of the Chief Data Governance and Management (CDGM), shall appoint a Chief Information Security Officer (CISO) to the Data Governance Office. The CISO role may be filled by a suitably qualified internal FBR employee or an external third-party consultant.

8.1.2.6. Member IT, upon recommendation of the Chief Data Governance and Management (CDGM), shall appoint a Data Governance and Compliance Officer (DGCO) to the Data Governance Office. The DGCO role may be filled by a suitably qualified internal FBR employee or an external third-party consultant.

8.1.3. Identification of Stewards and Custodians:

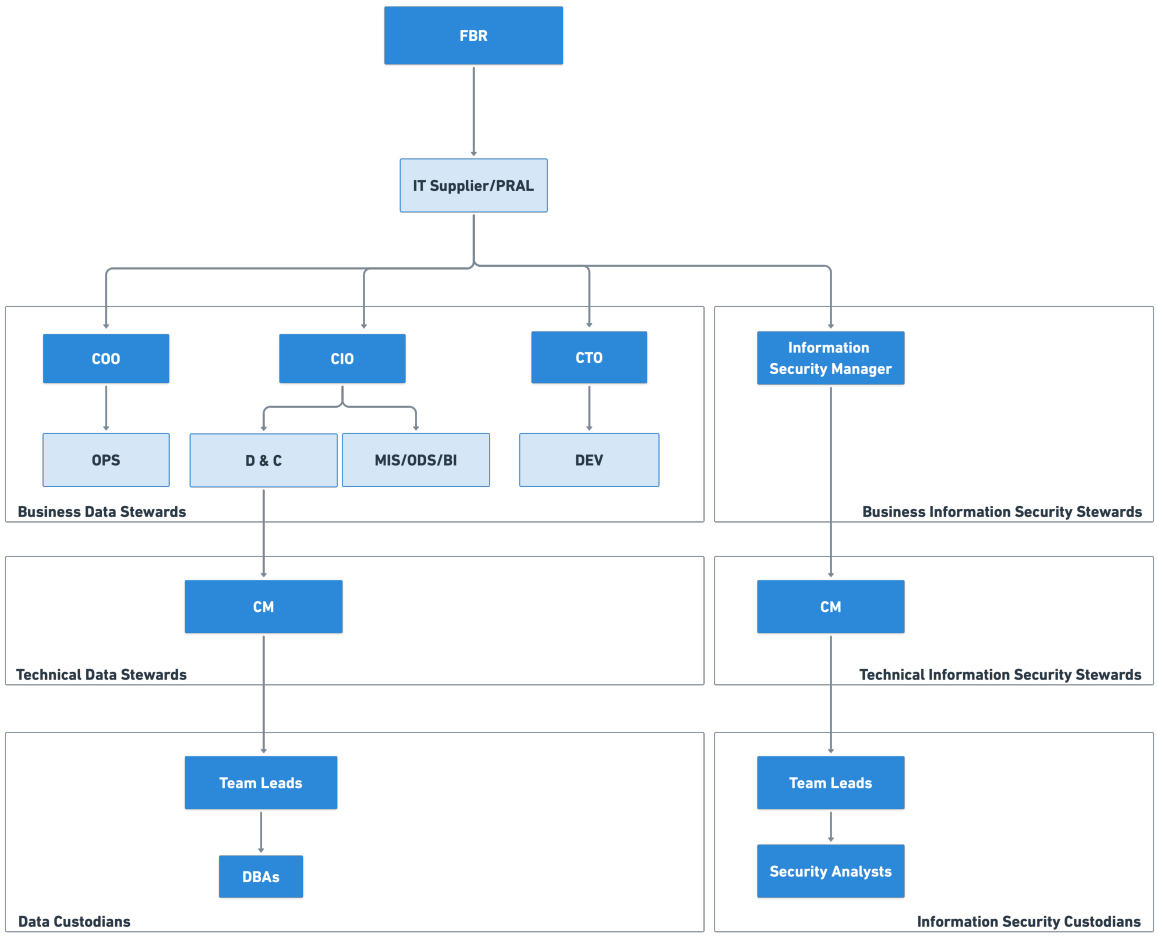


Figure 2. Placement of Stewards and Custodians within organizational hierarchy.

8.1.3.1. Member IT, upon the nomination of the Chief Data Governance and Management (CDGM), shall identify key IT Managers/Executives of IT Supplier/PRAL as Data Stewards and Information Security Stewards. These individuals are chosen based on their expertise and role within the organization, ensuring that business and technical aspects of both data governance and information security are adequately represented. Data Stewards and Information Security Stewards typically include, but are not limited to, roles such as Chief Operations Officer (COO), Chief Technology Officer (CTO), Chief Information Officer (CIO), Information Security Manager, and Chief Managers.

8.1.3.1.1. Data Stewards shall supervise Data Custodians of IT Supplier/PRAL, who are the operational staff under their respective domains. Data Custodians are responsible for the practical aspects of data governance, operationalizing data governance policies at the ground level. Data Custodians typically include, but are not limited to, roles such as Database Administrators (DBAs), Developers, System Administrators, and Data Analysts.

8.1.3.1.2. Information Security Stewards shall supervise Information Security Custodians of IT Supplier/PRAL, who are the operational staff under their respective domains.

Information Security Custodians are responsible for practical application of information security measures. Information Security Custodians typically include, but are not limited to, roles such as IT Security Analysts, Network Security Administrators, and other specialists who are adept in various facets of information security.

8.1.4. Centralized Data Governance Structure

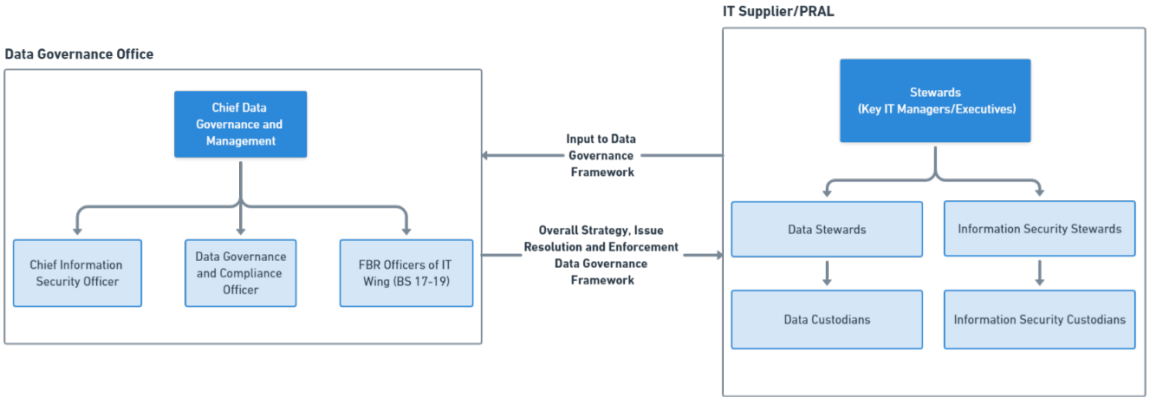


Figure 3. Centralized operating model for Data Governance.

Departmental data governance within IT Supplier/PRAL, is key in implementing the Data Governance Policy at the ground level, ensuring their adaptability and effectiveness organization wide.

8.1.4.1. Relevant departments shall provide specific insights and operational feedback to the Data Governance Office (DGO), integrating departmental needs into the broader governance framework.

8.1.4.2. Data Stewards and Information Security Stewards shall serve as critical links between their departments and the Data Governance Office (DGO) advocating for departmental needs while aligning with overarching governance policies.

8.1.4.3. Data Custodians and Information Security Custodians shall be responsible for implementing and managing the day-to-day aspects of data governance within their respective departments. Data Custodians handle the operational aspects of data management, such as data processing, storage, and quality control. In parallel, Information Security Custodians focus on the practical implementation of information security measures, such as managing security infrastructure, monitoring for security breaches, and responding to security incidents.

8.2. Roles and Responsibilities

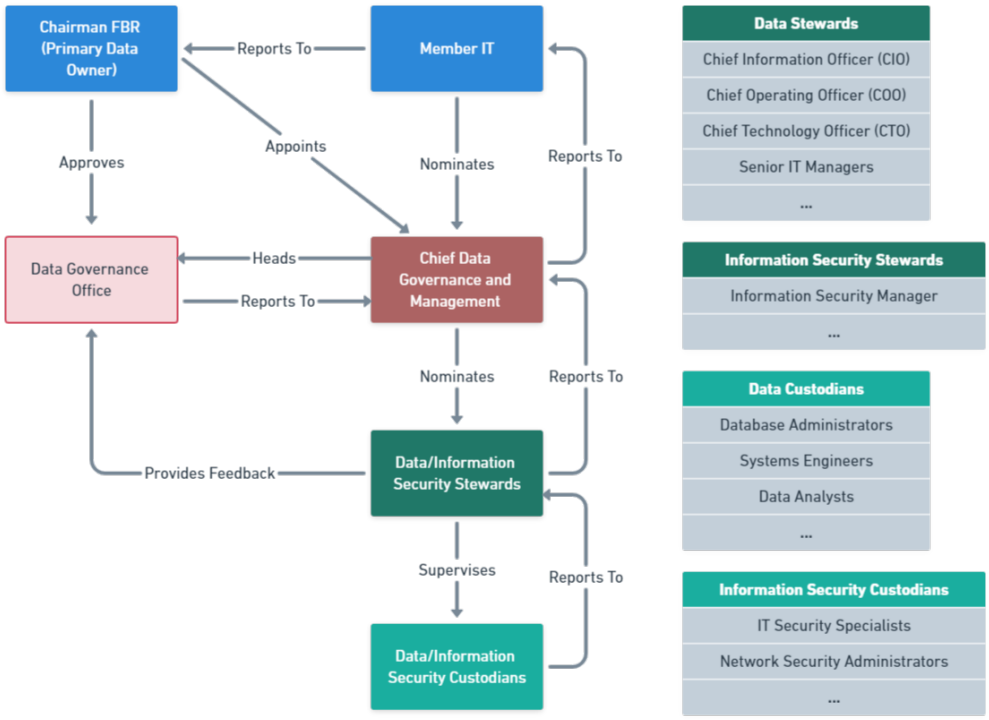


Figure 4. Interconnected Roles and Relationships within the Data Governance Framework.

The data governance roles defined below speak only to the responsibility of a position pertaining to data governance and do not correlate to the actual functional and hierarchical organization structure in FBR and in IT Supplier/PRAL. Depending on resource availability, one role may be assigned to multiple persons or multiple roles may be assigned to one person. Additionally, a role that rightly falls under the purview of an individual may be delegated to another.

8.2.1. Chairman FBR/Board-in-Council

The Chairman FBR/Board-in-Council is crucial in providing leadership and direction for FBR's data governance efforts. By fulfilling these responsibilities, the Chairman FBR/Board-in-Council ensures that FBR maintains a robust, compliant, and effective approach to managing its critical data assets and protecting them from security threats.

Responsibilities:

8.2.1.1. Shall be responsible for approving the Data Governance Policy, ensuring it aligns with FBR's strategic objectives.

8.2.1.2. Shall give formal approval for the establishment of the Data Governance Office (DGO).

8.2.1.3. Shall hold ultimate responsibility for all data held by FBR, ensuring its integrity, security, and compliance with relevant laws and regulations.

8.2.1.4. Shall appoint an officer from the IT wing as the Chief Data Governance and Management (CDGM), based on the recommendation of the Member IT.

8.2.1.5. Shall serve as the final decision-making authority in all matters related to data governance.

8.2.2. Member IT

The Member IT plays a pivotal role in the operationalization and management of the FBR's data governance initiatives. The Member IT bridges the strategic directives set by the Chairman FBR/Board-in-Council with the day-to-day management of data governance.

Responsibilities:

8.2.2.1. Shall recommend suitable candidate for the role of Chief Data Governance and Management (CDGM) to Chairman FBR for approval.

8.2.2.2. Shall appoint BS 17-19 officers of the IT Wing, upon recommendation of CDGM, to the Data Governance Office (DGO).

8.2.2.3. Shall appoint a Chief Information Security Officer (CISO) and Data Governance and Compliance Officer (DGCO), upon recommendation of CDGM, to the Data Governance Office (DGO).

8.2.2.4. Shall monitor data governance initiatives and reports progress to Chairman FBR/Board-in-Council.

8.2.2.5. Shall ensure that necessary resources are available to establish, implement, operate, review, maintain, and improve the FBR's data governance practices.

8.2.2.6. Shall be responsible for ensuring that the Chief Data Governance and Management (CDGM) adheres to and is compliant with all relevant data governance policies, standards, and procedures.

8.2.2.7. Shall maintain accountability for effective execution of the Data Governance Policy.

8.2.2.8. Shall provide oversight to the Data Governance Office (DGO).

8.2.2.9. Shall resolve data-related incidents in coordination with the DGO, ensuring efficient risk mitigation and issue resolution.

8.2.3. Chief Data Governance and Management (CDGM)

Chief Data Governance and Management (CDGM) leads the overall development, implementation, monitoring, and continuous improvement of the data governance policy and practices.

Responsibilities:

8.2.3.1. Shall head the Data Governance Office (DGO) to operationalize the implementation and enforcement of data governance practices across FBR and IT Supplier/PRAL.

8.2.3.2. Shall maintain regular communication with Member IT to update on data governance initiatives and compliance matters.

8.2.3.3. Shall make recommendations to the Member IT for the appointment of Chief Information Security Officer (CISO) to oversee and fortify the organization's information security posture, aligning it with the overall data governance strategy.

8.2.3.4. Shall make recommendations to the Member IT for the appointment of a Data Governance and Compliance Officer (DGCO) to assist the Data Governance Office (DGO) in the enforcement of Data Governance Policy across FBR and IT Supplier/PRAL.

8.2.3.5. Shall communicate the Data Governance Policy decisions to FBR officers/officials, IT Supplier/PRAL, service suppliers, and third-party contractors.

8.2.3.6. Shall manage data governance training programs and awareness campaigns.

8.2.3.7. Shall oversee the development and standardization of data rules, definitions, processes, standards and procedures.

8.2.3.8. Shall take the lead in developing comprehensive data performance metrics, ensuring these metrics effectively measure and align with the FBR's strategic objectives.

8.2.3.9. Shall oversee the documentation and application of business rules, guaranteeing that they are consistently applied and integrated into data governance practices.

8.2.3.10. Shall keep track of Stewards and Custodians, ensuring clear guidance on roles and responsibilities.

8.2.3.11. Shall determine which roles have access to specific systems or data, and grant access to data at the appropriate granularity within the system.

8.2.3.12. Shall facilitate effective communication between the DGO, IT Supplier/PRAL, and other FBR departments.

8.2.3.13. Shall serves as the central point of contact for internal and external stakeholders on data governance and information security matters.

8.2.3.14. Shall manage and coordinates responses to data breaches or security incidents, ensuring swift and effective resolution.

8.2.3.15. Shall review the Data Governance Policy, suggest improvements, and recommend changes to be made to the Member IT for subsequent approval of the Chairman FBR/Board-in-Council.

8.2.3.16. Shall translate high-level policy decisions into actionable and practical procedures and guidelines, upon approval of Member IT.

8.2.3.17. Shall conduct bi-annual reviews of all policies, standards, and procedures related to data governance and information security.

8.2.4. Data Governance and Compliance Officer (DGCO)

The Data Governance and Compliance Officer (DGCO) is responsible for supporting Chief Data Governance and Management (CDGM) in effectively executing and enforcing the Data Governance Policy.

Responsibilities:

8.2.4.1. Shall assist the CDGM in developing and refining data governance policies, standards, and procedures.

8.2.4.2. Shall monitor adherence to data governance policies, standards, and procedures across FBR and IT Supplier/PRAL.

8.2.4.3. Shall conduct periodic audits and assessments to ensure compliance and identify areas for improvement.

8.2.4.4. Shall conduct training sessions and awareness programs to instill a data governance culture within FBR and IT Supplier/PRAL.

8.2.4.5. Shall manage the documentation and reporting of data governance activities, maintaining transparency and accountability.

8.2.4.6. Shall assess risks related to data governance and recommend appropriate mitigation strategies.

8.2.4.7. Shall engage with stakeholders to understand their data governance needs, ensuring the data governance policy is effectively aligned.

8.2.4.8. Shall track and report on the performance of data governance initiatives and conduct quarterly maturity assessments, suggesting improvements as necessary.

8.2.5. Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is responsible for overseeing all aspects of information and data security.

Responsibilities:

8.2.5.1. Shall recommend the establishment and maintenance of the enterprise vision, strategy, and program to ensure adequate protection of information assets.

8.2.5.2. Shall identify, evaluate, and report on information security risks in a manner that meets compliance and regulatory requirements.

8.2.5.3. Shall provide recommendations for the development and maintenance of policies, standards and procedures for the information security program.

8.2.5.4. Shall oversee the investigation of security incidents and provide advice on appropriate responses to data breaches or attacks.

8.2.5.5. Shall advise on ensuring compliance with statutory and regulatory requirements regarding information access, security, and privacy.

8.2.5.6. Shall promote a culture of information security awareness and provide guidance on training staff in security responsibilities.

8.2.5.7. Shall recommend technology solutions that safeguard the organization's systems and data.

8.2.5.8. Shall provide strategic advice on emerging security threats and technologies, assessing their potential impact on the organization.

8.2.5.9. Shall develop and improve the FBR and Customs nation-wide information security governance, risk and compliance (GRC) policy framework, process, procedures, and deliverables.

8.2.5.10. Shall develop, lead, and improve FBR Cyber SOC operations.

8.2.5.11. Shall develop and improve the tools, service providers, team-members, and processes of vulnerability scanning, penetration testing, source code testing, disaster recovery testing, anti-malware solutions, security event logs monitoring solutions, and incident response solutions.

8.2.5.12. Shall periodically communicate the comprehensive information security risk posture to the FBR IT Wing.

8.2.5.13. Shall participate in the technical evaluation of new products, projects, and upgrades with the objective of improving the FBR information security posture and addressing emerging threats.

8.2.5.14. Shall ensure compliance and governance of the information security program of IT Supplier/PRAL.

8.2.5.15. Shall exercise periodic risk and compliance checks within all domains of the FBR nation-wide information security governance, risk, and compliance (GRC) program, including information and cyber security threat and risk assessment, risk remediation, governance, and tracking reports to IT Wing, defining the assets in the scope of the information security program, access control and multi-factor authentication, network security, application security, infrastructure security, databases and data storage security, IT disaster recovery planning, information security service provider management and compliance, information security testing and tracking the remediation of findings, human resource security, end-user security awareness program, IT administrator security awareness program, operational security, and physical and environmental security of paper media and buildings/facilities.

8.2.6. Data Stewards

Data Stewards are the subject-matter experts of IT Supplier/PRAL within their specific domain. They are responsible for managing the operational aspects of data governance, ensuring adherence to the data governance policies, standards, and procedures. Reporting directly to the Chief Data Governance and Management (CDGM), Data Stewards are categorized into two primary types:

Business Data Stewards: These stewards typically hold roles such as Chief Information Officer (CIO), Chief Operating Officer (COO), or other IT Executive roles. They focus on alignment of data governance with business strategies and objectives.

Technical Data Stewards: These stewards often occupy positions like Chief Manager or IT Managers, and concentrate on the technical aspects of data management, ensuring data quality, and compliance with technical standards and procedures.

Responsibilities:

8.2.6.1. Shall execute the data governance standards and procedures within their departments, aligning with the overall organizational strategy.

8.2.6.2. Shall report data-related issues to the CDGM and communicate decisions and actionable items to their teams.

8.2.6.3. Shall identify and classify critical data assets within their domain, upon approval by CDGM, ensuring compliance with data management standards and procedures, and quality requirements.

8.2.6.4. Shall be responsible for adherence to data management standards and procedures defined by FBR within their department.

8.2.6.5. Shall escalate all data-related issues to the CDGM in accordance with defined standards and procedures of FBR.

8.2.6.6. Shall advise on and propose criteria for data access management within their domains.

8.2.6.7. Shall collaborate in developing business data glossaries and rules, submitting these for approval to the Chief Data Governance and Management (CDGM).

8.2.6.8. Shall enforce data quality standards and procedures to monitor data quality within their domain.

8.2.7. Information Security Stewards

Information Security Stewards are subject-matter experts in information security within IT Supplier/PRAL, focusing on the security aspects of data and information within their specific domain. Reporting directly to the Chief Data Governance and Management (CDGM), they ensure that information security practices are in alignment with information security standards and procedures set by FBR. These stewards are divided into two primary types:

Business Information Security Stewards: These stewards typically holding positions such as Information Security Manager or other related executive roles. They concentrate on aligning information security initiatives with business objectives and strategies.

Technical Information Security Stewards: These stewards often occupy positions such as IT Security Managers, or other related roles. They focus on the technical implementation of information security measures, ensuring compliance with security standards and procedures.

Responsibilities:

8.2.7.1. Shall implement and oversee information security standards and procedures within their departments, ensuring these align with the information security policies set forth by FBR.

8.2.7.2. Shall report security-related issues and incidents to the Chief Data Governance and Management (CDGM) and communicate decisions and necessary actions to their teams.

8.2.7.3. Shall identify and classify critical information assets within their domain. Upon approval by the CDGM, they ensure these assets comply with information security management standards and procedures, as well as quality requirements.

8.2.7.4. Shall be responsible for ensuring adherence to information security management standards and procedures defined by FBR within their department.

8.2.7.5. Shall escalate all information security issues to the Chief Data Governance and Management (CDGM) as per the defined standards and procedures of FBR.

8.2.7.6. Shall advise on and propose criteria for information access management within their domains, ensuring secure and compliant access to data and information.

8.2.8. Data Custodians

Data Custodians include the operational staff of IT Supplier/PRAL such as Business Analysts, Database Administrators (DBAs), and other key operational staff. Their role is instrumental in the practical aspects of data management, encompassing data creation, capture, processing, storage, backup, and archival/dissemination.

Responsibilities:

8.2.8.1. Shall manage all systems within their scope, ensuring compliance with pre-mandated best practices, standards and procedures.

8.2.8.2. Shall handle all change requests for their respective systems, ensuring proper documentation and alignment with data governance policies, standards, and procedures.

8.2.8.3. Shall develop and implement use cases for datasets under their domain, under supervision of their respective Data Stewards.

8.2.8.4. Shall implement data quality controls for their systems.

8.2.8.5. Shall maintain awareness of and adhere to policies, standards and procedures related to their data responsibilities.

8.2.8.6. Shall provide technical input to data quality issues identification and execute data quality remediation as required.

8.2.8.7. Shall ensure the documentation and timely updating of data lineage for transparency and traceability.

8.2.8.8. Shall assist departments in developing business data glossaries and rules by providing suggestion and promoting a consistent understanding of data across the organization.

8.2.8.9. Shall execute data rules, definitions, processes, guidelines, data standards and procedures for data domains and systems under their custody.

8.2.8.10. Shall communicate any adverse impact on the systems to relevant Data Steward.

8.2.8.11. Shall ensure data compliance, storage, and quality, managing data access responsibly.

8.2.9. Information Security Custodians

Information Security Custodians consist of operational staff of IT Supplier/PRAL, such as IT Security Analysts, Network Security Administrators, and other key security operational staff. They play a pivotal role in the practical aspects of information security, including the implementation of security measures and maintaining the security of data throughout its lifecycle.

Responsibilities:

8.2.9.1. Shall manage all security systems and infrastructure within their scope, ensuring compliance with mandated standards and procedures for information security.

8.2.9.2. Shall handle security change requests for their respective systems, ensuring proper documentation and alignment with information security policies, standards, and procedures.

8.2.9.3. Shall develop and implement security use cases for systems under their domain, under the supervision of their respective Information Security Stewards.

8.2.9.4. Shall implement and monitor security controls for their systems to safeguard data against unauthorized access, breaches, and other security threats.

8.2.9.5. Shall maintain awareness of and adhere to information security policies, standards, and procedures related to their responsibilities.

8.2.9.6. Shall provide technical expertise in identifying and remediating security vulnerabilities and incidents.

8.2.9.7. Shall ensure the documentation and timely updating of information security measures and incidents for transparency and accountability.

8.2.9.8. Shall communicate any adverse security incidents or risks to the relevant Information Security Stewards.

8.2.9.9. Shall ensure compliance with information security protocols, managing access to sensitive data responsibly and maintaining the confidentiality and integrity of the data according to the information security policies, standards, and procedures.

8.3. Reporting and Escalation Procedure

Level	Responsibility	Action/Reporting	Escalation Criteria	Communication Channel(s)
Level 1	Data Custodians/Information Security Custodians	Regular reports on data quality, security incidents, compliance status Initial identification and handling of data related issues	Regular reports on data security incidents and handling routine security incidents.	Written reports and emails to Data/Information Security Stewards.
Level 2	Data Stewards /Information Security Stewards	Regular reports on data quality, compliance status, and oversight of Custodians' activities. Initial identification and handling of data-related issues. Initial identification and handling of data and security-related issues.	Minor issues in data quality or policy adherence. Escalated security incidents from Custodians.	Written reports and emails to the Chief Data Governance and Management (CDGM).
Level 3	Chief Data Governance and Management (CDGM)	Reviewing reports from Data/Information Security Stewards. Addressing escalated issues from Stewards.	Significant data quality concerns, policy breaches, recurring or complex security incidents.	Meetings with Stewards. Email or direct communication with Member IT if needed.
Level 4	Member IT	Involvement in high-level data governance issues. Decision-making on resource allocation and policy.	Systemic challenges in data governance. Major security breaches or compliance failures.	High-level meetings. Briefings to Chairman FBR/Board-in-Council.

The Data Governance Policy establishes a clear reporting and escalation procedure to address issues and challenges effectively:

- **Regular Reporting:** Data and Information Security Stewards are required to provide regular reports to the CDGM. These reports include updates on data quality, security incidents, and compliance status.
- **Escalation Path:** In case of data governance issues, such as breaches of policy or data quality concerns, there is a defined escalation path. Issues are first raised with the relevant

Stewards, then escalated to the Chief Data Governance and Management (CDGM), and then to the Member IT. If necessary, the case shall be escalated to Chairman FBR who has the final authority in these matters.

- **Documentation and Review:** All reports and escalations are documented. The Data Governance Office periodically reviews these reports to assess the effectiveness of data governance and make necessary adjustments.

This operating model ensures that data governance is a shared responsibility across the organization, with a structured approach to managing, reporting, and escalating data-related issues. It fosters a culture of accountability and continuous improvement in data governance practices.

9. Core Data Policies

9.1. Data Quality Management Policy

Policy Statements

Having an effective Data Quality policy is vital in the current digital landscape that relies on data-driven decision making. It ensures that the data is accurate, reliable and can be queried to extrapolate useful insights. This will facilitate strategic decision-making and optimize resource allocation on data correction. Relevant stakeholders and responsible officers across organizations need to ensure that:

9.1.1. Data should be relevant to the purpose for which it is used.

9.1.2. Data is sufficiently accurate for its intended purpose.

9.1.3. Data is clearly represented in detail and collected as close to the site of activity as possible.

9.1.4. Data is processed in conformance with relevant requirements, rules, and definitions to ensure integrity and consistency.

9.1.5. Data processes are defined to ensure consistency and comparability of data over time.

9.1.6. Systems and processes for data handling are scalable to accommodate growth and changes in data volume, variety, and velocity.

9.1.7. Data is complete, representative, unbiased, and should not contain redundant or duplicated records.

9.1.8. Data is made accessible to authorized users in a format that is easily understandable and usable, while maintaining security and privacy standards.

9.1.9. Data is compatible with and can be integrated into other systems or applications, enhancing its utility across different platforms.

9.1.10. Cost and effort for the data collection is according to the importance of data, timeliness requirements, and needed accuracy.

9.1.11. Data is safeguarded with appropriate security measures to prevent unauthorized access and ensure data confidentiality.

9.1.12. Data is collected immediately after a relevant event has occurred and is available for use and analysis within a reasonable timeframe.

9.1.13. Metrics are created for measuring data quality and regular reporting mechanisms to monitor these metrics over time.

9.1.14. Mechanisms are developed for early detection and correction of data anomalies and inconsistencies.

9.1.15. Automated tools are and systems are utilized for continuous data quality checks and validations.

9.1.16. There are clear processes and responsibilities for resolving data quality issues as they arise.

9.1.17. Periodic review of data is carried out to reflect changing needs.

9.1.18. Volume of data reflects the value gained from it.

9.1.19. Sufficient data of suitable quality is collected to ensure that meaningful conclusions are drawn.

9.1.20. A feedback loop is in place, involving users and data managers to constantly refine and enhance data quality.

9.2. Master and Reference Data Management Policy

Policy Statements

Having an effective Master and Reference Data Management policy is vital in the current digital landscape where there is a need for data consistency throughout the organization. Data consistency ensures that all operational processes run effectively. This will facilitate master and reference data being managed properly to allow a unified view of the data across all the systems present. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.2.1. Data ownership is defined to specify who will be responsible for managing master and reference data elements to ensure accountability and traceability.

9.2.2. Data quality and accuracy measures are defined for both master and reference data.

9.2.3. Classification of both master and reference data are based on sensitivity levels to allow for effective handling.

9.2.4. Processes are in place to ensure synchronicity among all the master and reference data elements across all systems.

9.2.5. Version control mechanisms are implemented for master and reference data to trace lineage, track changes, and auditing the data.

9.2.6. Regular audits are carried out to ensure that master and reference data are adhering to best practices.

9.2.7. All reference data sets are sourced, and defined in a consistent manner, to facilitate standardization.

9.2.8. There are processes in place to check master data records across all major systems in the organization to verify consistency between them.

9.2.9. There are processes in place to support continuous improvement in management of master and reference data, based on regular feedback and audits.

9.2.10. There are clear standards and procedures for the interoperability of master and reference data across diverse systems and platforms.

9.2.11. A disaster recovery plan is in place that specifically addresses the recovery and continuity of master and reference data.

9.2.12. Data management processes are applied to both reference and master data.

9.2.13. There is engagement with stakeholders to review and update master and reference data management practices in line with evolving business needs.

9.3. Metadata Management Policy

Policy Statements

Having an effective Metadata Management Policy is vital with the emergence of complex data architectures. It ensures cataloging and maintenance of metadata such as source and format, to provide context about the data within/associated with the organization. This will facilitate a better comprehension about data entities, their connections throughout the organization, and their integration across multiple systems to allow for improvement. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.3.1. All metadata is in accordance with defined data standards to ensure consistency across all datasets.

9.3.2. All metadata is in accordance with defined data standards to ensure consistency across all datasets.

9.3.3. Data custodians are responsible for creating and maintaining the metadata relating to their respective datasets.

9.3.4. All metadata is regularly updated to showcase the changes in data structures, sources, or any relevant information.

9.3.5. Metadata, at least, includes a title, description, source, format, owner, and access rights.

9.3.6. Metadata containing vulnerable or confidential information is secured in accordance with FBR's security policy.

9.3.7. For vulnerable or confidential datasets, access to metadata must be restricted to only authorized users.

9.3.8. Periodic reviews are carried out to ensure accuracy, relevance, and completeness of compliance.

9.3.9. All updates, changes, or risks involving metadata are comprehensively documented for audit purposes.

9.3.10. Metadata includes the department/individual responsible for the dataset.

9.3.11. Metadata includes information on the relationships and dependencies between different data sets.

9.3.12. Description given in the metadata is detailed- including explanation of the dataset, its purpose, information, and use.

9.3.13. Metadata is maintained in a format that promotes interoperability across different systems and platforms within the organization.

9.3.14. Metadata structures are scalable and flexible enough to accommodate evolving data needs.

9.3.15. Collaboration exists between departments to guarantee consistency and accuracy of metadata across the organization.

9.3.16. Automated tools are utilized for metadata generation and capture to increase efficiency and reduce manual errors.

9.3.17. Regular training is provided to employees to ensure awareness and compliance of Metadata Management policies.

9.3.18. Any cases of non-compliance with the metadata policies have immediate action taken towards it, in accordance with FBR policies.

9.3.19. Periodic reviews of the metadata policies are conducted to integrate modern/future technology, data management techniques/practices, and organizational requirements.

9.4. BI and Data Warehousing Policy

Policy Statements

Having an effective BI and Data Warehousing Policy is vital with increasing amounts of data being produced or collected by an organization. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.4.1. Data integration pipelines are developed that support FBR's "broadening of tax base" initiative and improve accuracy in tax collection and fraud detection.

9.4.2. Implementation of data quality measures are supported during the preprocessing of data to ensure that data stored in the warehouse is accurate, complete, and reliable.

9.4.3. Emphasis is placed on the need for security controls within the data warehousing and Business intelligence environments.

9.4.4. Standardized data integration methodologies are adopted, and enforcement of the defined best practices to ensure that data from source systems is efficiently loaded and transformed.

9.4.5. Data handling practices comply with national and international laws and regulations regarding data privacy, financial reporting, and taxation.

9.4.6. Data is integrated from various enterprise-level sources, to ensure standardization across different systems and departments.

9.4.7. Post-integration data quality checks are implemented to ensure ongoing accuracy and integrity of data within the data warehouse.

9.4.8. Strict user access controls and authentication mechanisms are implemented to regulate access to data in the warehouse, ensuring that only authorized personnel can view or manipulate sensitive data.

9.4.9. Organization stays updated with emerging technologies and trends in BI and data warehousing, assessing, and adopting innovations that can enhance analytical capabilities and data processing efficiency.

9.4.10. There is scalability to accommodate for increasing volume of data, which includes supporting optimized mechanisms for large-scale processing with minimal latency.

9.4.11. Data Warehousing solutions shall physically operate within environments approved by higher authorities and existing legislations.

9.4.12. There is clarity, accountability, and consistency in how enterprise data is managed, used, and shared within FBR and/or with external entities.

9.4.13. Enterprise data warehouse effectively supports decision-making and strategic objectives at the enterprise level through effective implementation and integration of ETL processes.

9.4.14. Scalable storage solutions and data management practices are implemented that can dynamically adjust to the fluctuating volumes of data.

9.4.15. Data management infrastructure can scale efficiently to handle Big Data workloads, accommodating rapid data growth while maintaining performance and reliability.

9.4.16. Storage solutions and processing frameworks are adopted, that are optimized for Big Data, such as distributed file systems and parallel processing architectures.

9.4.17. Advanced data visualization tools are leveraged, making complex data more accessible, understandable, and actionable for decision-makers.

9.4.18. There is a structured project lifecycle for Data Science initiatives, encompassing problem definition, data collection and preparation, model building, evaluation, and deployment.

9.4.19. Processes for the selection of appropriate data for analysis are established, prioritizing data sources based on relevance, quality, and potential to impact analytics goals.

9.4.20. Data mining techniques are employed to validate hypotheses and extract meaningful insights, leveraging statistical models and machine learning algorithms to identify patterns, trends, and signals within the data.

9.4.21. Continuous exploration and integration of new data analytics models, techniques, and tools are pursued.

9.4.22. Ethical guidelines for AI and data science models are developed and adhered to, addressing issues of bias, fairness, transparency, and accountability in model development and deployment.

9.4.23. Data science models are compatible with and can be integrated into existing business systems, applications, and workflows.

9.5. Document and Content Management Policy

Policy Statements

Having an effective Document and Content Management Policy is vital with the increasing need of managing and maintaining a vast number of documents and content produced by an organization. This ensures a systematic approach when it comes to lifecycle management for these documents to facilitate operations and knowledge sharing. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.5.1. Documents are stored with relevant information such as data, version number, classification label.

9.5.2. Consistent naming conventions are followed throughout the organization, so that employees can easily identify the nature of accessible documents.

9.5.3. Documents are shared from a centralized location (Shared Drive, Online Repository) that is accessible to all relevant users, instead of sending them through emails, messages, and other informal means.

9.5.4. Documents are taken off site when not actively in use. This data needs to be encrypted and stored in a password protected storage area.

9.5.5. Usage of digital signatures for official documents to authenticate authorship and approvals.

9.5.6. Editing access to documents is based on roles and responsibilities to maintain content integrity and prevent unauthorized changes.

9.5.7. Documents are stored in a searchable format with proper indexing to facilitate quick retrieval.

9.5.8. Storing of any type of documents on personal online storage drives is prohibited.

9.5.9. Version control systems are implemented to track changes in documents over time, ensuring that the latest versions are readily available and previous versions are archived properly.

9.5.10. Only necessary drafts of important documents are stored to avoid redundancy.

9.5.11. Formal documents that will be subjected to change/improvements throughout their lifecycle, include a revision history that includes the changes made, where, and the individual responsible for the changes.

9.5.12. Standardized templates are used for common document types to ensure consistency and professionalism across organizational communications.

9.5.13. Final versions of documents are stored in the same format across the organization whether that be docx, pdf or any other agreed upon format.

9.6. Data Integration and Interoperability Policy

Policy Statements

Having an effective Data Integration and Interoperability Policy is vital with the advent of integrated systems being utilized to manage processes within an organization. This ensures that different data systems and applications can communicate with one another and work effectively to facilitate seamless data flow and reliability throughout the organization. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.6.1. Identification of all data assets is done using unique identifiers that can then be used for referencing and tracking lineage.

9.6.2. Identifier schemes are managed by relevant groups, who are responsible for updating and maintaining these identifiers.

9.6.3. Data assets within the organization are created, collected, processed, and disseminated using defined data standards and procedures.

9.6.4. A business glossary is created, and maintained that includes common data-jargon, to ensure cohesive understanding throughout the organization.

9.6.5. Data across all assets is standardized in agreed-upon formats to enable distribution within/outside the organization or exchange.

9.6.6. Strategies are developed for the integration of legacy systems, ensuring they can effectively communicate and exchange data with newer systems.

9.6.7. Processes are created for assessing the quality of the integrated data to ensure its accuracy and validity.

9.6.8. Standardized data exchange protocols are enforced across all systems to ensure seamless interoperability and data integration.

9.6.9. Thorough testing and validation of data integration processes are mandated to confirm data integrity, accuracy, and functional interoperability.

9.6.10. Consistent data format and encoding standards and procedures are enforced across all systems to facilitate smooth data integration and prevent data loss or corruption.

9.6.11. Regular interoperability assessments are conducted for all systems to identify potential integration issues and plan for future upgrades or changes.

9.6.12. Security and privacy controls are implemented for all data integration processes, so sensitive data is properly protected.

9.6.13. Requirements are defined to facilitate data sharing with other entities, while ensuring that it does not go against defined metrics, standards and procedures for proper data sharing.

9.7. Data Security Policy

Policy Statements

Having an effective Data Security Policy is vital with the increasing number of security related incidents. It ensures that data is protected against unauthorized access and breaches through standards and practices that facilitate confidentiality, integrity and availability of data to develop trust from within the organization, as well as stakeholders and the general public. The policy statements with regards to Data Security are as follows:

- Encourage all employees, contractors, trainees, consultants, third party providers and vendors to share the commitment to provide appropriate levels of security and continuity across all functions that hold organization and customer information.
- Encourage employees, contractors, trainees, consultants, third party providers and vendors to share the obligation to keep information secure, assure privacy, and remain active in prevention of unauthorized or corrupt activity.
- Develop, implement, and improve security framework policies to enforce and monitor compliance to best global security controls, practices, regulations and other requirements.
- Provide required resources for establishing data security objectives in line with policy and continual improvement of the security system.
- Mandate that requirements of the data security policy and related present and future security policies are compulsory across all functions to ensure compliance with best practices.

9.7.1. **Network based policies:**

9.7.1.1. User sessions for administering infrastructure use the latest encrypted channels.

9.7.1.2. User network remains separate from server network infrastructure.

9.7.1.3. Infrastructure equipment is integrated with vulnerability scanners to ensure that scans are regularly performed.

9.7.1.4. Encryption and hashing are implemented to ensure confidentiality and integrity of information passing over the network.

9.7.1.5. Access is provided to diagnostic ports only to relevant teams and should be secured.

9.7.1.6. Ports and services not required for business activity or functionality are disabled or removed.

9.7.1.7. Management interfaces of network devices are connected to a separate, dedicated, management network.

9.7.1.8. Users' access to publicly published services are protected via web application firewalls.

9.7.1.9. Trust relationships between systems are avoided as they are a security risk.

9.7.1.10. Principle of least privilege is implemented for all business and technical functions.

9.7.1.11. Audit trails are enabled for all transactions and activities.

9.7.2. **Database security policies:**

9.7.2.1. Access to database systems follow access control practices as stated in the data usage policy.

9.7.2.2. Changes and modifications in databases follow defined standards and procedures.

9.7.2.3. Database connections are only created through proper authorization channels.

9.7.2.4. Database servers are physically secured.

9.7.2.5. Default/Superuser accounts are disabled after initial setup.

9.7.2.6. Users are prohibited from saving the content of the database on local drives of their devices.

9.7.2.7. Authorization is required to restore databases which follow formal standards and procedures for restoration and should be documented.

9.7.2.8. Database access shall be provided based on the principle of least privilege.

9.7.2.9. Database fields with confidential information are properly masked.

9.7.2.10. Database usernames and passwords are stored separately in a non-readable/writable file from the executing body of a program code.

9.7.3. **Application security policies:**

9.7.3.1. Static and dynamic code reviews are performed for all applications.

9.7.3.2. OWASP top ten vulnerabilities are fixed on priority.

9.7.3.3. Stress testing is performed based on need and exposure of the application.

9.7.3.4. Frequent Vulnerability Assessment and Penetration testing (both Internal and External) are performed for all critical applications, and all vulnerabilities are tracked and remediated in a timely manner.

9.7.3.5. Root privileges are disabled.

9.7.3.6. Applications are published and protected using WAF.

9.7.4. **Data encryption policies:**

9.7.4.1. Custom encryption algorithms and technologies are prohibited.

9.7.4.2. Password protection and encryption is used to keep confidential data secure over email messages.

9.7.4.3. File transfer programs such as secure FTP and SCP are used when transferring documents and data over the network.

9.7.4.4. Full disk encryption is used to protect sensitive data on devices.

9.7.4.5. Encrypted files are unlocked for anti-virus scans.

9.7.4.6. Servers and applications using SSL or TLS have certificates signed by trusted providers.

9.7.4.7. Confidential information stored on portable devices are encrypted using defined methods.

9.7.4.8. Web servers use secure transmission protocols such as HTTPS.

9.7.4.9. Mobile applications are configured with public certificates.

9.7.4.10. Cryptographic keys are secure from unforeseen circumstances such as loss, theft, or compromise throughout the lifecycle.

9.7.4.11. Key exchanges use approved cryptographic protocols.

9.7.4.12. Certificates are issued from trusted third-party providers.

9.7.4.13. Certificates for intranet servers are created by trusted authorities.

9.7.4.14. Certificates from internal CA are issued for a predetermined period.

9.7.4.15. Certificates and keys generated via certificate authority should be backed up.

9.7.5. **Endpoint security policies:**

9.7.5.1. All endpoints have endpoint protection software installed on them.

9.7.5.2. Endpoint protection software is set to be automatically updated to the latest malware definitions.

9.7.5.3. Disabling or tampering with endpoint protection software is prohibited.

9.7.5.4. Media from unknown sources is scanned for malware/viruses.

9.7.5.5. If automatic updating is not possible, the end user is responsible for regularly scanning and updating endpoint protection software after consulting with relevant departments.

9.7.5.6. Endpoint Protection software is configured to scan downloaded files from external sources to prevent infected files.

9.7.5.7. Software maintains a log of all occurring scans.

9.7.5.8. Software is configured to scan web pages for malwares.

9.7.5.9. Software automatically scans, clean, and remove malicious codes and files. Infected devices should be removed from FBR's private network until confirmed as safe.

9.7.5.10. Employees take reasonable initiatives to protect against malicious software and must always scan media before using.

9.7.5.11. Activities with the intention of creating and/or distributing malicious programs into FBR's network are strictly prohibited.

9.7.5.12. Endpoints with low specifications are updated with approved anti-malware software.

9.7.5.13. Guests connecting to the FBR network should connect to a separate guest network.

9.7.5.14. Third party contractors working with FBR for longer periods must install proper and approved endpoint protection software.

9.7.5.15. Endpoints shall automatically be locked after a certain time limit of inactivity.

9.7.6. **Log Management policies:**

9.7.6.1. Every Network element deployed in FBR infrastructure generates event logs for review and analysis.

9.7.6.2. The following must be logged where available:

9.7.6.2.1. Security: Security event information such as authentication failure, attempts, access and policy changes.

9.7.6.2.2. Application: Will vary.

9.7.6.2.3. System: Operational actions by Operating system components.

9.7.6.2.4. Logs for additional information that can vary per department must also be generated.

9.7.6.3. Critical systems, applications, databases and network devices must be integrated with SIEM for transmission of security logs.

9.7.6.4. Logs must be stored, retained, and removed as per defined rules, regulations and legal compliances.

9.7.6.5. Archived log period can be changed according to business, legal, and regulatory requirements and must be pre-approved by the CDGM.

9.7.6.6. Logs of servers, applications, databases, and network devices are retained on SIEM for a defined minimum number of days before archival and maintenance for another defined minimum number of days.

9.7.7. **Patch Management policies:**

9.7.7.1. System and network administrators/owners are responsible for being aware of new patch releases.

9.7.7.2. System and network administrators/owners ensure that versions of operating systems are upgraded on a regular basis so that they remain within a valid support lifecycle.

9.7.7.3. Patch stabilization is ensured when installing the latest patches.

9.7.7.4. If upgrading to the recommended version is not feasible, pre-approved alternate controls are applied.

9.7.7.5. Third-party related patches are applied as per patch priority and significance.

9.7.7.6. All new patches are reviewed, evaluated and tested by administrators.

9.7.7.7. A maintenance window is agreed upon for every week where relevant patches shall be applied after identification and testing.

9.7.7.8. If a patch is considered critical, then it should be installed immediately if exploits have occurred. If, however, exploits have not occurred, installation can wait.

9.7.7.9. Patches are installed from trusted sites.

9.7.7.10. Patch management teams must document all patch activities including monitoring, reviewing, testing, and installation.

9.7.7.11. Systems facing more threats or vulnerabilities must be accorded a higher priority in the patch management process.

9.7.7.12. If an emergency patch needs to be applied which may lead to loss of revenue or downtime, it must be declared as critical and applied to all managed systems on the network.

9.7.7.13. Logs are reviewed to keep track of systems and verify that patches have been installed.

9.7.7.14. Audit assessments take place to confirm that the latest patches are deployed across systems and applications.

9.7.7.15. Compliance and consistency protocols are in place to ensure that controls are in place for deployed and/or rebuilt systems that are up to date with the latest patch levels.

9.7.7.16. System built tools are applied where appropriate to assist with compliance and ensure updated patches are deployed.

9.7.8. **Physical Security policies:**

9.7.8.1. All entry points are secured with necessary access control mechanisms.

9.7.8.2. A robust visitor management system is implemented; visitors must be logged, provided with tags, and escorted when necessary.

9.7.8.3. Access is restricted to sensitive areas; authorized personnel should escort the visitors.

9.7.8.4. Biometric verification is installed at data centers to prevent unauthorized access.

9.7.8.5. CCTV cameras are installed strategically to monitor and record activities.

9.7.8.6. Main entry doors are monitored by CCTV accessed and monitored by administration.

9.7.8.7. CCTV recordings are retained for up to three months with access provided to authorized personnel or as per need and permission.

9.7.8.8. CCTV monitoring log sheets are updated daily/compiled monthly and submitted to relevant authorities.

9.7.8.9. Trained personnel are present for patrolling the premises with regular briefing and training.

9.7.8.10. Critical equipment is secured in locked storage areas with regular asset audits.

9.7.8.11. Contingency plans are in place for potential breaches.

9.7.8.12. Standards and procedures are implemented for reporting security breaches with a designated response team handling the investigation.

9.7.8.13. Regular audits are carried out for physical security measures.

9.7.8.14. Employees are trained in physical security protocols and best practices ensuring a security conscious culture.

9.8. Data Privacy and Protection Policy

Policy Statements

Having an effective Data Privacy and Protection Policy is vital to address privacy concerns of employees, stakeholders, and consumers. It ensures that explicitly defined controls are in place that guide the collection, handling, storage and sharing of Personally Identifiable Information (PII), according to legal and ethical standards. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.8.1. There is appropriate privacy and protection of information through secure handling techniques such as classification and cryptography.

9.8.2. Only the minimum necessary amount of personal information is collected, used, and stored, in line with the data minimization principle.

9.8.3. Clear standards and procedures for handling requests from data subjects, such as access requests, right to be forgotten, and data portability are established.

9.8.4. Clear and transparent privacy notices are provided to users about how their data is collected, used, and shared.

9.8.5. Information is only released on a need-to-know basis to individuals authorized to use such information.

9.8.6. Critical data and information are tailored to a specific requirement before release.

9.8.7. Critical data and information are kept secure and used for specific business purposes for which authorization must be obtained.

9.8.8. Electronic files containing critical data and information reside within protected information systems. FBR's documents containing such information are not printed.

9.8.9. Physical files containing personal information reside within a locked file cabinet or room when not being used.

9.8.10. Critical data and information are not to be downloaded onto personal, employee, or contractor systems or those not being protected by FBR.

9.8.11. Critical data and information are not sent through personal email.

9.8.12. Critical data and information are not sent to publicly available email systems.

9.8.13. Information is not disclosed after termination of an employee under any circumstances.

9.8.14. Disposing of such data, physical files are shredded, and electronic files are deleted as per disposal process.

9.8.15. Critical data and information are provided to third parties with strict requirements of security and use for specific authorized business purposes as contracted.

9.8.16. If breaches occur, the relevant authorities are informed within a certain timeframe with the affected party being notified based on management's discretion.

9.8.17. Consent is obtained from the user about collecting and processing data.

9.8.18. Discrepancies are identified, users have the right to have their information updated/corrected.

9.9. Data Storage and Operations Policy

Policy Statements

Having an effective Data Storage and Operations Policy is vital when it comes to managing the organization's digital infrastructure. It ensures that there are protocols in place that facilitate the effective storage, handling and maintenance of data assets as well as being extensible to handle increasing volumes and new formats of data. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.9.1. Data classified as confidential or internal is only stored in pre-approved locations and on pre-approved equipment.

9.9.2. Data is stored on electronic media for sustainability and extensibility. This would also allow better levels of security, accessibility and backup capability.

9.9.3. The following Electronic Data Storage policies are enforced:

9.9.3.1. Standards and procedures are established for storing digital data and are reviewed at regular intervals to gauge their need.

9.9.3.2. Temporary copies of digital data are reviewed at regular intervals to gauge their need.

9.9.3.3. All data related to operational processes within the organization are stored in a shared storage accessible to all employees and subject to certain access control mechanisms.

9.9.3.4. All confidential files are kept in a private repository and shared "on-need" basis, after the formal request approval.

9.9.3.5. Employees are not allowed to store personally identifiable information (PII) on shared storage, or company repositories unless explicitly required.

9.9.3.6. Any loss of data is reported through the proper channels and points-of-contacts need to be established.

9.9.3.7. Sensitive data storage on servers or in data centers require authentication controls to be put in place.

9.9.4. The following Non-Electronic Data Storage policies are enforced:

9.9.4.1. Standards and procedures are established for storing hardcopy data and are reviewed at regular intervals to gauge their need.

9.9.4.2. Anything hand-written is stored securely and recycled once data is no longer required.

9.9.5. Any backed up data that loses usability or does not contribute to existing processes after a certain period are either subject to disposal policy or get stored to an offsite location.

9.9.6. The need to retain different datasets at their respective locations is periodically reviewed.

9.10. Data Modeling and Design Policy

Policy Statements

Having an effective Data Modeling and Design Policy is vital when it comes to the structuring and organizing of data. It ensures that best practices are undertaken to create data models, represent business entities, their relationships and processes associated with them. This allows the organization to facilitate effective storage, retrieval and analysis of these datasets. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.10.1. High level data concepts, definitions, and relationships are defined.

9.10.2. Data modeling must align with organizational goals and requirements.

9.10.3. Data models are regularly updated and revised to reflect changes in business processes, requirements, and technological advancements.

9.10.4. Logical data models are developed in accordance with industry standard notations.

9.10.5. Data models are regularly updated and revised to reflect changes in business processes, requirements, and technological advancements.

9.10.6. Validation and testing processes for data models are implemented to ensure accuracy and effectiveness before deployment.

9.10.7. Attributes, types, and constraints of data must be documented.

9.10.8. Logical data models should be mapped onto physical storage structures.

9.10.9. Performance, scalability, and optimization is always considered while modeling.

9.10.10. Cost-effective data modeling practices are used that take into consideration resource utilization and budget constraints.

9.10.11. Data models are aligned with the organization's data warehousing and business intelligence strategies to facilitate efficient data analysis and reporting.

9.10.12. Modeling of data is done in collaboration with database administrators.

9.10.13. Normalization principles are followed since they are currently using relational database management systems (RDBMS).

9.10.14. Proper indexing is implemented for improved performance.

9.11. Data Usage Policy

Policy Statements

Having an effective Data Usage policy is vital when it comes to defining how data is accessed, shared and utilized to support operational and business processes. It ensures that there are guidelines in place to facilitate proper management, data access controls, sharing protocols, prevention of data misuse and protection of data. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.11.1. Workstation and Computer Facilities:

9.11.1.1. Measures are taken to protect systems since information on portable systems is vulnerable.

9.11.1.2. PCs, laptops, workstations are secured with automatically activated, password-protected screensavers for when the host is unattended, or by logging-off or locking the system.

9.11.1.3. Compliance with applicable policies for patch management, anti-malware, and software installation policies is mandatory.

9.11.1.4. Passwords are kept secure, and accounts must not be shared.

9.11.1.5. System-level and user level passwords are changed periodically.

9.11.1.6. Workstations are used for authorized purposes only.

9.11.1.7. Laptops with vulnerable information are kept in physically secure storages such as locked drawers or cabinets.

9.11.1.8. Intranet facilities provided by the company are used over approved/ private broadband services where applicable.

9.11.1.9. Logging into computer/systems with admin rights is prohibited as these rights require proper approval from IT department.

9.11.1.10. Users should not uninstall anti-virus solutions.

9.11.1.11. Users must not use FBR's network to gain unauthorized access to any external system. Confidential and internal information must not be disseminated unless required for performing work duties.

9.11.1.12. External parties are not allowed access to FBR systems and networks without explicit permission by the respective head of department.

9.11.2. Email usage policy:

9.11.2.1. Emails are only opened from trusted sources.

9.11.2.2. Caution is taken while opening emails with potentially malicious attachments or URLs from unknown sources which may contain malware such as viruses.

9.11.2.3. Sending unsolicited email messages, including "Junk mail" or advertising material to individuals is prohibited except for explicit requests from the receiver.

9.11.2.4. Use of official Email IDs for postings on public forums/ groups/ forums, etc., is strictly prohibited.

9.11.2.5. Sending emails, potentially, compromising FBR's reputation is strictly prohibited.

9.11.2.6. Intentionally sending viruses or malware to any users is strictly prohibited.

9.11.2.7. Unauthorized use or forging of email headers is prohibited.

9.11.3. Internet and Network Activities:

9.11.3.1. Users are only authorized to visit permitted sites to facilitate security and integrity of data.

9.11.3.2. Users cannot install legal/illegal and unapproved software including viruses and cracking/hacking tools. For legal software installation, requests can be made to the relevant department.

9.11.3.3. All hosts connected to FBR's intranet, whether owned by the employee or FBR, are monitored at system and network level for security regulations by relevant departments.

9.11.3.4. Access is blocked to a website deemed to contain illegal, offensive, malicious, or inappropriate material.

9.11.3.5. Port scanning/ security scanning is prohibited unless prior notification to the security department is made.

9.11.3.6. Executing any form of network monitoring- intercepting data unintended for the employee's host is prohibited unless part of the normal job/duty.

9.11.3.7. Circumventing user authentication or security of any host/ account/ network is prohibited.

9.11.3.8. Making fraudulent offers of products/ items/ services from FBR accounts is strictly prohibited.

9.12. Data Access and Control Policy

Policy Statements

Having an effective Data Access and Control Policy is vital in defining guidelines and protocols governing "who" can access "what" data and the level of access given to departments and individuals. It ensures that providing access to data is done in a way to prevent unauthorized access, mitigate security risk, and reduce organizational risk. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.12.1. There is a formalized process for registering new users and granting/prohibiting access to informational resources. This would include:

9.12.1.1. Access authorization process whereby individuals and/or entities will be assigned credentials, and access levels, and resources that they have access to.

9.12.1.2. Modification of user access privilege whereby changes will be introduced to the existing permissions granted, based on change of role, expiry of rights, or exiting from the organization.

9.12.2. Effective measures of identification are employed to accurately identify personnel via a thorough login process. This could be via UserIDs, GroupIDs, TemporaryIDs or Group Membership.

9.12.3. Password Management policies are in place to mitigate the risk of information breach/leakages. This could include criteria for setting passwords, for technological systems within the organization.

9.12.4. Access control features are present so that users only have access to data and functions necessary to perform their duties. This could be through multiple avenues such as limit on login sessions, MFA, idle-session timeout, role-based access control, etc.

9.12.5. Requirements are established for data owners to periodically conduct reviews of accounts and assets under their domain to ensure that appropriate privileges are assigned to user/service accounts, and any unauthorized users are removed.

9.12.6. Requirements are established for requesting and approval of access to FBR's informational assets by third parties.

9.12.7. Instructions are provided after access is granted to ensure that the recipient will take responsibility for not disseminating information within/outside the organization.

9.12.8. Remote access to FBR's resources is managed through a pre-approved method of access.

9.12.9. Access via VPN, also requires their own set of policies to ensure that access to organizational assets from outside the organization is done in a way as to not allow for unauthorized access:

9.12.9.1. VPN users will have similar levels of access as granted for regular work.

9.12.9.2. Authorized users are to ensure that unauthorized users are unable to access company networks from personal devices.

9.12.9.3. Authorized users are responsible for malicious activities and misuse of company assets by the access provided to them.

9.12.9.4. Authorized users shall use private VPN to connect to FBR's network. Approval would be required for access.

9.12.9.5. Temporary, generic, or test accounts shall not be created.

9.12.9.6. Multi-factor authentication for authorized users would be used for VPN access.

9.12.9.7. Authorized users shall ensure protection of the credential provided to them for the VPN.

9.12.9.8. Users will be responsible for all activities carried out through their systems/devices while connected.

9.12.9.9. Authorized users will ensure that their devices are not physically shared with third parties for remote access.

9.12.9.10. Authorized users shall not share passwords of application/servers/networks with third parties during remote access sessions.

9.12.9.11. Maintenance work such as troubleshooting, updates and support for vendors through remote access by third party contractors will require approval from respective authorities. All hosts that connect via remote access should have updated anti-viruses installed.

9.12.9.12. Cracked or Hacked tools for remote access are forbidden.

9.12.9.13. Remote access tools will require multi-factor authentication if possible and feasible.

9.12.9.14. Remote access tools will ensure use of strong encryption techniques.

9.12.9.15. Security mechanisms such as antiviruses and data-loss prevention software shall not be disabled or altered under any circumstances.

9.12.9.16. Site to site VPNs established with third parties should have the latest encryption and hashing protocols.

9.12.10. Requirements are established to document, monitor and control wireless access to information systems:

9.12.10.1. Employees can access wireless networks after authentication and registering their devices that need to connect to the network. An upper limit should be set for the number of devices that can be registered for one person.

9.12.10.2. All wireless connectivity features (including Bluetooth, Wi-Fi, NFC, etc.) must be disabled by default on all organizational devices.

9.12.10.3. Activation of these features is permissible only for authorized purposes and on devices that have been approved by the CDGM.

9.12.10.4. Maintain a whitelist of authorized devices that are permitted to use wireless connectivity features within the organizational network.

9.12.10.5. Conduct regular audits to identify and remove unauthorized devices connected to the network.

9.12.10.6. Wireless access points should be approved by relevant authorities.

9.12.10.7. Use advanced encryption system protocols.

9.12.10.8. Enable WiFi protected access keys.

9.13. Data Destruction Policy

Policy Statements

Having an effective Data Destruction Policy is vital in managing the disposal and destruction of data assets when they become obsolete, redundant and/or non-compliant. This ensures that data is destroyed properly to mitigate risk of data leakage, data breaches and unauthorized access. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.13.1. Data destruction/disposal methods adhere to international data standards.

9.13.2. Secure data erasure methods such as cryptographic wiping or physical destruction for digital storage devices is implemented so that data cannot be recovered post-destruction.

9.13.3. Data destruction processes comply with legal obligations regarding taxpayer information.

9.13.4. Care is taken so no individual, or organization is adversely impacted by material that was not properly destroyed.

9.13.5. Secure methods are implemented for the destruction of physical records, such as shredding or incineration, in compliance with environmental standards and security protocols.

9.13.6. Emergency data destruction protocols are developed for scenarios where immediate destruction is required due to security breaches or legal mandates.

9.13.7. A record is kept of all data destruction activities including the method, medium, data and other information relevant to the process.

9.13.8. Asset wonders are trained in their relevant data destruction methods to ensure proper procedures take place.

9.13.9. In case of third parties, there should be agreements in place to ensure data disposal after a certain time period. Proof of disposal must be required.

9.13.10. Since data is taxpayer data, there needs to be transparency and communication with regards to taxpayer records being destroyed, or taxpayers wanting their data destroyed.

9.13.11. Notification system is established to inform relevant stakeholders, including taxpayers, about the scheduled destruction of their data, providing transparency in data handling.

9.14. Third-Party Data Access and Sharing Policy

Policy Statements

Having an effective Third-Party Data Access and Sharing Policy is vital in this current landscape where data exchange is an integral part of operational and business functions within the organization as well as external entities. It ensures that data sharing activities are conducted in a secure, effective, and compliant manner by protecting sensitive and proprietary information, maintaining data's integrity, monitoring and auditing data sharing practices of third parties and formalizing sharing agreements to protect the organization's interests. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.14.1. All third-party data conforms to their contractual obligations, that need to conform to data protection laws and regulations.

9.14.2. Prior to sharing data with third parties, risk assessments are conducted to evaluate their data security posture and compliance with data protection laws.

9.14.3. All data sharing with third parties is governed by formalized data sharing agreements that clearly outline terms of use, data handling, and protection requirements.

9.14.4. Third-party data access agreements are regularly reviewed and updated so they remain compliant with evolving data protection regulations and organizational policies.

9.14.5. Mechanisms are implemented for obtaining consent from individuals whose data is being shared and notify them about third-party data sharing practices.

9.14.6. Clear exit strategies are included in data sharing agreements, outlining standards and procedures for data return or destruction at the end of the contract or in case of contract termination.

9.14.7. Provisions are included to manage and monitor any subcontractors that third parties might use, ensuring they also adhere to the same data protection standards.

9.14.8. There is an emphasis on sharing only the minimum amount of data that is necessary with third parties.

9.14.9. Access control measures are implemented when granted access to data and need to be formalized and signed-off on.

9.14.10. Regular auditing of outgoing and incoming data to ensure that the process remains compliant.

9.14.11. Techniques such as encryption, anonymization, and masking, are employed, and are applied whenever possible to protect sensitive data.

9.14.12. Transparency exists with regards to data sharing practices within/outside the organization to ensure third-party and stakeholder trust.

9.14.13. In case of breach of data, or sharing of data with unauthorized entities, measures are in place to notify relevant individuals of this concern.

9.14.14. Data is continuously checked and monitored to confirm that it is in accordance with the agreed upon terms.

9.14.15. There are clauses for data destruction or retrieval upon termination of contract.

9.15. Incident Response Policy

Policy Statements

Having an effective Incident Response Policy is vital in the current landscape where data exchange and collaboration with external entities is prevalent. It ensures that there are guidelines, standards and procedures in place that facilitate proper mitigation tactics, automated activities, and reporting channels to reduce organizational risk in the case of a security incident. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.15.1. Data security incidents are promptly reported by users.

9.15.2. Data security incidents are reported, documented, and managed in a timely manner.

9.15.3. Data security incidents are handled by authorized employees.

9.15.4. System for classifying the severity of data security incidents is implemented to prioritize response and resource allocation.

9.15.5. Data security incidents are assessed by authorized authorities to determine a risk management plan.

9.15.6. Data security incidents are informed to relevant bodies.

9.15.7. Root cause analysis is conducted after incident resolution to identify underlying causes and prevent future occurrences.

9.15.8. Standards and procedures are implemented for forensic analysis and preservation of evidence post-incident to support investigation and legal actions.

9.15.9. Post-incident reviews are mandated to assess the response effectiveness and prepare detailed reports for management review.

9.15.10. Regular incident response drills and simulations are conducted to ensure readiness and effectiveness of the response plan.

9.15.11. Clear communication plan is developed for notifying internal and external stakeholders, including customers and partners, about significant incidents in an appropriate manner.

9.16. Data Providers Engagement Policy

Policy Statements

Having an effective Data Providers Engagement Policy is vital when there is a requirement to receive data from external parties to enhance the organization's business and operational processes. It ensures that there are protocols, standards and procedures in place when engaging with data providers to facilitate receiving data that is accurate, relevant, normalized, follows a fixed format and aligns with organizational standards. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.16.1. Only authorized individuals are allowed to interface with data providers.

9.16.2. There are established data processing agreements with data providers before any formal engagement.

9.16.3. Data providers are aware of and follow FBR's policies.

9.16.4. Guidance is provided to assist data providers in transferring data effectively to FBR.

9.16.5. Data providers are communicated to about how their data will be used, stored, and protected within FBR.

9.16.6. A feedback mechanism for data providers is established to report issues, suggest improvements, or provide input on data-related processes.

9.16.7. Procedures for prompt correction of any errors or inconsistencies in data provided by external parties are defined and implemented.

9.16.8. There are communication channels to provide support to assist data providers both for technical and logistical issues.

9.16.9. There is a formalized offboarding process in place, to discontinue access, after data providers are no longer authorized.

9.16.10. Data providers must adhere to data handling rules and will be accountable for maintaining data accuracy and integrity.

9.16.11. There is regular monitoring of data provider performance to ensure adherence to controls and processes set in place.

9.16.12. Periodic audits and assessments of data providers are conducted to verify their compliance with the agreement terms, data standards and procedures.

9.16.13. Data providers comply with data security standards and procedures set according to the organization's needs.

9.17. Data Classification Policy

Policy Statements

Having an effective Data Classification Policy is vital in the current information-rich environment, where being able to effectively label data with their proper categories allows for their proper management and handling. It ensures that there are guidelines and metrics in place to properly classify data, formalize relevant controls for each category to facilitate regulatory compliance and legal requirements, and define scope of responsibilities for the data assets. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.17.1. Multi-level classification labels are established, clearly defined, and their impacts accurately articulated, to maintain consistent data handling and security practices.

9.17.2. Standards and procedures are created and used for marking classified information.

9.17.3. Data is classified according to its levels of sensitivity and the potential impact of disclosure, corruption, alteration, and destruction of it.

9.17.4. Classification labels, standards and procedures are regularly reviewed and updated to reflect current data handling needs and regulatory changes.

9.17.5. A formal process is established for the de-classification of data when it no longer requires a high level of protection.

9.17.6. Classification levels are included as part of the digital metadata for electronic documents and files to facilitate easy identification and handling.

9.17.7. Data is protected according to sensitivity classification applied.

9.17.8. Any data providing identification of an individual or entity is considered confidential and would require explicit permission for disclosure.

9.17.9. The marking of classified documents is established as the responsibility of the author or originator of the information.

9.17.10. Holders of wrongly marked classified documents contact the originator to suggest correct marking. Originator shall be responsible for applying the suggestion or keeping the existing marking.

9.17.11. Labels for classification of documents should be color-coded.

9.17.12. The owner of data is responsible for maintaining reliability and completeness.

9.17.13. Formal processes are implemented for resolving disputes over data classification decisions, including escalation standards and procedures to higher authority if needed.

9.18. Data Backup, Retention and Recovery Policy

Policy Statements

Having an effective Data Backup, Retention and Recovery Policy is vital when there is a need to protect an organization's critical data assets that are an integral part of their operational and business functions. It ensures that there are effective strategies to mitigate threats associated with critical data loss from human error, machine failure or security events, as well as processes to test backup and recovery methods and systems. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.18.1. Minimum controls required for backups of systems and data to meet organizational needs are defined.

9.18.2. Administrators perform regular backups of servers, applications, and databases prioritized by a defined criticality classification, ensuring high-criticality systems are backed up with higher frequency in accordance with business requirements.

9.18.3. Records of the backup copies including logs, system, applications, types, frequencies, date, and time as well as restoration standards and procedures are documented.

9.18.4. Backup media is classified, labeled, and given appropriate levels of physical and environmental protection consistent with main sites.

9.18.5. A notification system is implemented to alert administrators of backup failures or issues promptly.

9.18.6. Owners have regular backup restoration tests for respective assets where applicable and feasible to ensure active recovery when required.

9.18.7. Backup returns and information is kept by backup administrators, where applicable and technically feasible, in a separate storage device.

9.18.8. Any corporate data lost or damaged on local PC and laptops is the sole responsibility of the end user.

9.18.9. Asset owners emphasize that data backup frequency is aligned and updated as per the needs of the departments, requirements of a project or agreements with third parties.

9.18.10. Automated backup systems are employed where feasible to ensure consistent and timely data backups without reliance on manual processes.

9.18.11. Redundancy in backup systems is established, with particular emphasis on high-criticality systems, to prevent single points of failure, ensuring multiple copies of backups are available and retained as per their defined periods.

9.18.12. Any third-party or vendor-provided backup solutions comply with organizational standards and security requirements.

9.18.13. A comprehensive inventory of all applications is maintained, categorizing each based on its criticality to business operations and data sensitivity to determine the backup and retention priorities.

9.18.14. Data retention periods are clearly defined for each category of data and application. These periods are based on the criticality level, legal requirements, and business needs, ensuring a balance between availability, security, and cost-effectiveness.

9.18.15. For high-criticality applications and data, backups are performed at least daily, and retention periods are extended to ensure recovery capabilities in line with business continuity requirements.

9.18.16. For medium and low-criticality applications, backup frequencies and retention periods are adjusted according to a lesser degree of operational necessity but always comply with minimum set of requirements.

9.18.17. Regular audits are conducted to ensure that backup and retention practices for each application are in alignment with the documented criticality levels and are updated in response to changes in business operations.

9.18.18. The indefinite retention of data on tapes for all applications is re-evaluated, establishing specific retention timelines based on the revised criticality classification, to optimize storage and minimize unnecessary data hoarding.

9.19. Change Management Policy

Policy Statements

Having an effective Change Management Policy is vital in our current landscape where businesses are rapidly adapting to the latest processes and technologies. It ensures that there is a structured approach for managing and adopting changes within the organization with minimal disruption, as well as incorporating mechanisms of feedback. Relevant stakeholders and responsible entities across organizations need to ensure that:

9.19.1. Define formalized processes for submitting, reviewing and approving change request forms (CRFs) that are related to tax related processes, regulations and systems.

9.19.2. Thorough impact analysis is conducted for all proposed changes, evaluating their potential effects on existing workflows, system performance, and compliance requirements.

9.19.3. Changes to the data management processes or systems are in compliance with existing laws.

9.19.4. Changes to the data management processes or systems align with data privacy and security principles.

9.19.5. Prioritization and sequence of changes is based on their urgency, importance, and resource availability.

9.19.6. Establish effective standards and procedures for submitting, reviewing and implementing changes to tax related systems or processes, that ensure transparency.

9.19.7. Establish effective standards and procedures for selecting, testing, updating/upgrading technology systems that assist with processes such as tax collection, tax data integration and administrative tasks associated with FBR.

9.19.8. Monitoring and evaluation mechanisms are implemented post-implementation to assess the effectiveness of the changes and identify areas for further improvement.

9.19.9. All relevant third parties are kept under consideration while implementation of any changes are in process.

9.19.10. Emergency rollback standards and procedures are developed to quickly revert changes in case of unintended negative consequences.

9.19.11. Detailed documentation of all changes is maintained, including justifications, approvals, implementation steps, and post-change evaluations.

9.20. Data Architecture Policy

Policy Statements

Having a robust Data Architecture Policy is crucial in navigating the complexities of today's data-driven environment. It ensures data availability, reliability, and security across platforms, facilitating strategic decision-making and supporting data governance. This policy serves as a blueprint for integrating diverse data sources, promoting innovation, and guiding scalable growth. Relevant stakeholders and responsible entities across organizations must ensure that:

9.20.1. APIs are designed to ensure secure, scalable, and efficient access to FBR data services, optimizing for compatibility and integration with both internal and external systems.

9.20.2. API versioning is systematically managed to facilitate backward compatibility, ensure clear documentation for developers, and enable seamless transitions between versions without disrupting service availability or data integrity.

9.20.3. Databases are strategically designed to ensure data integrity, performance, scalability, and security, supporting the diverse needs of transactional and analytical operations within FBR, with a focus on optimizing for fast query performance and data accuracy.

9.20.4. Database schemas are optimized for efficient data storage and retrieval, employing normalization standards to eliminate data redundancy, while also considering denormalization where performance benefits justify its use.

9.20.5. Data models are developed using standardized modeling techniques, such as Entity-Relationship Diagrams and Unified Modeling Language, to accurately represent data structures, relationships, and constraints, facilitating clear communication and understanding across technical and business stakeholders.

9.20.6. Ensure that the Entity-Relationship notation is used consistently for data modeling across all projects, aiming for uniformity and standardization in data representation.

9.20.7. Data models are periodically reviewed and updated to accurately reflect changes in business processes, requirements, and data relationships, ensuring that the data architecture remains aligned with organizational needs and industry standards.

9.20.8. Enterprise architecture framework is developed to provide a comprehensive view of FBR's technology and information systems.

9.20.9. Cross-functional team is established to lead the Enterprise architecture initiative, including IT professionals, business strategists, and representatives from key departments.

9.20.10. Enterprise architecture supports integration and interoperability among disparate systems and platforms, leveraging APIs, middleware, and other technologies to facilitate seamless data exchange and process automation.

9.20.11. All data architecture models and diagrams are maintained in both metadata format and graphical (image) format, to support comprehensive understanding and utilization of data models.

9.20.12. Application projects initiate their data architecture work with a Conceptual Data Model during the Business Requirements phase, accurately representing major data entities and relationships in business terminology to support the project's data scope.

9.20.13. Logical Data Model is developed during the Design Phase of the project, detailing all required data entities and facilitating the generation of a physical data model.

9.20.14. Physical Data Model is created by the end of the Design phase, representing the physical table structures in scope of the project, and generated from the corresponding logical data model to ensure accuracy and consistency.

9.20.15. All Data Definition Language (DDL) scripts, such as CREATE TABLE/VIEW statements, are generated from the corresponding physical data model as much as feasible, rather than being manually created.

9.20.16. All Data Architecture work products are adequately labeled and documented. This includes logical models, physical models, model elements such as entities/attributes, DDL scripts, and database schema objects.

9.20.17. Data definition reports for both logical and physical models are produced for all types of applications.

9.21. Data Management Maturity Policy

Policy Statements

An effective Data Management Maturity Policy is essential in today's data-centric environment, ensuring the organization adopts a structured approach to improve data management capabilities, including governance, quality, and security. It sets a roadmap for ongoing enhancement aligned with organizational goals and industry standards. Relevant stakeholders and responsible entities across the organization need to ensure that:

9.21.1. A recognized Data Management Maturity Model is adopted as the standard framework for assessing maturity levels across various dimensions of data management.

9.21.2. Regular assessments are conducted on an annual basis and as part of major system overhauls or integrations to evaluate the current state of data management practices and identify areas for improvement.

9.21.3. Stakeholders from various departments and levels within the organization are engaged to ensure a comprehensive understanding of data management practices and challenges.

9.21.4. Clear, measurable criteria for each level of maturity within the chosen model are defined, ensuring that these criteria are aligned with organizational goals and industry standards.

9.21.5. A gap analysis is conducted as part of the assessment to identify discrepancies between current practices and desired maturity levels, focusing on areas that offer the most significant improvement in data management capabilities.

9.21.6. A detailed action plan based on the assessment findings is developed and documented, including specific initiatives, projects, and changes required to improve maturity levels.

9.21.7. Appropriate resources, including budget, personnel, and technology, are allocated to implement the action plan effectively.

9.21.8. Monitoring mechanisms are established to track the progress of initiatives outlined in the action plan and report on improvements in maturity levels to senior management and relevant stakeholders.

9.21.9. Provisions for training and awareness programs are included to enhance the data management capabilities of staff and ensure alignment with the organization's data management maturity objectives.

9.21.10. Technology solutions and tools are leveraged to automate assessment processes where possible and provide analytical capabilities for deeper insights into maturity levels and improvement areas.

9.21.11. A culture of continuous improvement in data management practices is fostered, encouraging feedback and innovative ideas from all levels of the organization.

9.21.12. Compliance and risk management considerations are integrated into the maturity assessment, ensuring that improvements in data management practices also enhance the organization's compliance posture and reduce data-related risks.

9.21.13. Where possible, the organization's data management maturity is benchmarked against similar organizations or industry averages to identify competitive gaps and opportunities for strategic improvements.

10. Communication and Training

10.1. Communication

10.1.1. Ensure all stakeholders are systematically informed about the Data Governance Policy and the relevant policies, standards, and procedures, using multiple communication channels for effectiveness.

10.1.2. Establish channels for stakeholders to provide feedback or seek clarification on the data governance policies to promote a two-way communication flow.

10.2. Training

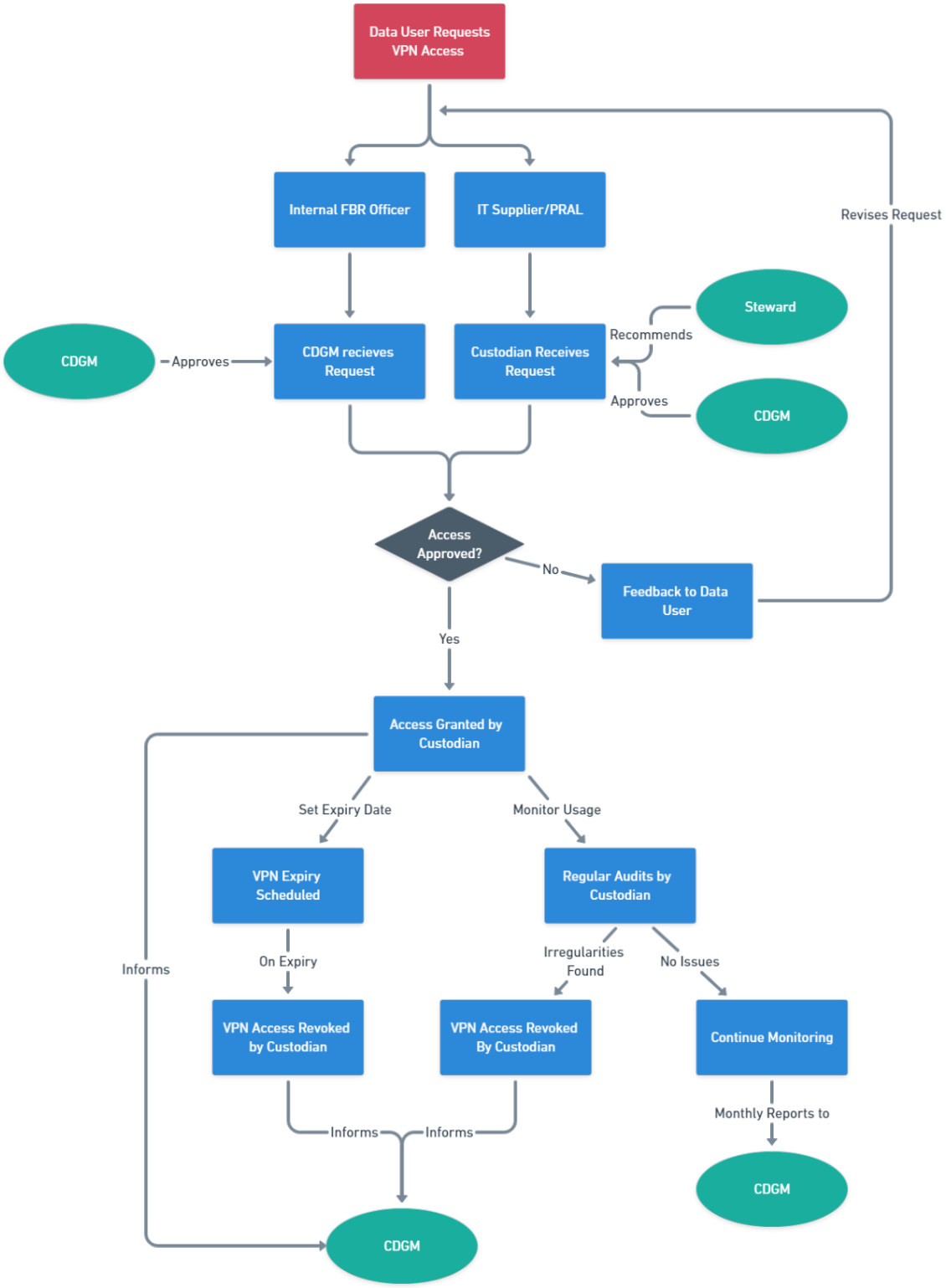
10.2.1. Incorporate data governance training into the induction program for all new employees, and third-party contractors.

10.2.2. Schedule regular training sessions as part of the staff's ongoing development to keep them updated on the latest data governance practices and changes.

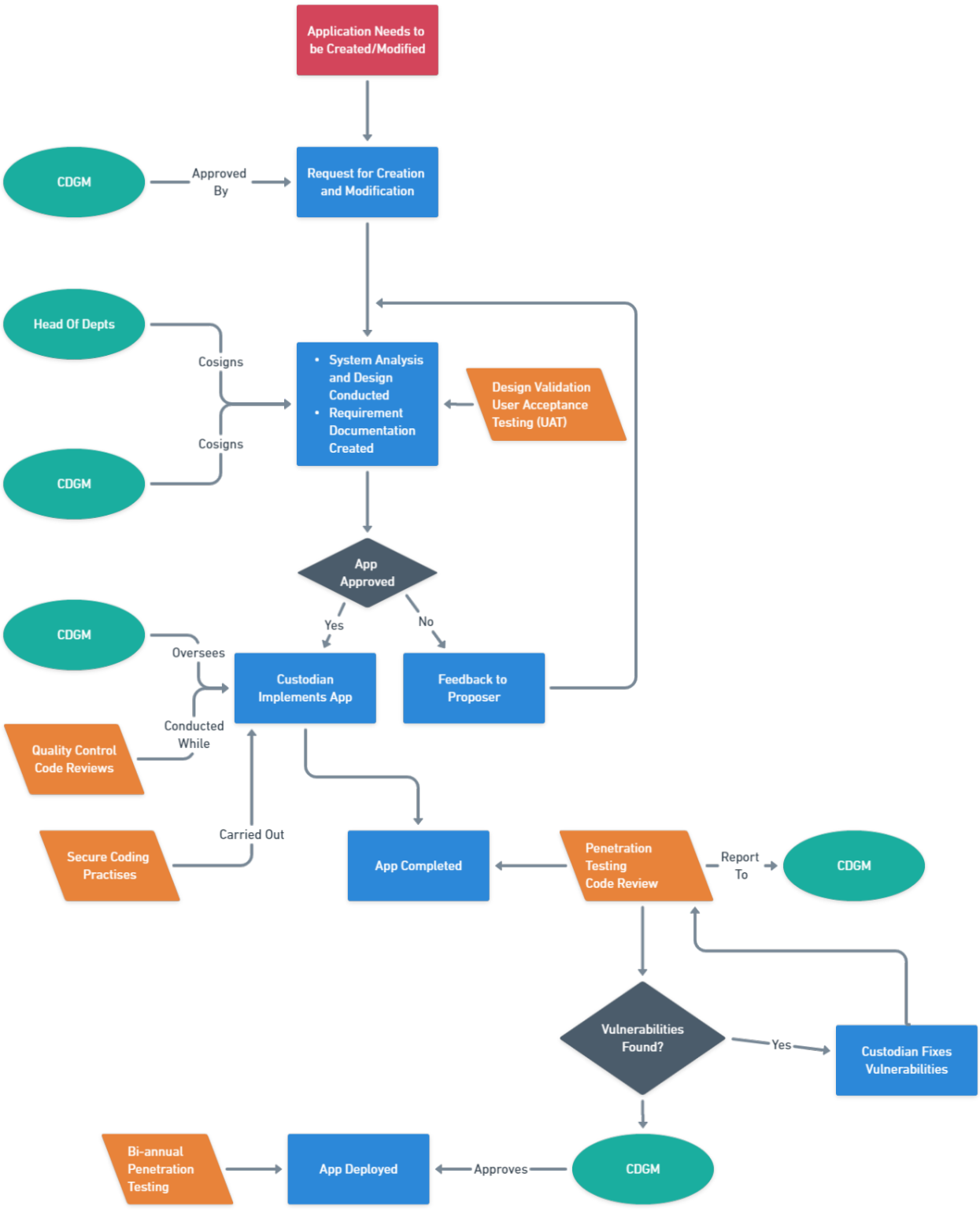
10.2.3. Make completion of specific data governance policy training mandatory before granting any staff member access to data. This includes through understanding of compliance requirements and implications of policy breach.

11. Procedural Flows for Critical Data Processes

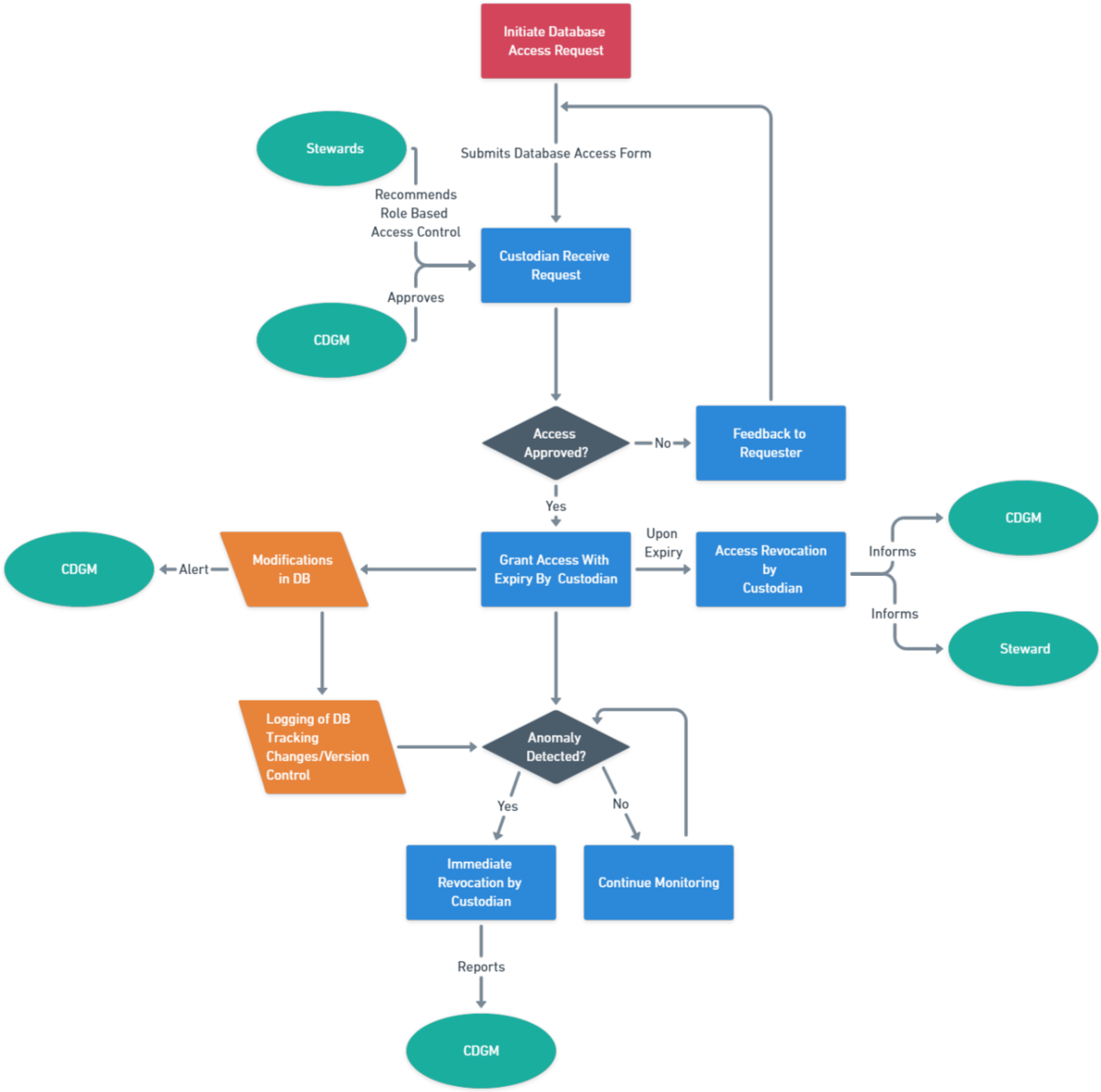
11.1. VPN Access



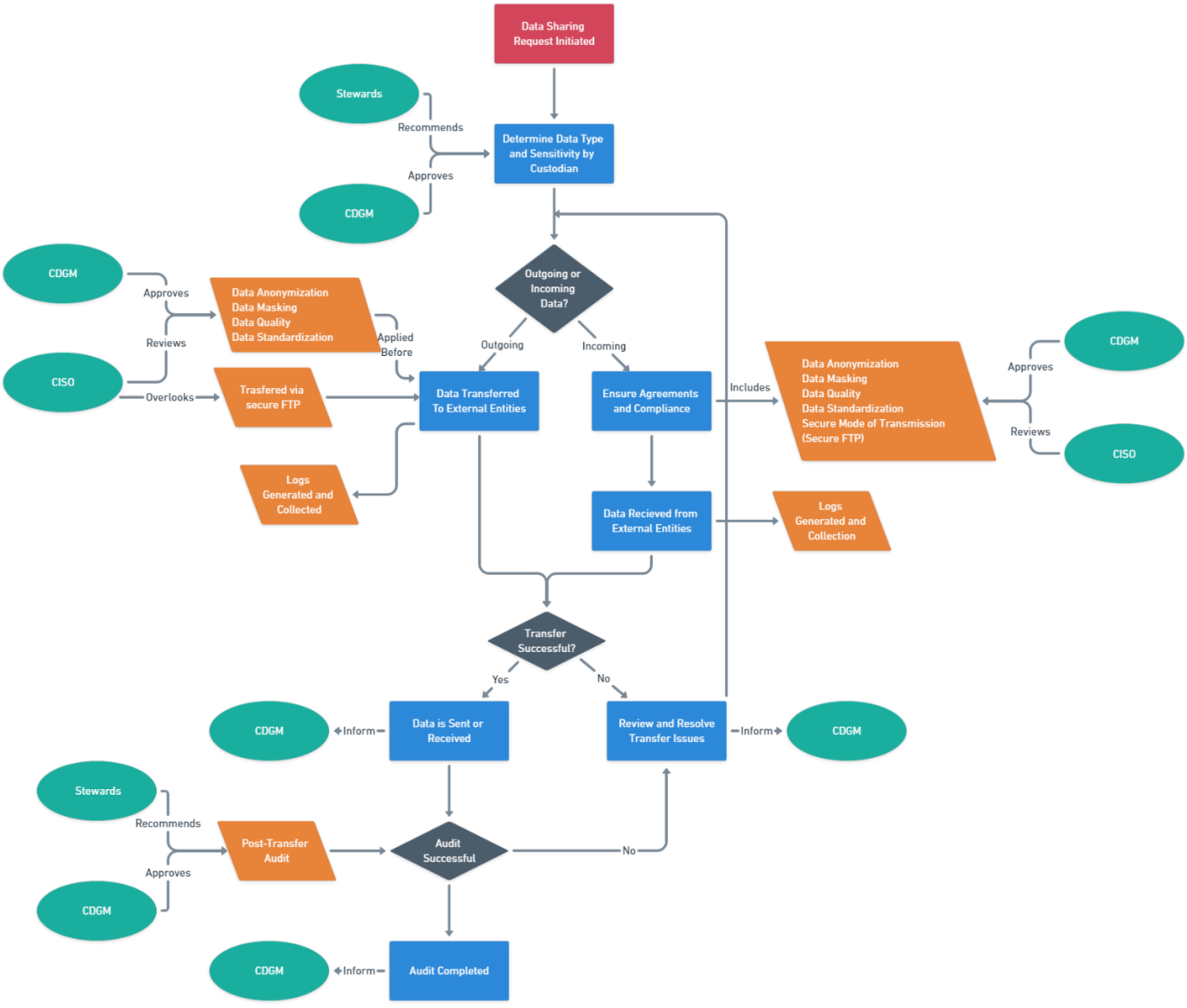
11.2. Application Creation and Modification



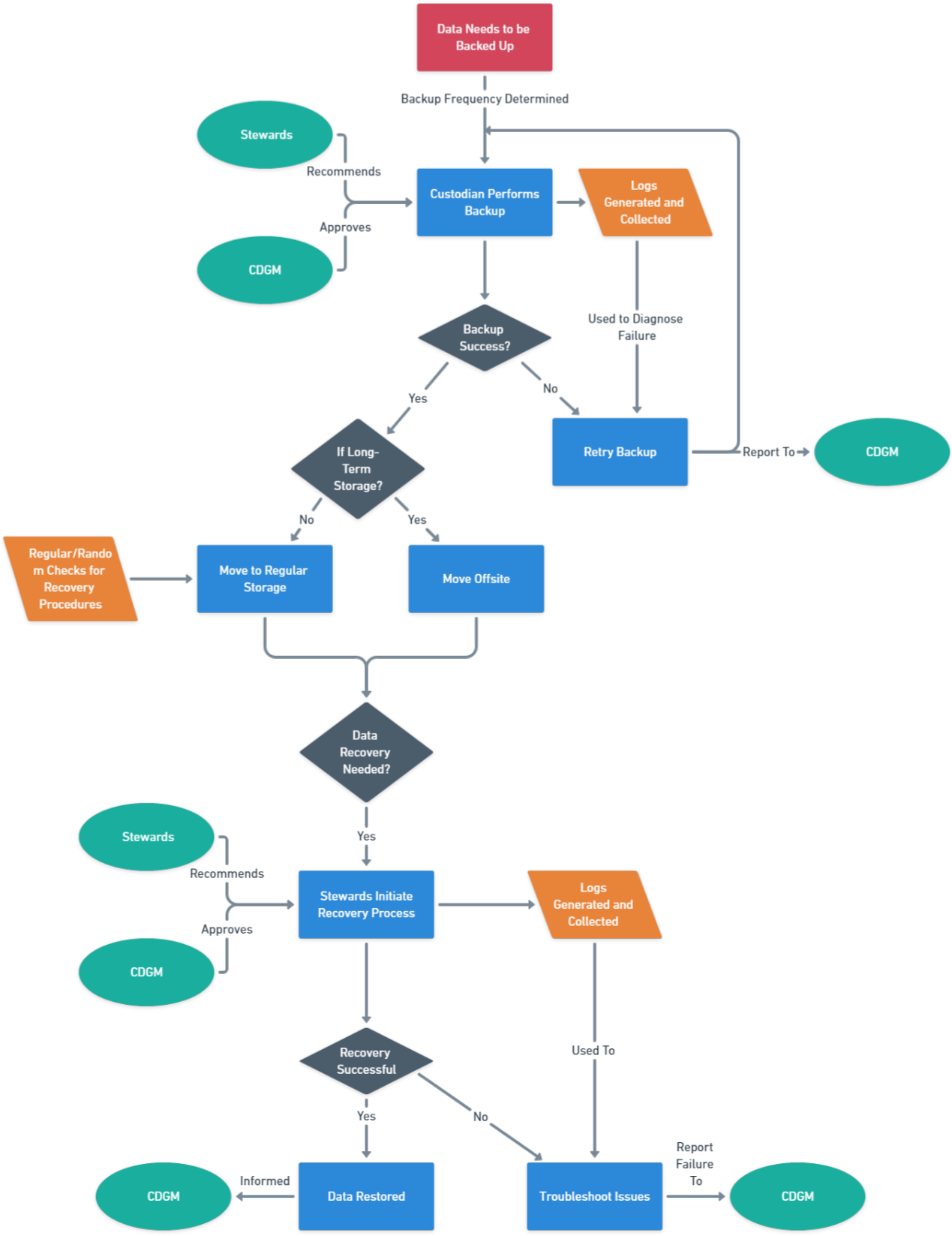
11.3. Database Access



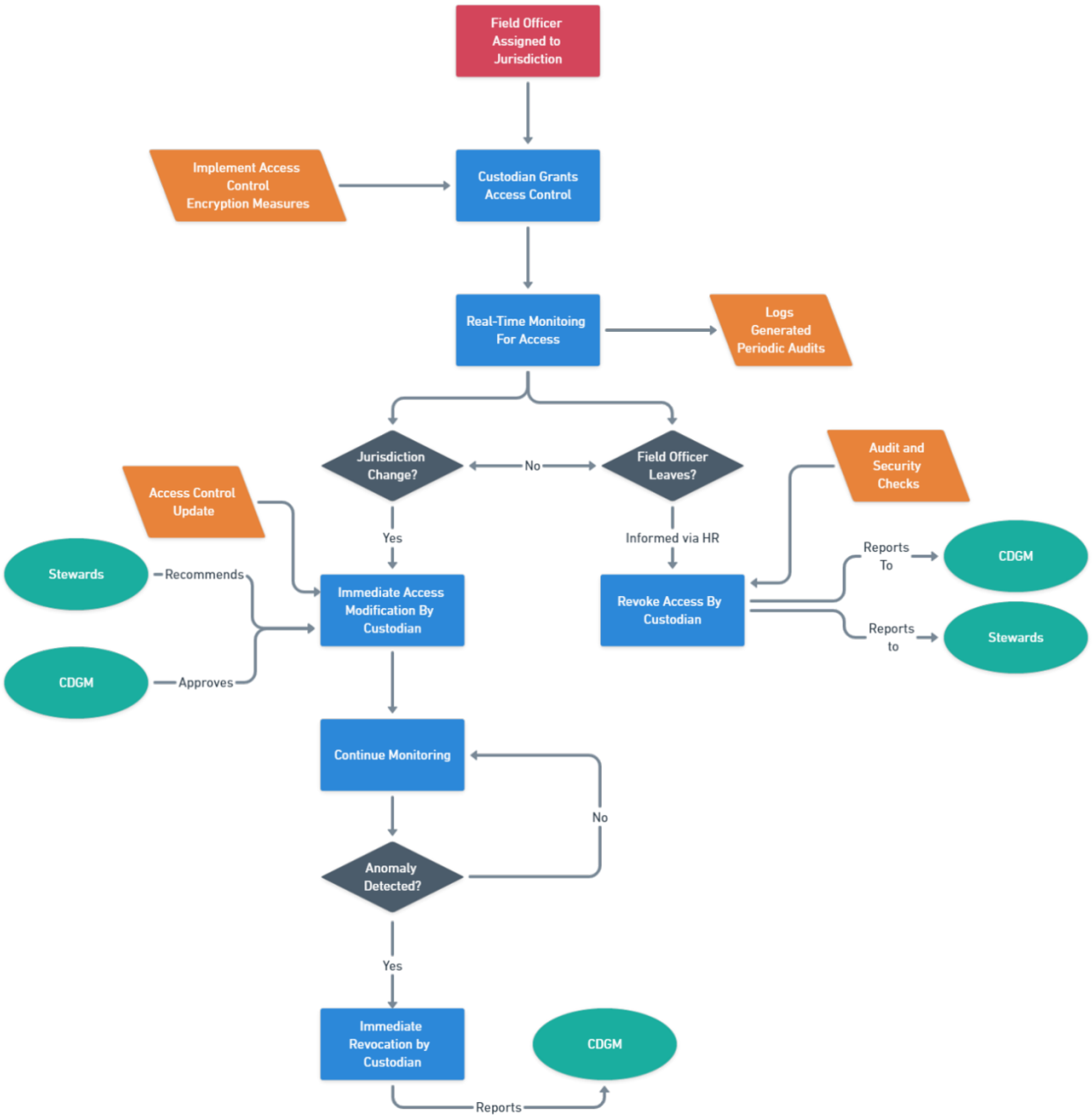
11.4. Data Sharing



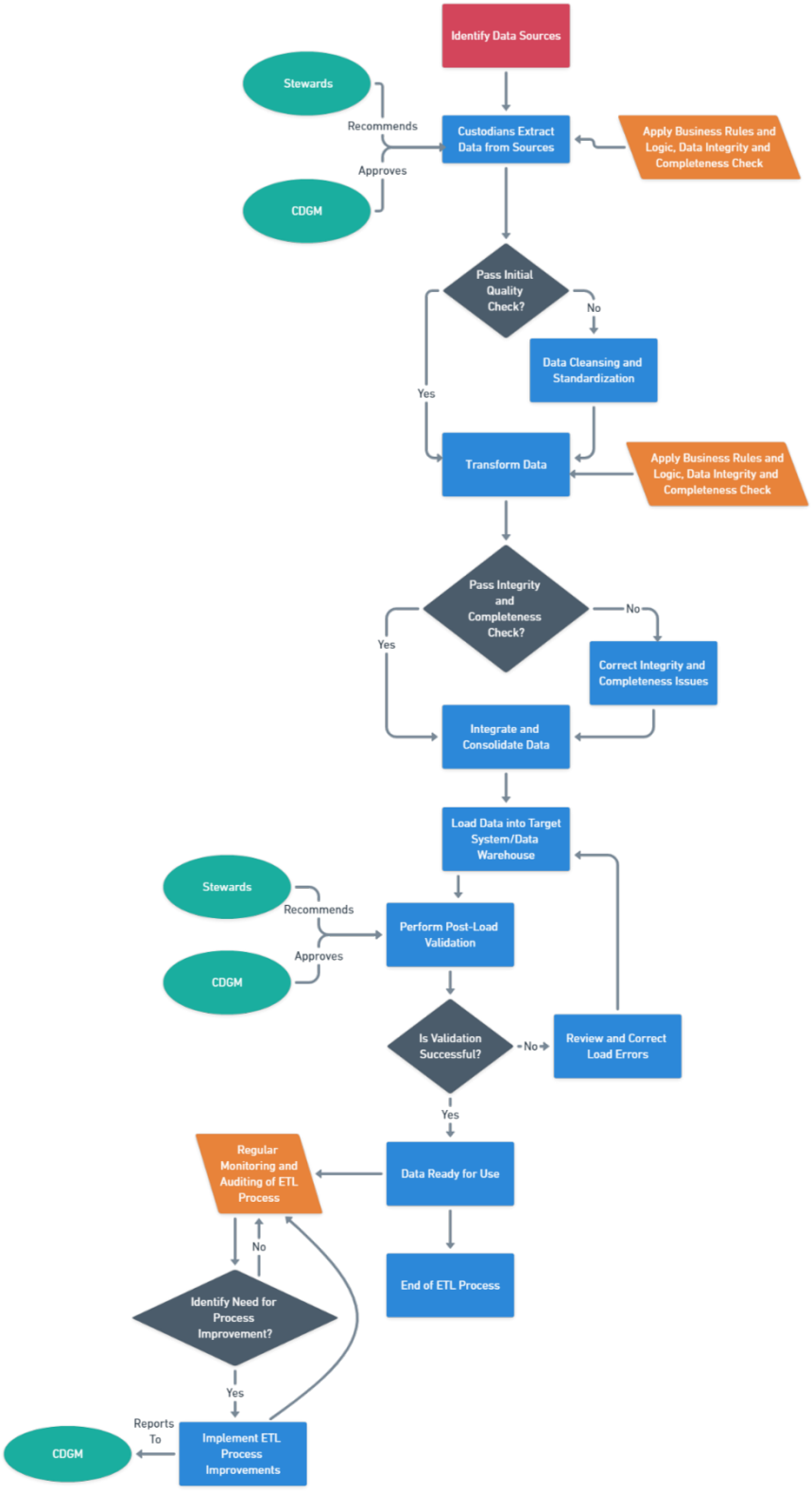
11.5. Database Backup



11.6. Jurisdiction Change



11.7. ETL Pipeline



11.8. Server Virtualization



12. Policy Review and Modification

The Data Governance Policy is a living document and will be reviewed and updated regularly to reflect changes in technology, business practices, regulatory requirements, and organizational objectives. The process for policy review and amendment involves soliciting feedback from stakeholders, assessing the need for changes, and making revisions. All amendments will be documented in the policy's revision history, and stakeholders will be informed of significant changes.

12.1. Review Schedule

12.1.1. The Data Governance Policy shall be reviewed on a bi-annual basis to ensure its continued relevance and effectiveness.

12.1.2. Additional reviews may be initiated in response to significant changes in technology, regulatory requirements, or organizational structure.

12.2. Procedures for Policy Amendments

12.2.1. Amendments to the policy can be proposed by any member of the Data Governance Office (DGO), followed by a structured review process.

12.2.2. Proposed changes shall undergo a thorough evaluation by the Member IT and sent to Chairman FBR/Board-in-Council for approval.

12.3. Feedback Mechanism

12.3.1. A feedback mechanism shall be established to gather inputs from all stakeholders on the effectiveness and applicability of the policy and constructive feedback will be considered during the policy review sessions to ensure continuous improvement.

13. Policy Compliance, Escalation and Exceptions

13.1. Compliance

This section mandates adherence to the stipulations and practices outlined in the Data Governance Policy. Compliance is essential for maintaining the integrity, security, and efficiency of our data management processes. All employees, contractors, and third-party partners including IT Supplier/PRAL are required to comply with the principles, policies, standards and procedures set forth in this policy. Adherence to these guidelines will ensure that data-related activities align with our organizational objectives and regulatory requirements.

13.2. Non-Compliance

Non-compliance with this policy can have significant repercussions, including potential risks to data integrity, security breaches, and regulatory penalties. Any instances of non-compliance will be thoroughly investigated, and appropriate remedial actions will be taken. This may include staff training, revisions to standards and procedures, or, in severe cases, disciplinary action. Regular compliance monitoring and reporting are integral to FBR's Data Governance Policy, ensuring accountability and adherence to FBR's data governance practices.

13.3. Escalations

Data governance issues should first be escalated within a department. Unresolved issues should be escalated to the Chief Data Governance and Management (CDGM), then to the Member IT who, if needed, will escalate it to Chairman FBR. The Chairman FBR is the final authority over all data governance issues.

13.4. Compliance Exceptions

In certain circumstances, deviations from this policy may be necessary. Such exceptions must be justified, documented, and signed off by the Member IT, upon the recommendation of the Chief Data Governance and Management (CDGM), after receiving approval from Chairman FBR. The process for seeking an exception involves submitting a detailed rationale, including the nature of the exception, its anticipated impact, and the proposed duration. These exceptions are reviewed on a case-by-case basis, ensuring that any deviations do not compromise the overall integrity and security of our data governance practices. All exceptions must be tracked and monitored.

ANNEXURES

Annex I: Alignment of Data Governance Policy with DAMA DMBoK v2

DAMA DMBoK v2	DAMA DMBoK v2 Domain	FBR Data Governance Policy Reference
Chapter 1	Data Management	6.1, 6.2, 7.1, 7.2, 7.3, 7.4, 7.5
Chapter 2	Data Handling Ethics	13.1, 13.2, 13.3, 13.4
Chapter 3	Data Governance	8.1, 8.2, 8.3, 12.1, 12.2, 12.3, 10.1, 10.2
Chapter 4	Data Architecture	9.16, 9.20
Chapter 5	Data Modeling & Design	9.10
Chapter 6	Data Storage & Operations	9.9, 9.13, 9.18
Chapter 7	Data Security	9.7, 9.8, 9.11, 9.12, 9.14, 9.15, 9.16, 9.17
Chapter 8	Data Integration & Interoperability	9.6
Chapter 9	Document & Content Management	9.5
Chapter 10	Reference & Master Data	9.2
Chapter 11	Data Warehousing & Business Intelligence	9.4
Chapter 12	Metadata Management	9.3
Chapter 13	Data Quality	9.1
Chapter 14	Big Data & Data Science	9.4
Chapter 15	Data Management Maturity Assessment	9.21
Chapter 16	Data Management Organization & Role Expectations	8.1, 8.2
Chapter 17	Data Management & Organizational Change Management	9.19

Annex II: Data Governance Policy Implementation Matrix

Policy Area	Responsible Entity	Operational Process
Data Quality Management Policy	DGCO	The DGCO oversees initiatives to maintain and improve data quality across the organization.
Master and Reference Data Management Policy	DGCO	The DGCO ensures the accuracy, consistency, and integrity of master and reference data.
Metadata Management Policy	DGCO	The DGCO is responsible for the creation, maintenance, and use of metadata to support data management practices.
BI and Data Warehousing Policy	DGCO	The DGCO oversees the management of BI and data warehousing to ensure data accuracy and accessibility.
Document and Content Management Policy	DGCO	The DGCO manages the lifecycle of documents and content, ensuring secure and efficient access and storage.
Data Integration and Interoperability Policy	DGCO	The DGCO facilitates seamless data integration and interoperability across systems.
Data Security Policy	CISO	The CISO implements and monitors security measures to protect data across all systems and processes.
Data Privacy and Protection Policy	CISO	The CISO ensures compliance with data privacy laws and manages data protection measures.
Data Storage and Operations Policy	DGCO	The DGCO oversees data storage solutions and operational practices for data security and efficiency.
Data Modeling and Design Policy	DGCO	The DGCO ensures that data models accurately reflect the organizational data structure and support data governance goals.
Data Usage Policy	DGCO	The DGCO sets and monitors guidelines for the appropriate use of data within the organization.
Data Access and Control Policy	CISO	The CISO manages access controls and ensures that data access is secure and compliant with zero-trust principles.

Data Destruction Policy	DGCO	The DGCO coordinates the secure deletion or destruction of data that is no longer needed.
Third-Party Data Access and Sharing Policy	DGCO	The DGCO manages data sharing with external entities, ensuring data security and compliance with agreements.
Incident Response Policy	CISO	The CISO leads the organizational response to data security incidents, including investigation and remediation.
Data Providers Engagement Policy	DGCO	The DGCO oversees the engagement with external data providers, ensuring compliance with data governance standards.
Data Classification Policy	CISO	The CISO is responsible for classifying data based on sensitivity and overseeing the protection of classified data.
Data Backup, Retention and Recovery Policy	DGCO	The DGCO implements data backup and retention strategies to ensure data recovery capabilities.
Change Management Policy	DGCO	The DGCO manages changes within the data governance framework, ensuring minimal disruption.
Data Architecture Policy	DGCO	The DGCO is responsible for maintaining a coherent data architecture that supports the organization's data needs.
Data Management Maturity Policy	DGCO, CISO	The DGCO orchestrates the organization's data management maturity assessments, identifying improvement areas and coordinating with the CISO for security-related maturity, to enhance overall data governance effectiveness.

Annex III: FBR Information & Cyber Security GRC Framework

FBR

Information & Cyber Security Governance, Risk & Compliance (GRC) Framework

FBR Information & Cyber Security GRC Framework

FBR
Information & Cyber
Security GRC
Framework

Owner: FBR IT Wing

Scope of Jurisdiction

1. FBR owned data centers:
   a) FBR (HQ), Islamabad
   b) AEOI Room, FBR (HQ), Islamabad
   c) Customs House, Karachi
   d) Metro Data Center, Islamabad

2. All Field Offices of FBR and FBR (HQ), Islamabad

3. Application development and deployment shops, PRAL

4. Service Providers other than PRAL who develop Tax/Customs applications for FBR

FBR Information & Cyber Security GRC Framework

Constitution of Information & Cyber Security Steering Committee

1. Member IT, FBR (Chairperson)
2. Chief (BDT-IT), FBR
3. Chief (IT), FBR
4. Secretary IT, FBR
5. CISO, FBR (Secretary of the Committee)

Meeting Frequency
At least quarterly and as and when deemed necessary by the Chairperson.

Representation of External Service Providers
Representatives of external service providers (e.g. PRAL) may be invited to present to or observe at the Committee, only with permission from the Committee Chairperson

	ISO 27001 ref	Requirement	Frequency of Review & Update	Proposer	Approver
1	4.3	Review and approve the scope of assets of the FBR information & cyber security GRC framework	Quarterly	CISO	Member IT
2	6.1.3	Review and approve the "ISO 27001 Applicability Domains" – refer **Annex I**	Annually		
3	5.2/5.3/ A.6.1.1	Review and approve the FBR Information Security Policy including roles, responsibilities and authorities related to information security	Annually		
4	6.1.2	Review and approve the information security risk assessment	Quarterly		
5	6.2/ 7.1/ 7.2	Review and approve the information security objectives & competence resource plan	Quarterly		
6	5.1/ 7.3/ 7.4	Communicate the importance of and create awareness about effective information security management across the FBR staff and officers in a visible manner	Quarterly		
7	7.5	Review and approve the information Security Documentation	Quarterly		
8	8	Review and approve the implementation plans and actions for the information security solutions/processes	As per project timelines		
9	9/ A.18.2.3	Conduct information security performance evaluation through Internal Audit	Annually		
10	10/ A.18.2.1	Direct corrective actions and continual improvement through External Audit	Annually		

Annex I: ISO 27001 Applicability Domains

	ISO 27001 ref	Domain	Proposer	Approver
1	A.5	Information security policies to defend against FBR information compromise, in accordance with FBR's operational requirements, laws and regulations	CISO, FBR	Member IT, FBR
2	A.6	Management framework to initiate and control the implementation and operation of information security within the organization.		
3	A.7	Human resource security prior to employment, during employment and upon termination or change of employment		
4	A.8.1	Assign responsibility for information and information processing assets		
5	A.8.2	Classify and label information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification		
6	A.8.3	Prevent unauthorized disclosure, modification, removal or destruction of information stored on removable/mobile media.		
7	A.9.1	Limit access to information and information processing facilities		
8	A.9.2	ensure authorized user access and to prevent unauthorized access to systems and services		
9	A.9.3	Make users accountable for safeguarding their authentication information.		
10	A.9.4	Prevent unauthorized access to systems and applications		
11	A.10.1	Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information		
12	A.11	Physical and environmental security of information assets under the custody of PRAL		
13	A.11	Physical and environmental security of information assets under the custody of FBR		
14	A.12.1	Ensure correct and secure operations of information processing facilities.		
15	A.12.2 A12.5	Ensure that information and information processing facilities are protected against malware and ensure the integrity of operational systems		

Annex I: ISO 27001 Applicability Domains

	ISO 27001 ref	Domain	Proposer	Approver
16	A.12.3	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	CISO, FBR	Member IT, FBR
17	A.12.4	Log security events and transmit to the FBR Security Operations Center		
18	A.12.6	Take measures to evaluate and remediate the risk from technical vulnerabilities and penetration exploits in systems and application source code		
19	A.13.1	Ensure the protection of information in networks and its supporting information processing facilities		
20	A.13.2	Maintain the security of information transferred within an organization and with any external entity.		
21	A.14	Build and test for information security within system acquisition, development and maintenance processes		
22	A.15	Protect information that can be compromised due to involvement of vendors and service providers		
23	A.17.1	Embed information security continuity in FBR's business continuity management systems		
24	A.17.2	Ensure redundant availability of information processing facilities		
25	A.18.1	Build controls to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security, intellectual property and data privacy		
26	A.18.2.2	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies		
27	A.12.4	Monitor security events 24 x 7 x 365 by maintaining appropriate solutions and staff in the FBR House Security Operations Center		
28	A.16.1	Respond to incidents, investigate incidents and collect/store evidence of compromise		
29	A.12.6.1	Perform technical vulnerability scanning, penetration tests, application source code security tests and evaluate the findings		

Annex IV: FBR Incident Response Procedure

	Incident Response Actions			Maintenance & fine-tune actions		
	L1	L2	SOC Manager	L1	L2	SOC Manager
Falcon Complete	- Monitor Endpoint Security including "Activity Dashboard", "CrowdScore Incidents" and "Endpoint Detections". - Investigate the detection and analyses the process execution and parent-child relation . - Check the basic detail like severity ,Tactics & Techniques ,Host ID. - Check the indicator status on Threat Intelligence Platform (if any). - Check the current status of process if it's terminated or currently running. - Gather the information about a particular Host and user from "Discover" and "Investigate" feature. - If required, Open a case with the Falcon Team through Message center. - If required, acquire any required data(files) through "Real Time Response" feature for further analysis. - If required, upload suspicious files to CrowdStrike sandbox to analyze the files. - Report to the relevant team according to the escalation matrix under the supervision of L2 or report directly to L2 if Falcon overwatch detects and reports anomaly. - L1 reporting includes all the necessary information gathered from the detections.	- Support L1 Analyst staff and analyzes information gathered by the Level 1 analyst to evaluate a particular incident. - If required, Open a case with the Falcon Team through Message center. - Use Message Center to communicate with Falcon Complete team for queries. - If required, acquire any required data(files) through "Real Time Response" feature for further analysis. - If required, upload suspicious files to CrowdStrike sandbox to analyze the files. - Communicate with IT teams for resolving queries escalated by Falcon Complete team. - If FBR Rewterz SOC's own threat analysis concludes that endpoint should be contained, then FBR Rewterz SOC should go ahead and contain and communicate the outage to FBR data center within 3 minutes of imposing the containment. - If Falcon Complete team recommends FBR Rewterz SOC to contain endpoint, L2 should contain the endpoint and then should communicate the outage to FBR data center within 3 minutes of imposing the containment. - Assist IT teams in ensuring that the affected system has been successfully remediated and restored. - Ensures that a technical summary of the incident is prepared. - Gives recommendation to correct the issue or provide a work around that will provide functionality that approximates normal service as closely as possible. - Performs deep-dive incident analysis by correlating data from various sources - If an incident reoccurs or is likely to reoccur, notify problem management so that root cause analysis can be performed and a standard work around can be deployed	-Tracking the incident from start to end and finalizing incident reports -Providing guidance and direction to the SOC team and other teams involved in incident response. - Assist in communication with the management. -Reports on security operations to the management -Ensuring incident identification, assessment, quantification, reporting, communication, mitigation and monitoring. -Provide support to L2	- Identify requirements necessary for increasing the visibilty and report to L2. - Check inactive sensor reports from crowdstrike	- Engage with Falcon Team for any queries regarding support. - Create Custom reports as per the requirement. - Create workflows as per the requirement - If PC Support (FBR PC Support team) notify changes to PCs/laptops to SOC whenever changes are made, L2 update the assets in Crowdstrike - If DC teams (KHI/ISB) notify changes to assets to SOC contact person i.e. additions, deletions, IP changes etc., L2 update the assets in crowdstrike. - Make inquiry about inactive sensors and connect with DC team to resolve the issue.	- Check and validate if the custom dashboards and reports provide the meaningful information and satisfies t requirement. -Provide any recommendations in orc to create more visibility in environmer in collaboration with Management and Falcon Complete team. - Use "User Management" tab to assign the roles and access privilege to users. -Take approval from the management related to "Maintenance token" for uninstalling sensor. - Reconcile changes advised vs. changes implemented on a monthly basis.
Falcon IDP	- Monitor the following tabs: 1- Domain Security overview 2- Identity-based Detections 3- Detections Dashboard 4- Identity-based Incidents 5- Privileged Identities 6- Users 7- Endpoint 8- Risk Analysis 9- Event analysis 10- Event analysis dashboard - Analyze events in the above mentioned tabs and report to L2 if any anomaly observed. - Investigate detections triggered in "Identity-based Detection" and "Identity-based Incidents" and gather relevant evidences like usernames, involved endpoint, severity etc and report to L2. - Check "System Notifications" tab to look if any integrated source for IDP disconnect with the CrowdStrike and report to L2. - L1 reporting to L2 includes summary of the detections and its relevant evidences.	- Support L1 Analyst and analyze the anomaly reported by L1 and ensure that the technical summary includes all the necessary information. - Engage the relevant teams if the reported anomaly is true positive. - Assist IT teams for complete remediation and provide recommendations. - Use threat hunter tab to look for malicious events and engage relevant team for resolution. - Generate reports using "Report" tab as per the requirement and escalate it to the relevant team. - Participate in a formal incident rapid response process for high priority incidents	-Tracking the incident from start to end and finalizing incident reports -Providing guidance and direction to the SOC team and other teams involved in incident response. - Assist in communication with the management. - Provide support in triaging the incidents - Provide support to L2	- Identify the requirements necessary for increasing the visibilty in identity based events and report to L2.	- Create custom reports as per the requirement. - Create Custom Dashboard for Falcon IDP using "Dashboard and Reports" tab as per the requirement.	- Check and validate if the custom dashboards and reports provide the meaningful information and satisfies tl requirement. - Provide any recommendations in order to create more visibility in environment in collaboration with Management and Falcon Complete team.
QRadar SIEM	- Monitor "Dashboard", "Offense", "Log Activity" and "Network Activity" tabs. - Monitor and analyses cyber security events with the use of QRadar (SIEM). - Report to the relevant team under the supervision of L2 or report to L2 for ticket escalation. - L1 reporting to L2 includes summary of the detection and its relevant evidences.	- Analyze the anomaly reported by L1 and ensure that the technical summary includes all the necessary information. - Engage the relevant teams according to the escalation matrix if the reported anomaly is true positive. - Properly triage and respond to identified malicious activity. - Assist IT teams for complete remediation and provide recommendations. - Review SOC Analyst ticket queue, review tickets, closure or reassignment as needed - Monitor Offense tab and ensure that all the offenses are investigated.	-Tracking the incident from start to end and finalizing incident reports -Providing guidance and direction to the SOC team and other teams involved in incident response. - Assist in communication with the management. - Provide support to L2	- Identify requirements necessary for monitoring and report to L2 - Email to the DC team if log source is down.	- Assist deployment team in: 1- Logs Clipping: Used to remove unwanted logs. 2- Logs Integration: Used to integrate new log source 3- Flow Integration: Used to integrate flow sources 4- Apps Integration: Used to integrate new apps 5- Parsing: Used to map the payload data in different fields - Create usecases (rules) and dashboards. - Create Reference sets for use cases. - Assist TISS team to extract custom properties from the payload to use it in usecases (rules) and dashboard. - Fine-tune usecases (rules) - Monitor EPS status. - Email to the DC team if log source is down. - If DC teams (KHI/ISB) notify changes to assets to SOC contact person i.e. additions, deletions, IP changes etc., L2 communicate and assist deployment team for updating assets in Qradar.	- Assist deployment team for Custom Parser Creation - Check and validate if the custom dashboards,usecases and reports provide the meaningful information and satisfies the requirement. - Suggest Custom Dashboard and usecases to monitor malicious events - Conduct gap analysis of SIEM after significant change or as per the requirement. - Validate the tasks perform by deployment team - If DC teams (KHI/ISB) notify change to assets to SOC contact person i.e. additions, deletions, IP changes etc., SOC manager communicate and assis deployment team for updating assets Qradar. - Reconcile changes advised vs. changes implemented on a monthly basis.
QRadar SOAR	- Investigate the Ingested events from Qradar SOAR. - Analyze the artifacts enriched by SOAR. - Use playbooks as per the requirement - Create ticket and escalate to L2 for validation.	- Validate the ticket reported by L1 and escalate it to the relevant teams if the ticket is true positive. - Use playbooks as per the requirement.	- Assist in communication with the management. - Provide support in triaging the incidents - Assess incident reports - Provide support to L2	- Identify the requirements and provide suggestion for playbooks.	- Create and test playbooks as per the requirement - Identify the requirements and provide suggestion for playbooks.	- Validate the playbooks - Asses and recommend playbooks
Fortigate Internet Edge	- Monitor Dashboard in Qradar related to FortiGate - Monitor Inbound/outbound connections. - Report to L2 if any anomaly is observed. - Respond to offense tab in Qradar related to FortiGate security events. - L1 reporting to L2 includes summary of the detection and its relevant evidences.	- Analyze the anomaly reported by L1 and ensure that the technical summary includes all the necessary information. - Engage the relevant teams if the reported anomaly is true positive. - Assist IT teams for complete remediation and provide recommendations.	- Assist in communication with the management. - Provide support in triaging the incidents - Assess incident reports - Provide support to L2	- Identify the gaps and requirements necessary for monitoring and report to L2.	- Create Dashboard and usecases (rules) in Qradar related to FortiGate - Fine tune usecases (rules) related to FortiGate - Validate FortiGate logs, assist and engage with deployment team to enable and disable relevant and irrelevant events - Assist TISS team to extract custom properties from the payload to use it in usecases (rules) and dashboard.	- Suggest Custom Dashboard and usecases to monitor malicious events as per the requirement. - Check and validate if the custom dashboards and usecases (rules) provide the meaningful information and satisfies the requirement. - Support L2 for validating logs and provide recommendations

Fortiweb DMZ Internet Edge	- Monitor Dashboard of FortiWeb and FortiAnalyzer. - Report to L2 if any anomaly observed. - L1 reporting to L2 includes summary of the detection and its relevant evidences.	- Analyze the anomaly reported by L1 and ensure that the technical summary includes all the necessary information. - Engage the relevant teams if the reported anomaly is true positive. - Assist IT teams for complete remediation and provide recommendations.	- Assist in communication with the management. - Provide support in triaging the incidents - Assess incident reports - Provide support to L2	N/A	N/A	N/A
Cisco ESG	- Monitor Dashboard of Cisco ESG - Analyze emails that are tagged as: 1.Virus Detected 2.Spam Detected 3.Contains Malicious URLs 4.Outbreak Filters - Report to L2, if any suspicious email observed. - Download email reports on daily basis from Cisco ESG and email to FBR info sec team.	- Analyze the anomaly reported by L1 and ensure that the technical summary includes all the necessary information. - Engage the relevant teams according to the escalation matrix if the reported email is malicious. - Assist IT teams for complete remediation and provide recommendations.	- Support and assist the SOC with email security related incidents. - Assist in communication with the management. - Provide support in triaging the incidents - Assess incident reports	N/A	N/A	N/A
Sangfor WSG-1	- Monitor Dashboard of SANGFOR IAG. - Monitor logs tab in report center. - Report anomaly to L2 if observed.	- Analyze the anomaly reported by L1 and ensure that the technical summary includes all the necessary information. - Engage the relevant teams according to the escalation matrix if the reported anomaly is true positive - Assist IT teams for complete remediation and provide recommendations.	- Assist in communication with the management. - Provide support in triaging the incidents - Assess incident reports - Provide support to L2	N/A	N/A	N/A
Sangfor WSG-2	- Monitor Dashboard of SANGFOR IAG. - Monitor logs tab in report center. - Report anomaly to L2 if observed.	- Analyze the anomaly reported by L1 and ensure that the technical summary includes all the necessary information. - Engage the relevant teams if the reported anomaly is true positive. - Assist IT teams for complete remediation and provide recommendations.	- Assist in communication with the management. - Provide support in triaging the incidents - Assess incident reports - Provide support to L2	N/A	N/A	N/A

Task Name: Monitoring Of Inactivity Of sensors in Servers(Crowdstrike)			
S.No	**Action**	**Responsibility**	**Frequency**
1	Custom alert enabled in Crowdstrike that will send Falcon sensor status of servers after	L1 & L2	24 hours
2	Email to DC team if any inactive Falcon sensor found on the report generated by Crowds	L1 & L2	
3	Assist DC team to resolve the issue and make sure the connectivity is established betwe	L2	

Task Name: Monitoring Of Inactivity Of sensors in Workstation (Crowdstrike)			
S.No	**Action**	**Responsibility**	**Frequency**
1	Custom alert enabled in Crowdstrike that will send Falcon sensor status of workstations	L1 & L2	Weekly
2	Email to Support team if any inactive Falcon sensor found on the report generated by Cr	L1 & L2	
3	Assist Support team to resolve the issue and make sure the connectivity is established b	L2	

Task Name: Monitoring Of Qradar Agent			
S.No	**Action**	**Responsibility**	**Frequency**
1	Rule created in Qradar that will triggered in Offense tab if the log source stopped sendi	L1 & L2	When the rule triggers
2	Sent Email to DC and Qradar deployment team and assist deployment team to update c	SOC Manager & L2	

FBR SOC Contact List	
IP Phone	1177
FBR Emails	fbr.socl1@rewterz.com
	fbr.socl2@rewterz.com
	fbr.socl3@rewterz.com
Cell Phone / Rewterz emails	0332-3038761 (Uzair Mughal-Soc Manager) "uzair.mughal@rewterz.com"
	0321-5264267 (Raja Umer- L2) "raja.umer@rewterz.com"
	0314-5103234 (Hassam Ishfaq - L1) "hassam.ishfaq@rewterz.com"
	0315-0094257 (Abdul Wahab - L1) "abdul.wahab@rewterz.com"
	0312-5725859 (Furqan Tariq - L1) "furqan.tariq@rewterz.com
	0300-5592669 (Waseem Abbas-L1)
	0319-2201672 (Kashif Khan - L1)