

National Data Management Guidelines

Data Security, Privacy, and Other Regulations

Table of Contents

1. Data Security, Privacy, and Other Regulations Domain Introduction

- 1.1 Disclaimer
- 1.2 Domain Overview
- 1.3 Target Audience
- 1.4 Abbreviations and Glossary
- 1.5 Readability Guide
- 1.6 Stakeholders Involved
- 1.7 Key Success Factors
- 1.8 Compliance with National Data Standards

2. National Regulation Alignment

- Overview

3. Data & Information Security

- Overview

4. Personal Data Privacy

- Overview

5. Other Regulations

- Overview

6. Data Classification

- Overview
- 6.1 Data Classification Operations
- 6.2 QDTI

7. Regulation Monitoring

- Overview

8. Regulation Audit & Improvement

- Overview

9. Appendix

- 9.1 Templates & Frameworks
- 9.2 Pre-Launch Security and Risk Review for Platforms

1. Data Security, Privacy, and Other Regulations Domain Introduction



1.1 Disclaimer

The National Cyber Security Agency (NCSA) is the government entity responsible for cybersecurity in Qatar. NCSA serves as the national authority on this topic from a regulatory perspective. Therefore, the data security, data classification, and data privacy controls and corresponding specifications for the Data Security, Privacy, and Other Regulations Domain will be detailed and addressed by NCSA.

Guidelines regarding the operationalization of data classification will be detailed in this document (activity 6.1 – Data Classification Operations), and compliance to this activity will be covered under the National Data Management Compliance Assessment by NPC. Compliance to all other aspects of Data Classification are monitored by NCSA

1.2 Domain Overview

Key Components of the Data Security, Privacy, and Other Regulations Domain

The Data Security, Privacy, and Other Regulations domain ensures that government entities align their data practices with national laws, regulatory frameworks, and cybersecurity standards. It reinforces the foundational role of secure, ethical, and compliant data management within Qatar's digital governance landscape.

While the operational authority for data security, privacy, and classification compliance resides with the National Cyber Security Agency (NCSA), and cloud adoption is governed by MCIT, this domain provides high-level guidance on how entities can remain aligned with key national regulations—such as the National Information Assurance (NIA) Standard, the Personal Data Privacy Protection Law (PDPPL), the Cloud First Policy, the National Data Classification Policy, the Right to Access Information Law, and the Cybercrime Prevention Law.

NPC's role in this domain is to ensure entities are aware of their regulatory obligations and to provide operational guidance where applicable. The only specification under this domain that falls under the National Data Management Compliance Assessment is Data Classification Operations, which outlines the steps required to implement classification labeling, catalog registration, and escalation mechanisms.

Organized into thematic focus areas—Regulation Alignment, Data & Information Security, Personal Data Privacy, Data Classification, and Monitoring—this domain serves as a bridge between national policy mandates and internal operational readiness

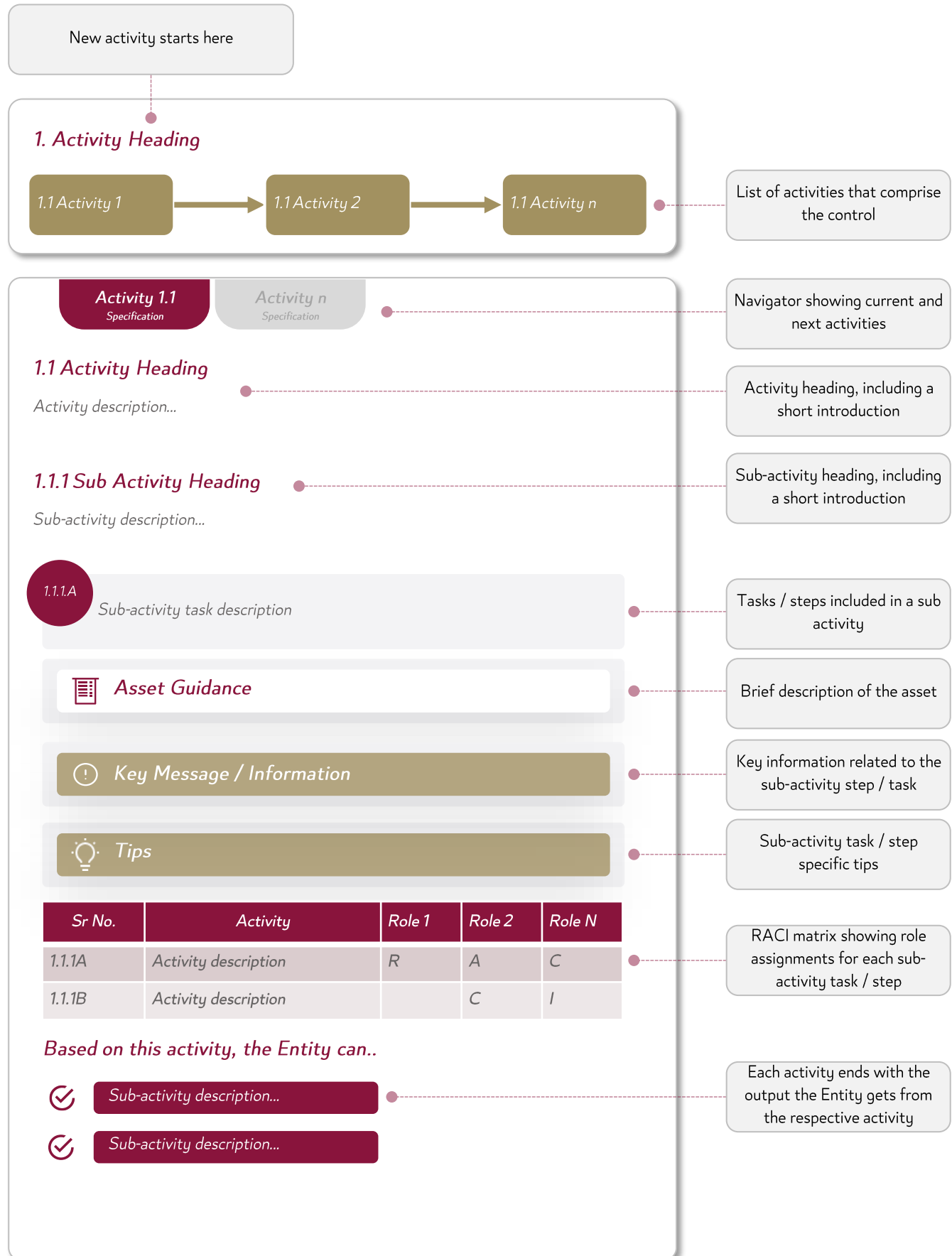
1.3 Target Audience

This handbook is intended for the Data Management and Security Directors. It is also suitable for team leads and other individuals deemed responsible for data security, personal data privacy, regulatory compliance, and classification oversight within the Entity. Additionally, the handbook is relevant to professionals working in IT operations, risk management, and internal audit. The handbook helps align internal practices with national regulations and standards, while supporting the Entity's broader data governance responsibilities.

1.4 Abbreviations and Glossary

Abbreviation/Term	Definition / Long Name
DSPO	Data Security, Privacy and Other Regulations
NCSA	The National Cyber Security Agency
PDPPL	Personal Data Privacy Protection Law
C4	Top Secret Data, represented by the standard color “Dark Red”
C3	Secret Data, represented by the standard color “Red”
C2	Restricted Data, represented by the standard color “Orange”
C1	Internal Data, represented by the standard color “Blue”
C0	Public Data, represented by the standard color "Green"
NIA	The Standard for National Information Assurance
ISMS	Information Security Management System
CSPs	Cloud Service Providers
MCIT	Ministry of Communications and Information Technology
QDKC	Qatar Data Knowledge Case
QDTI	Qatar Data Trust Index
RBAC	Role-Based Access Control
TLS	Transport Layer Security
DLP	Data Loss Prevention
Data Quality Score (DQS)	The Data Quality Score (DQS) is a score that focuses exclusively on data quality, using the seven recognized data quality dimensions. It is one of the two components of the overall Qatar Data Trust Index (QDTI) score. The DQS is composed of two key dimensions: Data Quality Assessment and Data Quality Governance.
Data Compliance Score (DCS)	The Data Compliance Score (DCS) is a score that focuses on measuring compliance with national data standards. It represents the second and final component of the overall Qatar Data Trust Index (QDTI) score. The DCS assesses compliance across the four dimensions of the National Data Management Framework: Data Strategy & Governance, Data Enablement, Data Value Harvesting, and Data Protection & Privacy.

1.5 Readability Guide



Note: Should an activity only contain one sub activity, this sub activity will be in the format of "1.1.A" instead of "1.1.1.A"

1.6 Stakeholders Involved

Below are the stakeholders and actors who contribute to the different processes outlined in the upcoming chapters.

Stakeholder	Role Description
Data Governance Office (DGO)	A Data Governance Office (DGO) is the centralized national body in the National Planning Council responsible for facilitating and coordinating data governance efforts across all associated government entities. It serves as the principal body overseeing the management of data as a strategic asset, ensuring that data-related processes align with the national objectives and comply with relevant policies and regulations.
Data Management & Security Director	The Data Management and Security Director is responsible for leading and overseeing the development and implementation of the data agenda within the government entity, ensuring alignment with strategic objectives and compliance with security regulations. This role promotes best practices in data management while ensuring robust security measures are in place to safeguard the Entity's data assets. The director bridges business and IT to support data-driven decision-making, elevate data as a strategic asset, and ensure data is managed and secured across its lifecycle. Additionally, the director fosters a culture of data security and literacy within the entity, supervises the value realization agenda for data, and ensures alignment with national security policies and standards, as well as the vision of executive leadership.
Data Management and Governance Section Head	The Data Management and Governance Section Head is responsible for leading, managing, and overseeing both data management and governance initiatives within the government entity. This role focuses on establishing and implementing best practices to ensure data governance and management align with the Entity's business requirements, strategic objectives, and compliance with national data standards. The Section Head collaborates with various teams across the Entity to develop and operationalize frameworks, policies, and processes for data governance and management. This includes improving data quality, accessibility, and protection, while also ensuring data lifecycle management practices are in place. The Section Head fosters a data-driven culture and ensures that data is treated as a strategic asset to drive decision-making and operational excellence.

Stakeholder	Role Description
Data Architecture and Analytics Section Head	The Data Architecture and Analytics Section Head oversees the data architecture and analytics agenda/initiatives within the government entity, ensuring alignment with strategic objectives and national data management standards. This role is responsible for designing and maintaining a secure, scalable data infrastructure that supports data integration, management, and accessibility, as well as Overseeing data modeling, database design, and system integration, developing advanced analytics, data visualization, and reporting solutions to enable informed decision-making. The Section Head collaborates with departments to identify key performance indicators (KPIs), analyze trends, and provide actionable insights that optimize processes, enhance service delivery, and support policy-making. By combining expertise in data architecture and analytics, this role drives a culture of data-driven innovation and operational excellence across the Entity.
Information Security and Risk Management Section Head	The Information Security and Risk Management Section Head is responsible for overseeing the Entity's cybersecurity agenda, integrating risk management and compliance into governance frameworks. This role ensures the protection of information assets by implementing robust security measures, monitoring risks, and fostering a culture of security awareness. The Section Head collaborates across departments to align security initiatives with organizational goals and regulatory requirements, ensuring resilience against cyber threats and compliance with national and international standards.
Data Governance Specialist	The Data Governance Specialist oversees the frameworks, policies, and procedures of governance and ensures their implementation to guarantee the effective management and utilization of data and resources within the Entity. This role includes developing and maintaining governance structures, leading compliance initiatives, and fostering a culture of accountability and transparency.
Data Quality Specialist	The Data Quality Specialist is responsible for overseeing data quality management processes within the entity. This role involves implementing data quality standards, monitoring data quality, and ensuring data consistency and effective usage across the Entity. The Data Quality Specialist collaborates with various teams to address data issues and enhance overall data quality.
Metadata Specialist	The Metadata Specialist is responsible for managing the Entity's data catalog and metadata assets to enhance data visibility, accessibility, and governance. This role focuses on developing and maintaining metadata standards, ensuring metadata quality, and supporting integration with the data catalog. The specialist plays a key role in enabling data discovery, supporting data-driven initiatives, and ensuring alignment with the Entity's data governance and management strategies.

Stakeholder	Role Description
Data Compliance Specialist	The Data Compliance Specialist ensures the Entity's data practices comply with national regulations, organizational policies, and international standards. This role manages data privacy, security, and governance compliance, conducts audits, mitigates non-compliance risks, and promotes awareness of regulatory requirements. The specialist works with stakeholders to embed compliance controls into data processes, ensuring adherence to legal and ethical standards.
Data Architect	The Data Architect is responsible for designing and implementing the Entity's overall data architecture, including logical and physical data models. This involves creating secure, scalable data structures that align with business needs, security requirements, and national and international data management and governance standards. The Architect ensures proper data integration, quality, and accessibility across systems, working with teams to maintain consistency and accuracy, and support data-driven decision-making to optimize data as a strategic asset.
Data Visualization Officer	The Data Visualization Officer is responsible for building dashboards and visual reports based on data, which are used to provide insights to leadership for decision-making.
Data Engineer	The Data Engineer transforms data into a format that can be easily analyzed and utilized. The Data Engineer works closely with other stakeholders to ensure data quality is maintained and implemented systems adhere to the highest possible standards.
Business Data Analyst	The Business Data Analyst is responsible for analyzing data from multiple sources to provide actionable insights that drive strategic and operational decisions within the Entity. This role involves designing reports and dashboards to effectively communicate findings, collaborating with cross-functional teams to ensure data accuracy and relevance, and aligning analytics with business objectives. The Analyst plays a key role in enabling data-driven decision-making and identifying opportunities to improve processes and outcomes.
Data Strategy Expert	The Data Strategy Expert is tasked with developing and promoting a data management and analytics strategy to achieve broad acceptance across the government entity. The expert identifies innovative ways to utilize data to achieve strategic objectives and enhance effective decision-making. Additionally, they introduce frameworks and practices to deliver accurate, reliable, and actionable data insights.

Stakeholder	Role Description
Data Owners	Data Owners are responsible for their department's (or sub-department's) data and its quality throughout its lifecycle across systems and ownership boundaries. They are accountable for supporting, guiding, reviewing, correcting, and/or approving the work of the data stewards managing their data to ensure their datasets are maintained to the highest possible standards.
Data Stewards	Data Stewards are responsible for identifying datasets related to relevant subdomains for inventory purposes and monitoring data quality metrics within and across entities. They are nominated as a business representative with a deep understanding of a specific data subdomain and can identify functional data requirements and needs.
Internal Audit Team	The Internal Audit Team is responsible for independently evaluating the Entity's data classification practices, security control enforcement, and regulatory compliance posture. In the context of this QDKC, they support or lead independent reviews of classification activities, assess the effectiveness of escalation and resolution processes, and track remediation progress. They also advise on audit methodology and risk-based prioritization.
Information Security Team	The Information Security Team ensures that the Entity's information assets are protected in accordance with national regulations and the National Information Assurance Standard. In this QDKC, the team helps define and implement technical controls based on classification levels (e.g., encryption, access control), supports audit activities, and reinforces classification awareness through digital platforms and system integrations.
IT Team	The IT Team provides the technical implementation support required to enforce classification and security policies across platforms and systems. This includes configuring metadata fields, setting up automated watermarking or access banners, and ensuring tools such as document management tools, and file servers, can support classification-based controls and tracking.
Internal Communications Team	The Internal Communications Team supports the delivery of classification awareness campaigns, reinforces policy adoption through internal messaging, and helps promote the use of updated templates and reporting channels. They also assist in promoting onboarding content, alerts, and reminders related to classification, data security responsibilities, and reporting obligations.

Stakeholder	Role Description
Data Custodian	The Data Custodian is responsible for implementing the operational and technical measures that support the enforcement of classification-based controls. This includes applying system-level protections (e.g., encryption, logging, access configurations) and ensuring that controls match classification levels as defined in the National Data Classification Policy. The Custodian also collaborates with security and governance teams on control testing and risk mitigation.
Data Committee	In the context of this QDKC, the committee reviews and approves critical governance procedures such as the classification escalation and resolution process (6.1.E), endorses classification audit findings, and ensures cross-functional accountability. It also coordinates with the National Data Governance Office (DGO) where required.

1.7 Key Success Factors

Regulatory Awareness and Alignment: Ensure that all data-related activities within the Entity comply with national regulations, including the National Information Assurance Standard, Personal Data Privacy Protection Law, National Data Classification Policy, Cloud First Policy, the Right to Access Information Law, and the Cybercrime Prevention Law.

Operational Integration of Classification: Incorporate data classification into documentation templates, metadata catalogs, and user workflows to ensure that sensitivity levels are clearly defined, consistently applied, and easily understood across the Entity.

Clear Escalation and Resolution Mechanisms: Establish transparent, well-governed processes to investigate and resolve data misclassification, misuse, and non-compliance with security or privacy policies.

Independent Oversight and Review: Regularly engage third-party reviewers or internal audit teams to evaluate the effectiveness of classification practices, adherence to regulatory requirements, and ensure ongoing compliance.

Governance-Endorsed Processes: Obtain formal approval from the Entity's Data Committee for classification escalation procedures and ensure all key stakeholders are aware of their roles in maintaining regulatory compliance.

Culture of Privacy and Security: Promote accountability and best practices across teams to foster a proactive culture of data security and privacy by promoting awareness and enabling a unified approach to data security, privacy, and classification

Security by Design and Default: Integrate security and privacy principles into the earliest stages of system and platform design. Ensure encryption, access controls, audit trails, and logging are configured as standard components—not afterthoughts—to protect data at rest, in transit, and during processing.

Cross-Functional Collaboration on Security and Privacy: Facilitate regular coordination between IT security teams, risk management, legal/compliance, and data governance stakeholders. Strong collaboration helps ensure that controls are practical, well-understood, and effectively implemented across departments and data flows.

1.8 Compliance with National Data Standards

National Data Standards		QDKC
Control	Specification	Activity
DSPO.1.1 National Regulation Alignment	Covered in - National Information Assurance Standard - Personal Data Privacy and Protection Law - National Data Classification Policy - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law	Covered in - National Information Assurance Standard - Personal Data Privacy and Protection Law - National Data Classification Policy - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law
DSPO.2.1 Data & Information Security	Covered in National Information Assurance Standard	Covered in National Information Assurance Standard
DSPO.2.2 Personal Data Privacy	Covered in Personal Data Privacy and Protection Law	Covered in Personal Data Privacy and Protection Law
DSPO.2.3 Other Regulations	Covered in - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law	Covered in - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law
DSPO.2.4 Data Classification	DSPO.2.4.1 Data Classification Operations F And covered in National Data Classification Policy	6.1 Data Classification Operations And covered in National Data Classification Policy
DSPO.3.1 Regulation Monitoring	Covered in - National Information Assurance Standard - Personal Data Privacy and Protection Law - National Data Classification Policy - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law	Covered in - National Information Assurance Standard - Personal Data Privacy and Protection Law - National Data Classification Policy - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law
DSPO.3.2 Regulation Audit & Improvement	Covered in - National Information Assurance Standard - Personal Data Privacy and Protection Law - National Data Classification Policy - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law	Covered in - National Information Assurance Standard - Personal Data Privacy and Protection Law - National Data Classification Policy - Cloud First Policy - Cybercrime Prevention Law - Right to Access Information Law

2. National Regulation Alignment



2. National Regulation Alignment

This control ensures that the Entity's data security, privacy, classification, and storage practices are aligned with the most current and authoritative national regulations. Before implementing any specification or process in the Data Security, Privacy, and Other Regulations domain, the Entity must review and align its internal practices with the latest version of the following national regulations:

- The National Information Assurance (NIA) Standard, issued by the National Cyber Security Agency (NCSA)
- The Personal Data Privacy Protection Law (PDPPL)
- The National Data Classification Policy
- The Cloud First Policy, issued by the Ministry of Communications and Information Technology (MCIT)
- Cybercrime Prevention Law, issued by the Ministry of Justice
- The Right to Access Information Law, issued by the Ministry of Justice

In cases where these national frameworks conflict with any guidance provided in the National Data Standards, the national laws and policies shall take precedence. Entities must remain vigilant in tracking updates to these policies and ensure that all downstream data-related activities reflect the most current regulatory direction.

Guiding Principles for National Regulation Alignment

1. **Respect Legal Hierarchies:** National laws and policies (e.g., NIA Standard, PDPPL) take precedence over other internal or technical standards and must guide all data governance decisions.
2. **Monitor for Policy Updates:** Ensure Entity teams are regularly informed of changes to national regulations and adjust internal practices accordingly.
3. **Use Standards as Anchors:** Treat national frameworks as the foundational reference point when implementing security, privacy, and classification controls.

3. Data & Information Security



3. Data & Information Security

This section ensures that the Entity establishes and maintains a secure information environment. All responsibilities, requirements, and practices related to data and information security are governed by the National Information Assurance (NIA) Standard, issued and maintained by the National Cyber Security Agency (NCSA).

The NIA Standard provides detailed guidance for managing access control, encryption, vulnerability management, incident response, and other security domains necessary to protect data throughout its lifecycle. Entities are expected to adopt and operationalize the controls defined in the NIA Standard to prevent unauthorized access, data breaches, and system-level threats.

Compliance with this control is outside the scope of the National Data Management Compliance Assessment. Oversight, enforcement, and audits related to information security are under the direct authority of NCSA.

Entities should coordinate closely with their internal Information Security teams to ensure alignment with NIA requirements and maintain readiness for NCSA-led assessments or audits.

Guiding Principles for Data & Information Security

1. **Adopt NIA as the Security Blueprint:** Implement the NIA Standard as the Entity's authoritative guide for information security management.
2. **Embed Security Across the Lifecycle:** Ensure security controls are applied from data creation to disposal, not just at the perimeter.
3. **Coordinate with Information Security Teams:** Treat implementation as a shared responsibility with Information Security experts to ensure proper configuration and oversight.

4. Personal Data Privacy



4. Personal Data Privacy

This control ensures that the Entity protects the privacy of individuals by referencing the Personal Data Privacy Protection Law (PDPPL) of the State of Qatar. The PDPPL governs how personal data must be collected, stored, processed, and shared, with an emphasis on transparency, accountability, and individual rights.

The law outlines the obligations of data controllers and data processors, including requirements for consent, individual rights, lawful processing, breach notification, and third-party sharing. It also mandates appropriate technical and organizational measures to protect personal data from misuse, unauthorized access, or loss.

Enforcement of the PDPPL is overseen by the NCSA, and not through the National Data Management Compliance Assessment conducted by NPC. However, Entities are expected to integrate PDPPL requirements into their broader data governance and security practices.

Entities should collaborate closely with legal, compliance, and information security teams to ensure full alignment with PDPPL obligations and maintain readiness for regulatory reviews or investigations.

Guiding Principles for Personal Data Privacy

1. Transparency, honesty and respect for human dignity
2. Data minimization
3. Accuracy
4. Storage limitation
5. Integrity and confidentiality
6. Purpose limitation
7. Accountability

5. Other Regulations



5. Other Regulations

This section ensures that the Entity aligns with key national regulatory frameworks that impact data storage, processing, and accessibility—specifically the Cloud First Policy and the Right to Access Information Law.

The Cloud First Policy, issued by the Ministry of Communications and Information Technology (MCIT), requires government entities to prioritize cloud-based solutions when procuring or refreshing IT systems. The policy outlines principles for data residency, security, vendor management, and the adoption of endorsed Cloud Service Providers (CSPs). Entities must ensure that their infrastructure and service models are consistent with Cloud First guidelines.

The Cybercrime Prevention Law, issued by the Ministry of Justice, regulates and penalises crimes pertaining to hacking of information systems, information programs, information networks and websites.

The Right to Access Information Law, issued by the Ministry of Justice, establishes the public's right to access information held by government ministries, agencies, and affiliated public institutions. It promotes transparency and accountability, and requires entities to handle information access requests in a lawful and timely manner.

Compliance with these regulations is overseen by the issuing authorities and not through the National Data Management Compliance Assessment. However, entities must integrate these regulatory requirements into their broader data management and governance practices.

Guiding Principles for Other Regulations

1. **Prioritize Cloud by Design:** Follow the Cloud First Policy when procuring or designing IT systems to maximize flexibility, scalability, and compliance.
2. **Enable Public Transparency:** Ensure data handling aligns with the Right to Access Information Law by maintaining well-governed, accessible public data when appropriate.
3. **Treat Compliance as a Strategic Enabler:** Embed regulation alignment into planning and system architecture, not just policy documentation.

6. Data Classification



6. Data Classification

This control ensures that the Entity classifies its data assets in accordance with the National Data Classification Policy, which defines standardized classification levels (C0 to C4) based on sensitivity, confidentiality, and usage context. Proper classification is essential to applying appropriate security, privacy, and access controls across data systems.

While the policy framework and enforcement are governed by the National Cyber Security Agency (NCSA), the operational implementation of classification activities is further defined in the detailed sub-control DSPO.2.4.1 – Data Classification Operations, which is included in this handbook.

Entities must ensure their classification practices reflect national standards and are consistently applied across documents, datasets, platforms, and communications. Classification outcomes must be integrated into metadata, security configurations, and data catalog systems to ensure appropriate handling throughout the data lifecycle.

Compliance with the classification policy is monitored by NCSA, but operational execution of classification (as described in DSPO.2.4.1) falls within the scope of the National Data Management Compliance Assessment conducted by NPC.

However, as part of the Qatar Data Trust Index (QDTI), the entity will evaluate its adherence to the Data Classification control, specifically in DSPO.2.4.1 Specification, which is included in the National Data Security, Privacy, and Other Regulations Domain Standards.

The remaining section of this chapter will detail the below activity to guide the execution of the below:



Guiding Principles for Data Classification

- 1. Understanding the nature of data:** Understanding data is the starting point in the methodology used to classify data. It is important to understand data as it may have a bearing on the way it is handled, stored, secured, processed, or exchanged. We need to understand, if the data is structured or unstructured, what is the source of data, is the data personal or owned by an organization, does it contain in its nature, any kind of risk when it is collected or processed or shared, etc.
- 2. The lifecycle approach:** Data, in its nature is changing. Therefore, classification may change during its lifecycle. Data could be at many different stages such as: creation, import, movement, modification, use, copying, storage, erasure or removal, restoration. Therefore, the process of classifying data must consider data lifecycle. The stages of data management lifecycle are addressed in the next section of this document.
- 3. Classifying based on risk assessment:** The primary purpose of the data classification process is to take an approach that makes it easier for organizations to protect them from potential risks. Therefore, risk assessment is one of the basic principles that must be considered when classifying data, which determines the sensitivity and importance of this data for the work carried out by the organization.
- 4. Balancing Needs:** It is important to consider the balance and proportionality between the risks that threaten the data, and the level of classification that is chosen. The data classification process must achieve the most appropriate classification level which is as low as possible but as high as necessary, along with the necessary level of protection without exaggeration and without adding any administrative, financial, or technical burdens that may constitute an obstacle to the conduct of business within the organization.
- 5. Establishing Data Governance:** To ensure the success of Data Classification within the organization, it is important that the business establishes a suitable governance framework. It is recommended that a person within the management owns the data classification program and is accountable for its implementation and adoption within the organization. The process of classifying data does not belong to a single person or entity, but rather requires concerted efforts within the organization to ensure that the process is implemented in accordance with the principles and best practices. A high-level governance must be established across the organization with clearly defined roles and responsibilities for the different stakeholders within the organization.

6.1 Data Classification Operations

Data Classification Operations define the set of minimum practices that each Entity must implement to operationalize the National Data Classification Policy. This includes embedding classification labels into templates and metadata, applying visual and automated classification indicators, and establishing governance mechanisms to monitor, escalate, and resolve classification-related issues.

These operations ensure that classification is not a one-time exercise, but an ongoing, integrated part of how data is created, labeled, stored, and shared. By embedding classification into documentation practices, digital systems, and metadata catalogs, Entities can ensure appropriate protection, access control, and handling of data assets based on their sensitivity.

This activity also requires Entities to introduce escalation channels for classification misuse, ensure metadata consistency in the Data Catalog, and validate classification efforts through independent review. These operational steps form the basis for assessing compliance with the classification control under the National Data Management Compliance Assessment.

The following steps guide the Entity through implementing the foundational operational requirements of data classification.

Process – Data Classification Operations

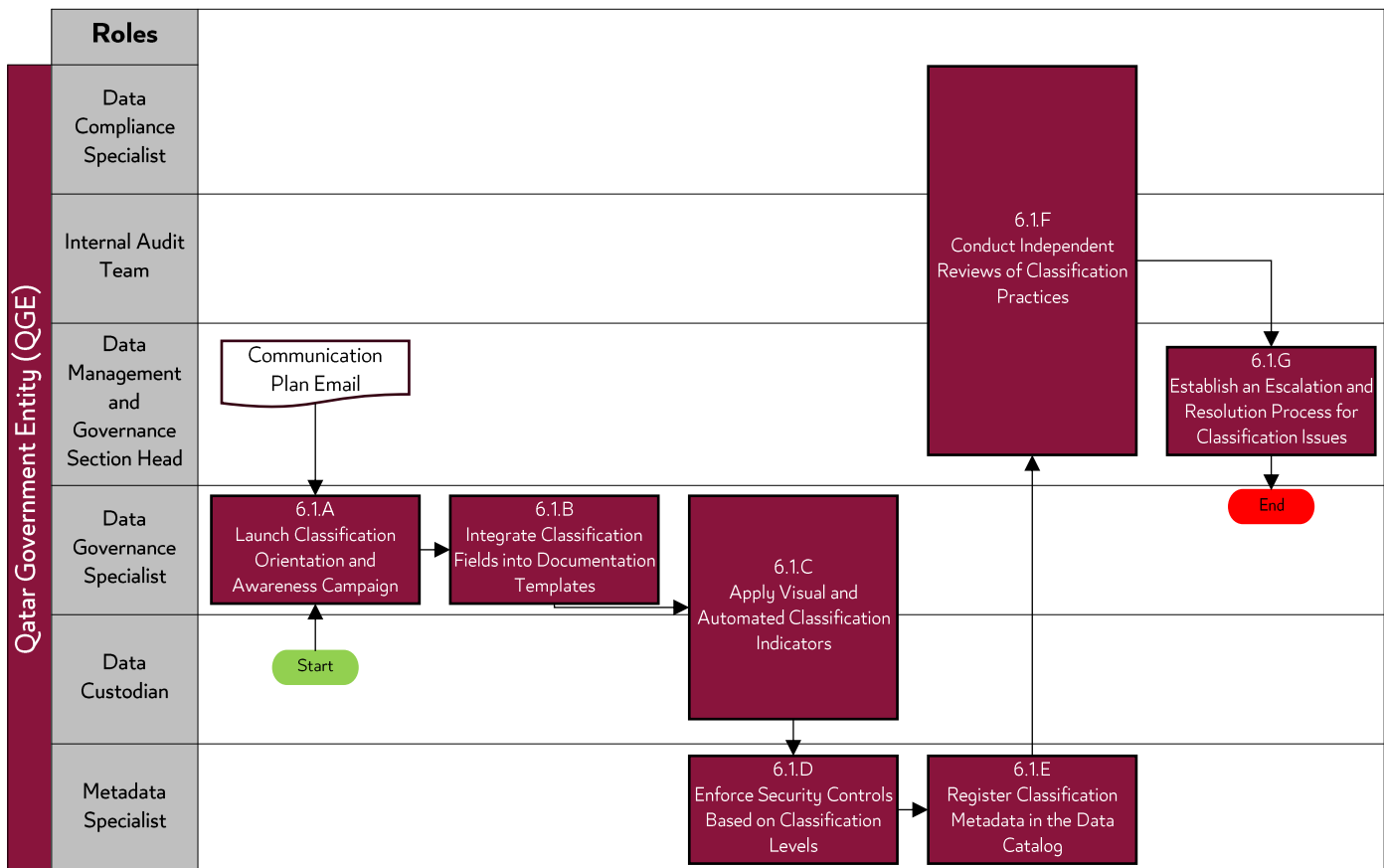


Figure 1: Data Classification Operations Process Map

Legend: Process Step Decision Process Start Process End Document Off-Page Reference

6.1.A
(1/2)

Launch Classification Orientation and Awareness Campaign: This step guides the Entity to ensure that all staff are aware of the National Data Classification Policy, understand their individual responsibilities, and know how to correctly classify documents, emails, and other unstructured content. This is a critical enabler of classification enforcement—without it, users may misapply labels or omit classification altogether. The Data Governance Specialist is responsible for leading this step, in collaboration with the Information Security Team and Internal Communications Team.

- i. **Develop targeted communication materials:** The Data Governance Specialist prepares a set of engaging, easy-to-understand materials to introduce classification concepts.
 - a. Create a policy summary one-pager/email explaining C0–C4 levels, examples, and consequences of misclassification.
 - b. Develop visual aids (e.g., posters, banners, infographics) showing where and how to classify documents.
 - c. Prepare an FAQ document and quick-start guide to be embedded in the document and content management tool.

Asset Guidance

Illustrative

The Change Management Communication Plan Email Template is a sample email template that the Entity can leverage to announce the integration of classification fields into documents.

Subject: [IMPORTANT] Notification of [Change Description] – Please Review

Dear [Recipient Name/Team],

We would like to inform you of an important change that will take effect as of [Date]. This change relates to [briefly describe the change, e.g., a new data governance policy, system update, or process change] and is part of our ongoing efforts to improve [mention the purpose of the change, e.g., data quality, compliance, or operational efficiency].

What Is Changing?

- [Clearly state what is being changed, e.g., "We are updating our data governance framework to include new privacy regulations."]
- [If applicable, include any specific systems or processes affected by the change.]

Why Is This Change Happening?

- This change is necessary to [explain the reason, e.g., "align with new regulatory requirements," "improve data accuracy and reporting," or "support our data management strategy"].

How Does This Impact You?

- [Clearly explain how the change will affect the recipient's role, team, or department, e.g., "You will need to follow the updated policy for handling customer data."]
- [If applicable, mention any new responsibilities, processes, or systems the recipient needs to be aware of.]

What Do You Need to Do?

- [Provide clear instructions on what actions the recipient should take, e.g., "Review the updated policy by [Date]" or "Attend the training session on [Date]."]
- [If no immediate action is required, state that clearly, e.g., "No action is required from you at this time."]

Support and Resources

We have provided the following resources to assist you with this change:

- [Link to any documents, training materials, or guides]
- [Provide contact information for any support teams or help desks that can assist with questions.]

Next Steps

- [Outline the next steps, e.g., "We will follow up with a training session on [Date]" or "Please reach out to [Support Contact] if you have any questions."]
- [If applicable, remind the recipient of key deadlines, e.g., "Please ensure you complete the necessary steps by [Date]."]

Thank you for your cooperation in ensuring a smooth transition. Your understanding and collaboration are crucial to the success of this change.

If you have any questions or concerns, please don't hesitate to contact [Support Contact/Your Team's Name] at [email/phone number].

Best regards,
[Your Name]
[Your Position]
[Your Department]
[Contact Information]

6.1.A
Cont.
(2/2)

- ii. **Conduct awareness sessions across departments:** The Data Governance Specialist organizes orientation sessions to introduce the classification framework and answer questions.
 - a. Schedule sessions for each department, prioritizing high-volume content creators (e.g., legal, planning, HR, comms).
 - b. Use real-world examples to show how classification applies to common content types (e.g., meeting minutes, reports).
 - c. Record at least one session for on-demand access via the Entity's intranet or LMS.
- iii. **Reinforce awareness through embedded nudges and channels:** The Information Security Team and the Internal Communications Team support ongoing reminders using Entity platforms.
 - a. Embed classification reminders or pop-ups into frequently used document templates or file-saving workflows.
 - b. Publish reminders and tips in internal newsletters, email footers, or intranet banners.
 - c. Include classification training in onboarding checklists and role-specific induction programs.

6.1.B

Integrate Classification Fields into Documentation Templates: This step guides the Entity to embed data classification fields into all official documentation templates, enabling employees to easily apply the appropriate classification when creating content. This ensures consistency, visibility, and accountability across all document types while reinforcing the National Data Classification Policy. The Data Governance Specialist is responsible for executing this step, in coordination with the Information Security Team, and the Internal Communications Team.

- i. **Identify high-use documentation templates across the Entity:** The Data Governance Specialist coordinates with departments to catalog commonly used templates.
 - a. Collect templates used for reports, memos, meeting minutes, policy documents, emails, and official correspondence.
 - b. Prioritize templates used for interdepartmental, external, or public communication.
 - c. Ensure coverage across both Arabic and English template versions.
- ii. **Add classification fields to cover pages, headers, and footers:** The Data Governance Specialist updates all approved templates to include standard classification input areas.
 - a. Include a "Classification Level" field on the cover page of each template, with options: C0 (Public), C1 (Internal), C2 (Restricted), C3 (Secret), C4 (Top Secret)
 - b. Add the selected classification to the header or footer on all subsequent pages.
 - c. Ensure formatting is standardized (e.g., bold font, color-coded if applicable) and integrated into the document style.
- iii. **Publish and communicate updated templates to all staff:** The Internal Communications Team distributes the updated templates and communicates their mandatory use.
 - a. Replace outdated versions in all shared drives, template libraries, and internal portals.
 - b. Notify staff via internal comms channels (email, Teams, newsletter) about the new classification-ready templates.
 - c. Provide a brief user guide or pop-up prompt embedded in templates to explain how to select the correct classification.

6.1.C

Apply Visual and Automated Classification Indicators: This step guides the Entity to enforce proper classification practices by embedding visual cues (e.g., watermarks, color codes) and, where feasible, automation into its document workflows. These indicators reinforce the classification selected by employees and reduce the risk of mislabeling or inappropriate document handling. The Data Governance Specialist and Data Custodian are responsible for leading this step, in collaboration with the Information Security Team, IT Team., and the Internal Communications Team

- i. **Define visual standards for classification indicators:** The Data Governance Specialist establishes a clear visual identity for each classification level.
 - a. Set color coding conventions for each classification level:
 - Green for **C0 – Public**
 - Blue for **C1 – Internal**
 - Orange for **C2 – Restricted**
 - Red for **C3 – Secret**
 - Dark Red for **C4 – Top Secret**
 - b. Define placement and formatting rules for headers, footers, borders, or watermarks.
 - c. Apply visual standards across both Arabic and English templates to ensure consistency.
- ii. **Configure watermarking and automated labelling features:** The Information Security Team, with input from the Data Custodian and Data Governance Specialist, sets up automated visual enforcement in document systems.
 - a. For Microsoft Word, Excel, and PowerPoint templates:
 - Configure default watermark options based on selected classification (e.g., “C2 – Restricted” diagonally across pages).
 - b. For email communications (e.g., Outlook):
 - Enable default footer tags or banner notices based on classification tags.
 - c. For document management systems (e.g., SharePoint, file servers):
 - Apply classification-based access banners or metadata tags on upload.
- iii. **Communicate and train users on classification indicators:** The Data Governance Specialist, supported by the Internal Communications Team, informs users of how visual and automated indicators are applied.
 - a. Share before-and-after examples showing how classification is reflected in document layout.
 - b. Issue a reference guide explaining what each color and watermark means, and when it applies.
 - c. Include indicator training as part of the broader classification orientation (see Step 6.1.A).

6.1.D

Enforce Security Controls Based on Classification Levels: This step ensures that the Entity enforces appropriate technical and administrative security controls aligned with the classification level assigned to each dataset, in full compliance with the National Data Classification Policy. The Data Custodian leads this step, in close collaboration with the Information Security Team, System Owners, and Data Governance Specialist.

- i. **Identify applicable protection controls based on classification:** In alignment with the National Data Classification Policy, use the CIA-based classification matrix (Confidentiality, Integrity, Availability) and the classification label (C0–C4) to determine security requirements.
 - a. For example:
 - C3–C4 (Secret/Top Secret): Require encryption at rest and in transit, strong access controls, logging, and multi-factor authentication.
 - C2 (Restricted): Role-based access control (RBAC), watermarking, and transmission safeguards.
 - C1 (Internal): Internal access restrictions with minimal technical barriers.
 - C0 (Public): No protection controls unless required by business policy.
- ii. **Apply controls according to data state.** Ensure that controls vary based on how data is handled:
 - Data-at-rest: Disk-level encryption, secure storage policies.
 - Data-in-transit: TLS encryption, email DLP rules.
 - Data-in-use: Screen masking, session timeout, export restrictions.
- iii. **Embed controls into platforms and document management systems:** Coordinate with IT and platform teams to ensure controls are technically enforced.
 - a. Configure Document and Content Management tools, analytics platforms, SharePoint, and network shares to restrict access and apply protections dynamically based on classification metadata.
- iv. **Monitor and test enforcement mechanisms:** Periodically verify that classification-based protections are working as intended.
 - Conduct sample-based access reviews.
 - Simulate breach or misuse scenarios to test control strength.
 - Log incidents and integrate into broader cybersecurity monitoring.

6.1.E

Register Classification Metadata in the Data Catalog: Ensure that the classification levels assigned to data assets are consistently recorded as metadata attributes in the Entity's Data Catalog. This step operationalizes classification enforcement across digital systems by embedding classification into metadata structures, enabling appropriate access control, visibility, and governance. The Metadata Specialist leads this activity in collaboration with the Data Stewards, and Data Owners

- i. **Populate classification metadata for all registered assets:** Apply classification levels in alignment with the national data classification policy to existing and newly registered datasets.
 - a. Tag all existing cataloged datasets with the appropriate classification level
 - b. Ensure classification is applied as part of all new metadata registration workflows
 - c. Validate completeness of classification metadata across the catalog
 - Run completeness reports to flag missing or inconsistent classification values
 - Require data owners or stewards to address any gaps
- ii. **Monitor and govern classification metadata over time:** Ensure classification metadata remains accurate and up to date.
 - a. Establish periodic reviews of classification metadata accuracy
 - Schedule annual or bi-annual reviews for cataloged datasets
 - Prioritize reviews for high-sensitivity assets (C3 and C4)
 - b. Maintain logs of classification changes in metadata history
 - Enable traceability for audits, incidents, or investigations
 - c. Integrate classification metadata with other data governance tools
 - Use classification metadata to support access control, reporting, and automated workflows
 - Align metadata policy enforcement with other governance domains

6.1.F
(1/3)

Conduct Independent Reviews of Classification Practices: Appoint an independent reviewer—either an internal audit function not involved in data classification or an external assurance provider—to periodically assess the Entity's data classification activities for consistency, accuracy, and alignment with the National Data Classification Policy.

Independence is essential to ensure the review is unbiased, credible, and free from conflicts of interest. An internal audit team may be suitable if it operates independently from data governance and reports directly to senior management or the audit committee. In high-risk or sensitive environments, or where deep technical expertise is required, an external party (e.g., compliance assessor) may be engaged.

This external validation mechanism enhances transparency, mitigates organizational bias, and supports continuous improvement in classification practices. The Data Management and Governance Section Head is responsible for commissioning and overseeing this activity alongside the Internal/External Audit Team and Data Compliance Specialist, in collaboration with the Information Security and Legal Team.

- i. **Determine the systems, data domains, and documentation types to be included in the audit:** Ensure reviews cover both operational execution and policy adherence.:
 - Prioritize systems handling C2–C4 classified data

6.1.F
Cont.
(2/3)

- Include a representative sample of metadata entries, and access logs
- Apply strict access control and data handling measures when engaging third-party reviewers:
 - Grant access only to required documentation, not to full datasets.
 - Require signed confidentiality agreements and NDA clauses.
 - Conduct onboarding with the Information Security Team to brief auditors on data sensitivity and control expectations.
 - Monitor and log auditor access activity using audit trail systems.
- b. Define audit criteria based on the National Data Classification Policy and DSPO.2.4.1 specifications
 - Review for completeness of classification, accuracy of assigned levels, proper use of indicators, and catalog registration
- c. Develop or adapt an evaluation checklist to guide the independent review process
 - The checklist should cover key components such as:
 - Presence and visibility of classification in document templates
 - Accuracy and completeness of classification metadata in the catalog
 - Application of required visual indicators (headers, watermarks, etc.)
 - Enforcement of access controls based on classification level
 - Evidence of classification training and awareness among users
 - Existence of escalation and resolution records for classification breaches
 - Include yes/no validations, issue severity scoring, and recommendations
- ii. **Engage a qualified third-party or internal assurance function:** Ensure the review is unbiased and methodologically sound.
 - a. Appoint an independent auditor, consultant, or internal audit team not directly involved in classification activities:
 - Verify that the party has experience with data governance, security, or compliance audits
 - b. Issue a formal terms of reference for the review:
 - Specify roles, timelines, deliverables, and confidentiality requirements
 - c. Coordinate access to necessary documentation and systems:
 - Ensure the reviewer has visibility into classification templates, metadata systems, and escalation workflows
- iii. **Document findings and drive remediation actions:** Ensure review outcomes are used to improve classification maturity.
 - a. Compile and publish a formal audit report with key findings, root causes, and improvement opportunities:
 - Share with the Data Committee, DGO, and any relevant internal governance boards

6.1.F
Cont.
(3/3)

- b. Track recommendations and assign accountability for remediation:
 - Use issue tracking tools (e.g., JIRA, AuditBoard, or Microsoft Planner) to manage follow-ups. or internal audit systems to manage follow-ups
- c. Use audit results to inform updates to policies, training, templates, and catalog processes:
 - Close the loop by incorporating lessons learned into governance routines

6.1.G
(1/2)

Establish an Escalation and Resolution Process for Classification Issues: Implement a formal process to identify, investigate, and resolve issues or complaints related to data misclassification, misuse of sensitive data, or non-compliance with the National Data Classification Policy. This step ensures accountability, transparency, and the ability to take corrective action in a timely manner. The process must be approved by the Data Committee and communicated to all relevant stakeholders. The Data Management and Governance Section Head owns this process, in coordination with the Information Security Team, Legal Team, and the Data Committee.

- i. **Design a structured and transparent escalation process:** Ensure that issues are captured, tracked, and handled efficiently.
 - a. Define entry points for raising classification issues or concerns:
 - Channels may include service desk tickets, email aliases, or intranet forms
 - b. Outline the workflow for issue investigation, analysis, and resolution:
 - Include triage, root cause analysis, classification reassessment, and policy remediation (if needed)
 - Ensure the process includes timestamps and clearly assigned responsibilities
 - c. Maintain a historical log of all classification-related escalations:
 - Use a central system or register with audit trail capabilities
 - Record issue type, classification level, severity, resolution time, and corrective actions taken
- ii. **Ensure cross-functional governance and approval:** Involve key stakeholders across legal, information security, data governance, and risk functions to ensure the escalation process is comprehensive, enforceable, and aligned with both regulatory and operational requirements.
 - a. Present the draft escalation process to the Data Committee for review and approval:
 - Ensure that legal, compliance, and information security teams are included in the review
 - Address recommendations from internal audits or classification reviews (6.1.D)
 - b. Define roles and responsibilities across stakeholder groups:
 - For Example:
 - **Reporter:** Anyone identifying the issue
 - **Investigator:** Data Steward, Data Owner, or Metadata Specialist
 - **Approver:** Data Committee, Legal, or DGO depending on impact

6.1.G
 Cont.
 (2/2)

- c. Define roles and responsibilities across stakeholder groups:
- Critical (C3/C4 misuse or breach) – response within 24 hours
 - Moderate (C2/C1 inconsistency) – response within 5 business days

iii. **Communicate the escalation process to all key stakeholders:** Promote awareness and ensure the process is actively used.

- a. Publish the approved escalation process and contact channels on the Entity's intranet or data governance portal
- b. Conduct awareness sessions for system owners, data stewards, and catalog users
- Include in onboarding and data policy training materials
- b. Reinforce obligations in the event of a classification breach involving personal or sensitive data:
- In cases of compromised data, require that the Data Committee and the National Data Governance Office (DGO) be notified within 72 hours as per DSPO.2.4.1

RACI Matrix - Data Classification Operations

Indicative

Sr No.	Activity	Data Committee	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	Information Security Team	Data Custodian	Metadata Specialist	Data Owners	Data Stewards	IT Team	Internal Communications Team	Internal Audit Team	Data Compliance Specialist	System Owners	Legal Team
6.1.A	Launch Classification Orientation and Awareness Campaign			A	R	C						C				
6.1.B	Integrate Classification Fields into Documentation Templates			A	R	C						C				
6.1.C	Apply Visual and Automated Classification Indicators			A	R	C	R				C	C				
6.1.D	Enforce Security Controls Based on Classification Levels			A	C	C	R				C				C	
6.1.E	Register Classification Metadata in the Data Catalog			A				R	C	C						
6.1.F	Conduct Independent Reviews of Classification Practices		A	R		C							R	R		C
6.1.G	Establish an Escalation and Resolution Process for Classification Issues	C	A	R	I	C	I	I	I	I	I	I	I	I	I	C

RACI Matrix Legend: **R:** Responsible **A:** Accountable **C:** Consulted **I:** Informed

Based on this Activity, the Entity can

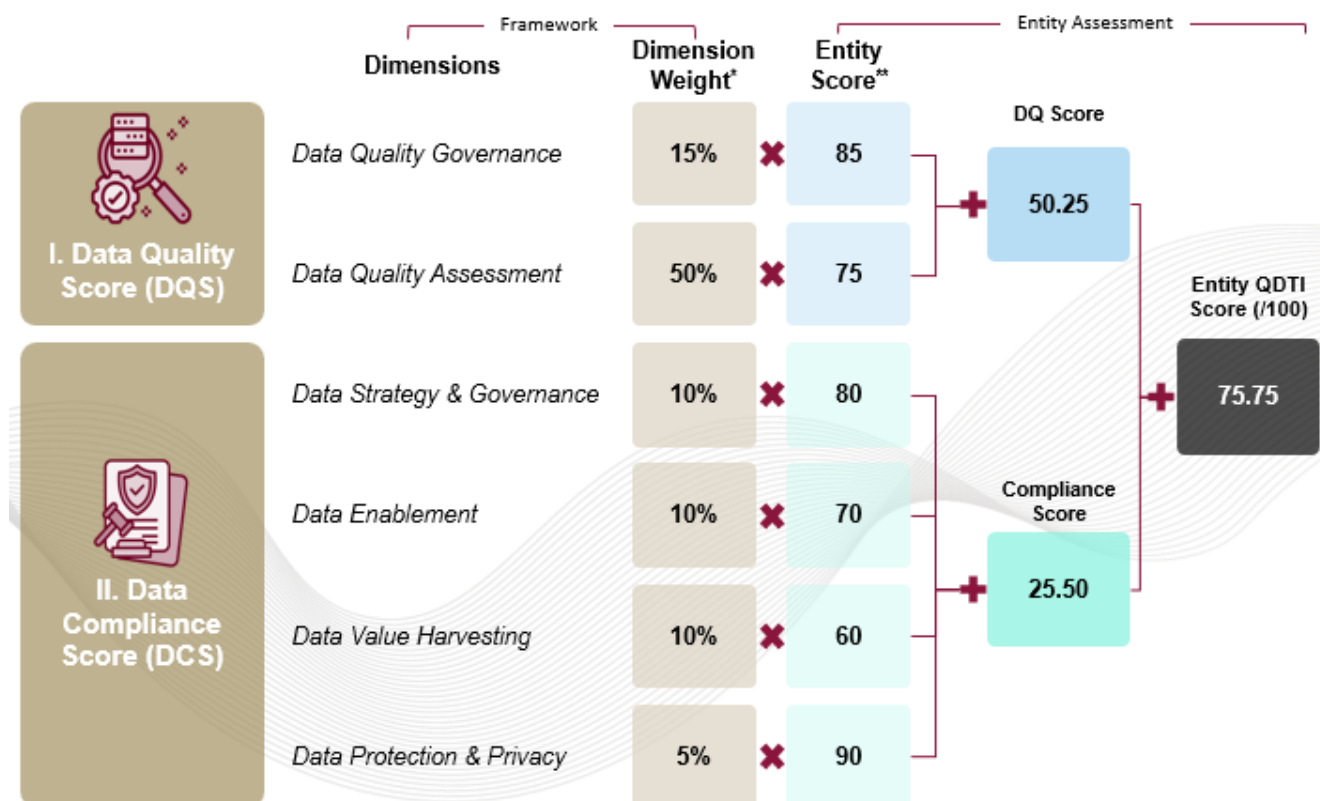


Establish Data Classification Operations

6.2 QDTI

The Qatar Data Trust Index (QDTI) is designed to measure and enhance data integrity across national entities by promoting adherence to governance standards and ensuring the accuracy, reliability, and responsible management of data. This initiative aims to build trust and support a robust digital economy. The overall QDTI score is derived from two dimensions: the Data Quality Score (DQS) and the Data Compliance Score (DCS), which together combine to determine the Entity's QDTI score.

This section outlines the steps needed to gather the necessary information for calculating the DCS.



*Note: The sum of the weights across all dimensions should add up to 100%

**Note: This score is calculated by computing the weighted average score of all the sub-dimensions under each respective Dimension (scores are on a scale of 0 to 100)

Figure 2: Illustrative QDTI Scoring Methodology for an Entity

6.2.A

Initiate Data Security, Privacy, and Other Regulations Compliance Assessment: The Data Management and Governance Section Head assigns the Data Compliance Specialist to oversee the assessment process. The specialist is responsible for managing the evaluation of the Entity's adherence to the Data Classification control, specifically in DSPO.2.4.1 Specification, which is included in the Data Security, Privacy, and Other Regulations domain.



Key Message / Information

The Data Security, Privacy, and Other Regulations Domain falls under the Data Defense and Resilience Dimension in the National Data Management Framework and, consequently, within the QDTI Dimension.

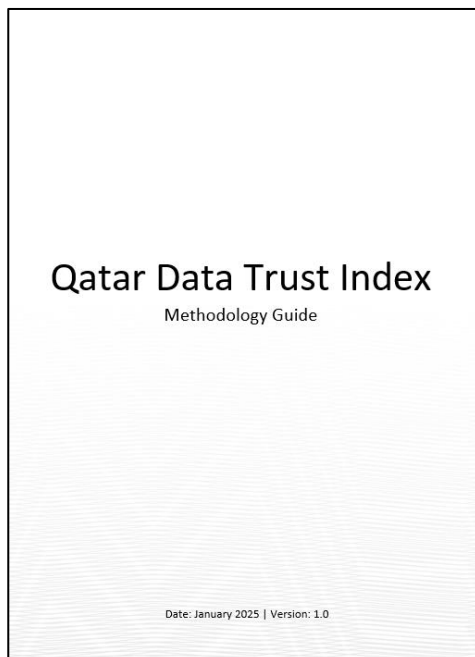
6.2.B

Conduct Data Security, Privacy, and Other Regulations Assessment: Initiate the self-assessment to evaluate adherence to the National Data Security, Privacy, and Other Regulations Domain Standards. This assessment will ensure compliance and accountability while identifying areas for improvement.

Asset Guidance

The **Qatar Data Trust Index Methodology Guide** can be leveraged to guide the Entity through the steps required to conduct the self-assessment.

Illustrative



Asset Guidance

The **QDTI Assessment Template** can be used to document compliance with the National Data Standards. This template is intended for use prior to the DGO launching the self-assessment on its platform to calculate the overall QDTI Score.

Illustrative

Domain	Control	Control Description	
DSPO	DSPO.1.1: National Regulation Alignment	The Entity shall review and align to the latest version of the approved NIAS, PDPPL, NDCP, CFP, and RAIL.	
DSPO	DSPO.1.1: National Regulation Alignment	The Entity shall review and align to the latest version of the approved regulations and in case of any conflict,	
DSPO	DSPO.2.2: Personal Data Privacy	The PDPPL, It offers advice and guidance, promotes good practice, carries out audits and advisory visits,	
DSPO	DSPO.2.3: Other Regulations	The regulations requires that entities, when embarking on projects involving new IT systems or technology	
DSPO	DSPO.2.4: Data Classification	This control mandates that the Entity shall classify its data assets in alignment with the NDCP, and comply	

Specification	Capability Level	Control Specification	Compliance
National Information Assurance Standard	As applicable in other regulation(s)	-	Not Applicable
Personal Data Privacy and Protection Law	As applicable in other regulation(s)	-	Not Applicable
Personal Data Privacy and Protection Law	As applicable in other regulation(s)	-	Not Applicable
Cloud First Policy	As applicable in other regulation(s)	-	Not Applicable
DSPO.2.4.1: Data Classification Operations	Foundational	To operationalize the National Data Classification Policy, the Entity shall, at a minimum, do the following: SS1.1	Compliant



Key Message / Information

The DGO will launch the self-assessment on its platform and will provide toolkits and host workshops to guide entities through the self-assessment process during the first year.

6.2.C

Submit Data Security, Privacy, and Other Regulations Score to the DGO: Submit the Data Catalog and Metadata Management Compliance Score to the DGO for evaluation



Key Message / Information

The DGO will calculate the Entity's overall Qatar Data Trust Index (QDTI) score only after the Entity has completed both the Data Quality Score (DQS) assessment and the required self-assessments for all other data management domains to determine the Data Compliance Score (DCS). Once all assessments are completed, the DGO will aggregate the compliance scores across domains to finalize the DCS, which will then be combined with the DQS to determine the Entity's overall QDTI score.



Key Message / Information

This compliance score does not include the other regulations (National Information Assurance Standard, Personal Data Privacy Protection Law, National Data Classification Policy, Cloud First Policy, the Cybercrime Prevention Law, and the Right to Access Information Law) outlined in this document that are not under the oversight of NPC.

RACI Matrix - QDTI

Indicative

Sr No.	Activity	DGO	Data Management & Security Director	Data Management and Governance Section Head	Data Compliance Specialist	Data Governance Specialist
6.2.A	Initiate Data Security, Privacy, and Other Regulations Compliance Assessment		I	A	R	
6.2.B	Conduct Data Security, Privacy, and Other Regulations Assessment		I	A	R	C
6.2.C	Submit Data Security, Privacy, and Other Regulations Score to the DGO	I	I	A	R	I

RACI Matrix Legend: **R:** Responsible **A:** Accountable **C:** Consulted **I:** Informed

Based on this Activity, the Entity can



Calculate DSPO Compliance Score

7. Regulation Monitoring



7. Regulation Monitoring

This section ensures that the Entity continuously monitors its compliance with national cybersecurity and data protection regulations through the implementation of a structured information security management system (ISMS). An ISMS is a framework of policies, procedures, and controls designed to systematically manage and mitigate information security risks, protect sensitive data, and ensure ongoing compliance.

Compliance with the regulations referenced in this handbook is overseen by the respective issuing authorities and not through the National Data Management Compliance Assessment (e.g., the Cloud First Policy is overseen by MCIT). However, compliance to activity 6.1 (Data Classification Operations) will be covered under the National Data Management Compliance Assessment by NPC.

Regulation monitoring helps Entities stay informed of emerging threats, updated security practices, and evolving regulatory requirements. While this QDKC does not define how monitoring must be executed, Entities are expected to implement the guidance set forth in the NIA Standard, including regular internal audits, risk assessments, incident tracking, and reporting.

Maintaining an active monitoring practice is essential for upholding data security, minimizing risk, and supporting broader national cybersecurity objectives.

Guiding Principles for Regulation Monitoring

1. **Monitor Continuously, Not Periodically:** Treat regulation monitoring as an ongoing function, not a one-time task.
2. **Use the NIA Standard as a Benchmark:** Leverage the National Information Assurance Standard as the guide for monitoring activities.
3. **Link Monitoring to Risk Management:** Implement clear workflows for raising and resolving classification concerns, including regulatory notification pathways.
4. **Promote Accountability Across All Units:** Make regulation monitoring a shared responsibility, not just the domain of IT or security. Business owners, data stewards, and system owners must actively participate in identifying, tracking, and reporting regulatory risks.
5. **Embrace Continuous Improvement:** Treat monitoring outcomes as inputs for system and policy enhancement. Use findings from incident reports, or gap analyses to improve controls, update classification practices, and strengthen regulatory alignment over time.

8. Regulation Audit & Improvement



8. Regulation Audit & Improvement

This section ensures that the Entity regularly audits its compliance with the regulations referenced and continuously improves its practices based on audit findings, emerging risks, and evolving legal and policy requirements.

The NIA Standard outlines how Entities should conduct internal security audits, address vulnerabilities, and implement corrective action plans. While the specifics of audit execution are outside the scope of this QDKC, Entities are expected to adopt and operationalize NIA-prescribed practices as part of their information security management systems. The audit scope must reflect the broader regulatory landscape beyond cybersecurity, with entities proactively engaging internal audit teams or external reviewers to assess compliance with all other regulations referenced in this QDKC.

Compliance with the regulations referenced in this handbook is overseen by the respective issuing authorities and not through the National Data Management Compliance Assessment. Nonetheless, proactive engagement in audit and continuous improvement activities is essential for reducing risk, supporting national cybersecurity readiness, and building public trust in government-held data.

Guiding Principles for Regulation Audit & Improvement

1. **Audit to Improve, Not Just Comply:** Use audit results to enhance processes, not just satisfy external obligations.
2. **Institutionalize Self-Assessment:** Promote internal checks and balances through periodic self-audits and readiness assessments.
3. **Close the Loop on Findings:** Track all audit recommendations through to resolution and review their impact post-remediation.

9. Appendix



9.1 Templates and Frameworks

Asset No.	Asset Name	Description	File Name
1	Change Management Communication Plan Email Template	Sample email template the Entity can leverage to announce changes across the Entity.	NPC_DGO_QDKC_General_Change Management Communication Plan - Email Template
2	Qatar Data Trust Index Methodology Guide	The Qatar Data Trust Index Methodology Guide can be leveraged to guide the Entity through the compliance self-assessment.	22012025_NPC_QDTI Methodology Guide_V1.0
3	QDTI Assessment Template	The QDTI Assessment Template can be used to document compliance with the National Data Standards.	23012025_NPC_QDTI Assessment Template_V1.0

9.2. Pre-Launch Security and Risk Review for Platforms

Before launching any platform, the Entity's Information Security and Risk Management team must ensure that the development team has responded to all required security and risk assessment questions below and submitted their responses for review and approval.

1. Summarize the objectives of the platform and this initiative
2. What are the expected functional capabilities of the platform in terms of:
 - a. **Users of the platform (Internal, Business, Citizens/Residents, International)**
 - b. **Key Features (Data Acquisition, Processing, Sharing, etc.)**
3. Is this a managed service and what is the agreed tenure?
4. Does the provider have all staff members available locally or operating from other regions?
5. List of functions performed by remote staff
6. What security measures are in place to ensure compliance with local regulations and utmost security and privacy of information assets?
7. What development methodology is being followed (Waterfall/Agile/SAFe)?
8. What are the current release plans/iterations (product features within the platform)?
9. Who are the main internal sections/stakeholders involved in this initiative (e.g. InfoSec, IT, PMO)?
10. Has the team performed thorough Threat Modeling and Comprehensive Risk Assessment?
11. Has the team identified all parties involved in this initiative and performed 3rd party risk assessment covering all parties including the provider itself?
12. Who are the main external stakeholders (vendors and service providers) involved in the platform?
13. Who will be the 3rd parties integrated or have access to the platform (e.g., Gov., service provider, etc.) and type of integration/connectivity?
14. What applicable laws/regulations compliance you need to adhere to aside from QCSF, PDPPL and NIA?
15. Describe your current data protection and privacy practices including classification, labeling and protection across environments (Dev, Test, UAT, Prod)
16. Has the team implemented requirements/recommendations related to security controls (e.g. Secure Identity, Network Security, Endpoint Security)?
17. Has the team developed and maintained an inventory of all assets related to this platform with classification levels and ownership assigned?
18. Has the platform been designed and built in accordance with the principles of Privacy by Design and Default?
19. Has the team developed an architecture document addressing security requirements and aligned with international CS frameworks and standards such as OWASP, NIST, CISA, CIS, and Zero Trust?
20. Has the team adopted Change Management process, including approval workflows, risk assessment, rollback, and post-implementation review?

21. Has the team developed and implemented Incident Management practices with appropriate logging and analysis?
22. Has the team defined and implemented secure development lifecycle (SDLC) practices?
23. Has the team performed any security-related activities during design, planning, development, and implementation?
24. Has the team planned for independent security assessment and penetration testing prior Go-Live?
25. Has the team identified Continuity and Disaster Recovery (DR) requirements and planned accordingly?
26. Does the team ensure alignment with NCSA AI Adoption Guidelines and industry standards for AI Ethics, Security, and Privacy?



المجلس الوطني للتخطيط
National Planning Council

دولة قطر • State of Qatar



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency