

National Data Management Guidelines

Document & Content Management



Table of Contents

1. Document & Content Management Domain Introduction

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

2. Document & Content Management Policy

- Overview
- 2.1 Document & Content Management Policy Creation
- 2.2 Document & Content Management Policy Publication

3. Document & Content Management Planning

- Overview
- 3.1 Document & Content Management Plan

4. Document & Content Management Assessment & Design

- Overview
- 4.1 Inventory Assessment
- 4.2 Document Prioritization
- 4.3 Workflow Prioritization
- 4.4 Information Architecture

5. Document & Content Management Implementation

- Overview
- 5.1 Document & Content Management Tool Implementation
- 5.2 Records & Content Capture
- 5.3 Versioning & Control
- 5.4 Backup & Recovery
- 5.5 Retention & Disposal
- 5.6 Document & Content Metadata
- 5.7 Content Publishing & Delivery

6. Performance Management

Overview

6.1 Document & Content Management KPIs

6.2 Document & Content Management Monitoring & Reporting

6.3 Document & Content Management SLAs

6.4 Document & Content Management Audit

6.5 QDTI

7. Appendix

7.1 Templates and Frameworks

1. Document & Content Management Domain Introduction



1.1 Domain Overview

The Document & Content Management domain focuses on ensuring that unstructured content including documents, records, media, and web content, is securely stored, consistently tagged, efficiently accessed, and governed across its full lifecycle.

Through structured assessment, architecture design, tool implementation, and performance monitoring, entities can manage documents in alignment with Qatar National Data Standards while supporting operational efficiency, and compliance.

This domain enables entities to move beyond fragmented content practices by establishing centralized governance, metadata-driven access, workflow automation, and robust retention and disposal processes, turning content from a risk into a strategic asset.

Organized across 5 phases: Policy, Planning, Assessment & Design, Implementation, and Performance Management, the Document & Content Management domain provides a clear framework to evaluate current capabilities, design future-state structures, configure tools, and continuously optimize governance outcomes.

By following this framework, entities ensure that content is not only well-managed and compliant, but also accessible, searchable, reusable, and resilient, supporting both day-to-day operations and long-term institutional knowledge.

Key Components of the Document & Content Management Domain

Document & Content Management Policy

This foundational phase defines the formal governance structure for how documents and content are managed across the Entity. It establishes the policies that ensure content is created, stored, accessed, retained, published, and disposed of in a secure, standardized, and compliant manner. By setting clear expectations and accountability, this phase enables consistent lifecycle management and supports alignment with Qatar's National Data Standards.

- **Document & Content Management Policy Creation:** Outlines the process for developing the Entity's Document & Content Management Policy, including its scope, objectives, governance roles, and alignment with national and internal standards.
- **Document & Content Management Policy Publication:** Details how the approved policy is reviewed, finalized, and formally published through the Entity's internal channels.

Document & Content Management Planning

This phase establishes the strategic planning foundation for governing unstructured content across the Entity. It ensures that document and content management efforts are grounded in current-state realities, aligned with national standards, and supported by a practical, phased roadmap for improvement and implementation.

- **Document & Content Management Plan:** Combines a baseline maturity assessment with a structured implementation roadmap. The roadmap translates insights from the maturity assessment into a sequenced plan of initiatives, ownership, timelines, and priorities to guide effective and sustainable implementation.

Document & Content Management Assessment & Design

This phase translates policy into actionable design by helping the Entity assess its current document landscape, prioritize high-value content and workflows, and design the structural foundation for effective content governance. It prepares the Entity for implementation by identifying what needs to be managed, how it should be structured, and where governance efforts should be focused.

- **Inventory Assessment:** Establishes a baseline view of all systems and repositories used to store documents and content, capturing system attributes, document types, volumes, and risks related to redundancy or uncontrolled storage.
- **Document Prioritization:** Guides departments in identifying and ranking their most critical documents and content assets based on operational importance, compliance risk, and user demand.
- **Workflow Prioritization:** Identifies and ranks the most important document-related workflows across the Entity for potential automation.
- **Information Architecture:** Designs the structural framework for organizing documents and content, including metadata, taxonomies, controlled vocabularies, navigation structures, and user interaction flows to support governance and usability.

Document & Content Management Implementation

This phase activates the structures and governance models designed in earlier phases by configuring the Document and Content Management Tool, capturing content, enforcing lifecycle controls, and enabling structured publishing. It operationalizes the Entity's document governance model and ensures that content is not only governed by policy but also managed effectively in practice.

- **Document & Content Management Tool Implementation:** Guides the selection, configuration, and deployment of the document and content management tool.
- **Records & Content Capture:** Establishes standardized processes to capture and classify both new and legacy content using structured metadata.
- **Versioning & Control:** Enforces change tracking, version history, and rollback capabilities across the DCM Tool, while enabling real-time collaboration and auditability.
- **Backup & Recovery:** Integrates the DCM Tool into the Entity's broader backup and recovery framework, with differential and incremental backup.
- **Retention & Disposal:** Implements retention rules and controlled disposal processes to manage document lifecycles in alignment with policy and regulatory requirements.
- **Document & Content Metadata:** Applies and enriches metadata tagging within the tool to support classification, access control, search, sensitivity tagging, and inter-document relationships.
- **Content Publishing & Delivery:** Defines the channels, approvals, and formatting rules for publishing content to internal and external platforms.

Performance Management

This phase ensures that document and content governance is not only implemented but actively measured, monitored, and improved over time. It provides processes to assess system usage, SLA compliance, audit readiness, and overall content governance maturity, enabling evidence-based oversight and continuous optimization.

- **Document & Content Management KPIs:** Defines and tracks performance indicators related to system usage, user adoption, metadata tagging, and digitization progress.
- **Document & Content Management Monitoring & Reporting:** Establishes regular performance monitoring and issue tracking processes, supported by automated dashboards and real-time alerts to identify bottlenecks, underperformance, and governance gaps.
- **Document & Content Management SLAs:** Formalizes service expectations between the Entity and its tool vendor, including uptime, support response times, and system performance metrics with escalation paths and compliance thresholds clearly defined.
- **Document & Content Management Audit:** Ensures the Entity is prepared to respond to internal and external audits by maintaining a consistent set of governance artifacts.
- **QDTI:** Evaluating the Entity's adherence to the National Document and Content Management Standards.

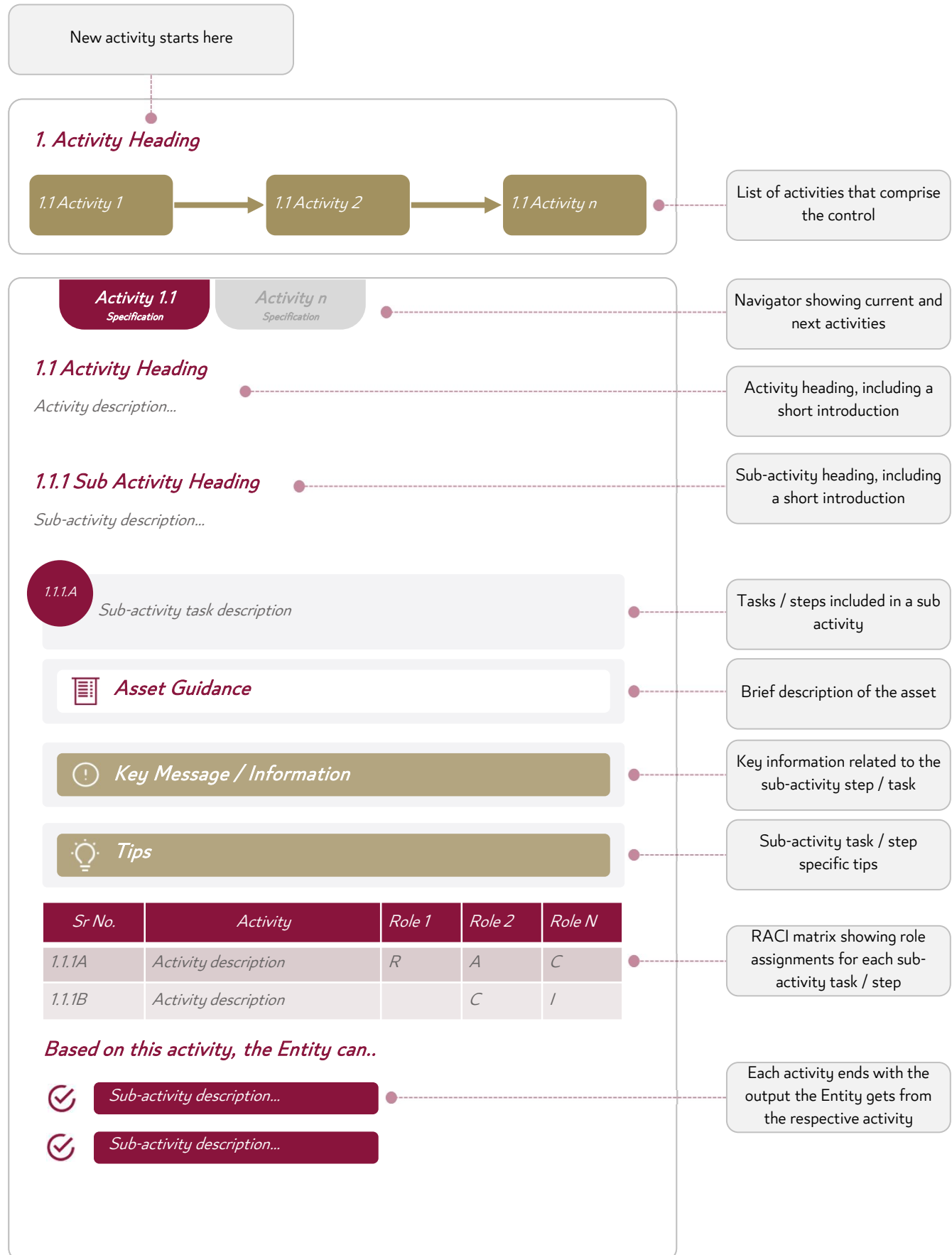
1.2 Target Audience

This handbook is intended for the Data Management and Security Director and Data Management and Governance Section Head. It is also suitable for metadata specialists, the IT Team, and department-level data stewards responsible for managing unstructured content. The handbook serves as a practical resource to guide the development and implementation of the Entity's document and content management program, forming a structured foundation for effective lifecycle governance and compliance.

1.3 Abbreviations and Glossary

Abbreviation/Term	Definition / Long Name
BC/DR	Business Continuity and Disaster Recovery — A set of processes to ensure continuity of operations and data protection in the event of disruptions.
BPMN	Business Process Model and Notation
Content Owner	The individual or role responsible for the accuracy, completeness, and classification of a document.
DCM	Document & Content Management
Differential Backup	A backup method that captures all changes made since the last full backup.
DMS	Document Management System — A platform used to store, organize, manage, and retrieve documents and unstructured content.
Disposal Approval Log	A register that records decisions and approvals for content that has reached end-of-life and is ready for removal.
Incremental Backup	A backup method that captures only the data changed since the last backup (full or incremental).
Information Architecture	The structural design for organizing, classifying, and navigating content within the document and content management tool.
KPI	Key Performance Indicator — A measurable value used to track performance of document and content governance activities.
Metadata	Descriptive and structural information about a document, such as Title, Owner, Sensitivity, Retention Period, etc.
QDKC	Qatar Data Knowledge Case
Retention Period	The length of time a document must be kept before it is eligible for disposal or archival.
RPO	Recovery Point Objective — The maximum tolerable period in which data might be lost due to an incident.
ROT	Redundant, Obsolete, or Trivial content — Documents or files that no longer serve business or compliance needs.
RTO	Recovery Time Objective — The maximum acceptable length of time to restore service after a disruption.
SLA	Service-Level Agreement — A formal commitment between the Entity and the tool vendor, defining expected service performance.
Version Control	A DCM Tool feature that tracks changes to documents, maintains history, and enables rollback to previous versions.
WCMS	Web Content Management System — A system used to create, manage, and publish digital content on web portals.
Workflow Prioritization	The process of identifying high-impact document-related workflows for automation or governance integration.
Document Prioritization	The activity of identifying and ranking the most important documents for structured governance.

1.4 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"

1.5 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 within 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.
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.
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.
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.

Stakeholder	Role Description
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.

1.6 Key Success Factors

Policy Alignment and Governance Commitment: Ensure that all document and content management practices are guided by a formal, approved policy aligned with Qatar's National Data Standards. Strong governance backing provides direction, accountability, and consistency across the Entity.

Clear Ownership and Role Definition: Assign well-defined roles for content ownership, metadata management, retention oversight, and system administration. Clear accountability ensures that responsibilities are distributed and that no content or process is left unmanaged.

System Integration and Tool Readiness: Implement a document and content management tool with robust capabilities for versioning, access control, metadata tagging, and workflow automation. System readiness is essential for enforcing governance in real time and at scale.

Structured Planning and Phased Execution: Use maturity assessments and phased roadmaps to prioritize and sequence improvements. This allows the Entity to manage complexity, allocate resources efficiently, and build momentum over time.

Retention and Lifecycle Control: Embed retention rules and disposal mechanisms into daily operations. Managing content from creation through archival or deletion reduces risk, clutter, and legal exposure.

Performance Monitoring and Audit Readiness: Define KPIs, monitor system usage, and establish service-level agreements (SLAs). Being audit-ready and performance-aware ensures continuous improvement and operational transparency.

User Adoption and Change Management: Provide clear guidance, user training, and communication around new processes and tools. Adoption is critical — even the best-designed systems fail without engaged users and steady reinforcement.

The following chapters will provide detailed guidance in each of these areas, offering actionable steps to establish robust document and content management practices and drive operational efficiency within the Entity.

1.7 Compliance with National Data Standards

National Data Standards		QDKC
Control	Specification	Activity
DCM.1.1 Document & Content Management Policy	DCM.1.1.1 Document & Content Management Policy Creation F	2.1 Document & Content Management Policy Creation
	DCM.1.1.2 Document & Content Management Policy Publication F	2.2 Document & Content Management Policy Publication
DCM.1.2 Document & Content Management Planning	DCM.1.2.1 Document & Content Management Plan F	3.1 Document & Content Management Plan
DCM.2.1 Document & Content Management Assessment & Design	DCM.2.1.1 Inventory Assessment A	4.1 Inventory Assessment
	DCM.2.1.2 Document Prioritization A	4.2 Document Prioritization
	DCM.2.1.3 Workflow Prioritization A	4.3 Workflow Prioritization
	DCM.2.1.4 Information Architecture A	4.4 Information Architecture
DCM.2.2 Document & Content Management Implementation	DCM.2.2.1 Document & Content Management Tool Implementation A	5.1 Document & Content Management Tool Implementation
	DCM.2.2.2 Document & Content Management Tool Implementation VA	
	DCM.2.2.3 Records & Content Capture A	5.2 Records & Content Capture
	DCM.2.2.4 Versioning & Control A	5.3 Versioning & Control
	DCM.2.2.5 Versioning & Control VA	
	DCM.2.2.6 Backup & Recovery A	5.4 Backup & Recovery
	DCM.2.2.7 Backup & Recovery VA	

Legend: Capability Level



Foundational



Advanced



Very Advanced

National Data Standards		QDKC
Control	Specification	Activity
DCM.2.2 Document & Content Management Implementation	DCM.2.2.8 Retention & Disposal A	5.5 Retention & Disposal
	DCM.2.2.9 Document & Content Metadata A	5.6 Document & Content Metadata
	DCM.2.2.10 Content Publishing & Delivery A	5.7 Content Publishing & Delivery
DCM.3.1 Document & Content Management Performance Management	DCM.3.1.1 Document & Content Management KPIs A	6.1 Document & Content Management KPIs
	DCM.3.1.2 Document & Content Management KPIs VA	
	DCM.3.1.3 Document & Content Management Monitoring & Reporting A	6.2 Document & Content Management Monitoring & Reporting
	DCM.3.1.4 Document & Content Management Monitoring & Reporting VA	
	DCM.3.1.5 Document & Content Management SLAs A	6.3 Document & Content Management SLAs
	DCM.3.1.6 Document & Content Management SLAs VA	
	DCM.3.1.7 Document & Content Management Audit A	6.4 Document & Content Management Audit

Legend: Capability Level



Foundational

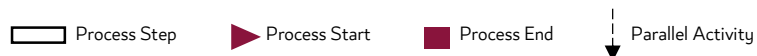
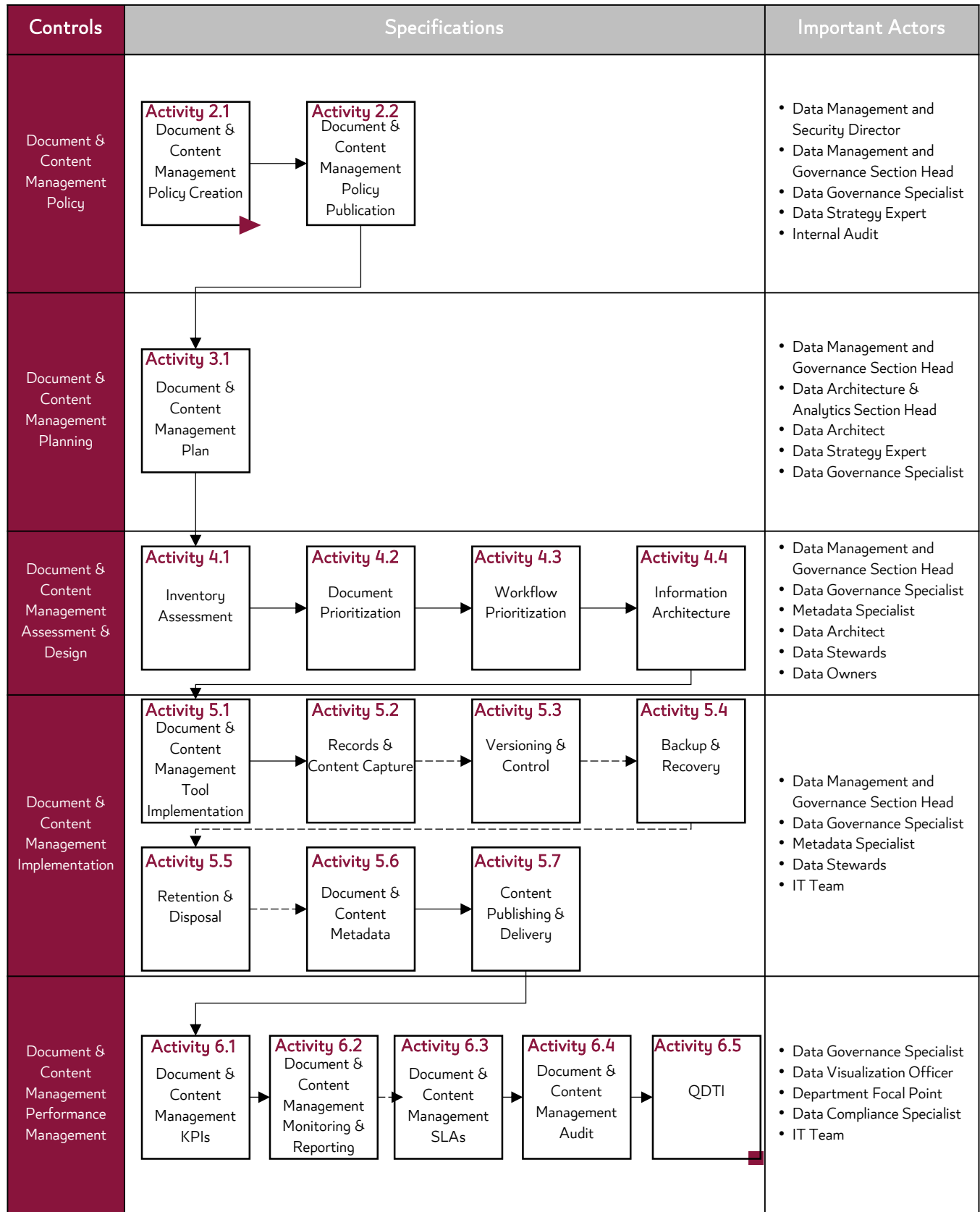


Advanced



Very Advanced

1.8 Domain Level Process Map



2. Document & Content Management Policy



2. Document and Content Management Policy

What is a Document & Content Management Policy and why does the Entity need it?

A Document & Content Management Policy is a set of formal, executive-level statements that govern the standardized and secure handling of documents and content across their full lifecycle—from creation and storage to access, versioning, retention, and archival. This policy ensures that content is managed consistently and in alignment with the Entity's broader data governance framework and the National Data Management Policy and Standards.

The policy defines clear responsibilities, security measures, and operational standards for how documents and content are handled, shared, and protected. It supports compliance with regulatory requirements, promotes operational efficiency, and reduces risks related to information loss, unauthorized access, or inconsistent retention practices.

A well-structured policy enables the Entity to manage diverse types of documents and digital content effectively, supporting collaboration, ensuring traceability, and maintaining data integrity. It also reinforces the importance of metadata, automation, and digital tools in optimizing content discoverability, reusability, and lifecycle governance.

To remain effective, the Document & Content Management Policy must be periodically reviewed, updated, and socialized. Continuous engagement with stakeholders and alignment with national and industry standards ensures the policy reflects evolving content governance needs.

The remaining sections of this chapter will detail the activities of the below process that will guide the Entity on executing the Document & Content Management Policy:



Guiding Principles for Document & Content Management Policy

1. **Appoint a Single Owner:** Designate a single owner for data policies to ensure accountability and clear leadership in data governance.
2. **Maintain a Data Policy Repository:** Publish and maintain a centralized repository of data policies that is easily accessible to all employees, promoting transparency and awareness.
3. **Annual Review and Updates:** Review data policies at least annually to ensure they remain valid and relevant, using disciplined version control to track changes and updates.
4. **Stakeholder Engagement:** Involve key stakeholders from different departments in the policy development and review process to ensure diverse perspectives and needs are considered.
5. **Training and Awareness:** Implement regular training sessions to educate employees about data policies and their importance, fostering a culture of data quality.
6. **Compliance and Standards:** Ensure that data policies align with relevant regulatory requirements and industry standards, facilitating compliance and risk management.

2.1 Document & Content Management Policy Creation

The Entity should establish a Document & Content Management Policy to ensure the secure, standardized handling and management of documents and content throughout their lifecycle.

Process - Document & Content Management Policy Creation

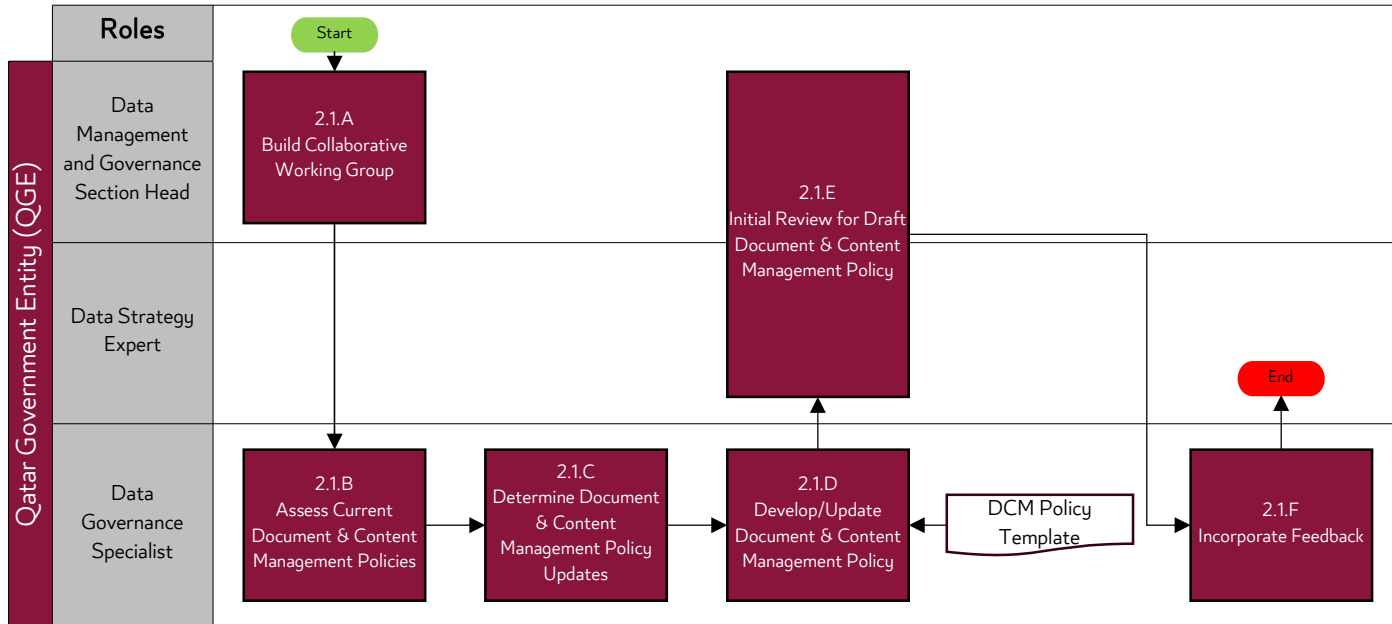


Figure 1: Document & Content Management Policy Creation Process Map

Legend: ■ Process Step ◆ Decision ● Process Start ● Process End □ Document ■ Off-Page Reference

2.1.A

Build Collaborative Working Group: To ensure the policy reflects operational realities, governance needs, and is not developed in isolation, the Entity must establish a collaborative working group of internal stakeholders and subject matter experts. This working group supports policy drafting by providing feedback, identifying operational considerations, and aligning the policy with Entity-specific contexts.

- i. **Establish the Collaborative Working Group:** Form a core team responsible for developing and reviewing the policy.
 - a. Led by the Data Governance Specialist, with oversight from the Data Management & Governance Section Head.
 - b. Include members from Data Governance, Metadata, Strategy, IT, compliance, and stewardship roles.
- ii. **Define Scope and Responsibilities of the Working Group:** Ensure the group's role is clear and time-bound.
 - a. Review proposed policy topics and structure.
 - b. Provide inputs during each phase of policy drafting and review.
 - c. Participate in validation and ensure alignment with Entity needs.
- iii. **Schedule Working Sessions:** Create a structured timeline for engagement.
 - a. Schedule policy drafting workshops and checkpoint reviews.
 - b. Ensure participation is documented and inputs are logged.

2.1.B

Assess Current Document & Content Management Policies: Before developing or updating the Document & Content Management Policy, the Entity must assess its current state. This includes reviewing any existing policies to identify gaps, overlaps, and misalignment with the Entity's data strategy, operational practices, and the National Data Standards. This assessment forms the foundation for effective and relevant policy development.

- i. **Conduct a Structured Policy Review:** Identify and evaluate any existing policies related to Document & Content Management.
 - a. If exists, review current documentation for:
 - Document & Content Management policy overview, purpose, scope, objectives, applicability, validity, policy statements, roles and responsibilities
 - Supporting Document & Content Management standards or procedures that may inform or support future policy development
 - b. Assess whether the policy content is outdated, incomplete, duplicated, or missing.
- ii. **Evaluate Alignment with Strategic and National Requirements:** Assess how well the current policy (if exists) supports key governance needs. Review for:
 - **Relevance to Strategic Objectives:** Does the policy align with the Entity's data strategy?
 - **Compliance with National Standards:** Does it reflect alignment with the current National Data Policy and National Data Standards?
 - **Clarity and Accessibility:** Is the policy easy to read, use, and apply?
- iii. **Document Findings and Key Gaps:** Summarize the outcomes of the assessment in preparation for step 2.1.C.
 - a. List key areas where new or updated policy content is needed.
 - b. Identify risks or inconsistencies that should be addressed (e.g., lack of version control, no update schedule).
 - c. Share findings with the collaborative working group for validation.



Key Message / Information

Building a working group ensures the policy is not developed in isolation but reflects the real governance needs of the Entity.

2.1.C
(1/2)

Determine Document & Content Management Policy Updates: Based on the findings from the policy assessment and input from the working group, the Entity must outline the specific updates or new content areas required in the Document & Content Management Policy. This step ensures that policy development is focused, complete, and responsive to both internal and national governance requirements.

2.1.C
Cont.
(2/2)

- i. **Define the Scope of Policy Creation/Update:** Translate assessment findings into a structured update plan.
 - a. Identify sections of the policy that need to be:
 - Created from scratch
 - Updated for alignment with strategy or standards
 - Removed due to redundancy or irrelevance
 - b. Determine whether the update (if any) qualifies as a major revision (e.g., structural change, expanded scope) or minor revision (e.g., wording adjustments).
- ii. **Prioritize Content Areas for Inclusion:** Ensure the policy covers all required Document & Content Management topics.
 - a. Reference Document & Content Management domain within the National Data Policy and National Data Standards to prioritize content including but not limited to:
 - Document lifecycle management
 - Security measures
 - Document and content management tool selection
 - Training and awareness
 - b. Map these areas against identified gaps and stakeholder feedback.
- iii. **Create a Policy Update Action Plan:** Develop a high-level roadmap for the policy drafting process.
 - a. Outline key tasks, responsible roles, and delivery timelines.
 - b. Align this plan with the collaborative working group's availability and input schedule.
 - c. Use the action plan to guide coordination with stakeholders and support tracking of progress throughout the development cycle.

2.1.D
(1/2)

Develop/Update Document & Content Management Policy: Using the agreed-upon creation/update scope and structure, the Entity must develop or revise the Document & Content Management Policy to ensure the secure, standardized handling and management of documents and content. The policy must be clear, actionable, aligned with strategic objectives, and compliant with the national data standards.

- i. **Draft Policy Content Using Approved Structure:** The Data Governance Specialist leads the drafting exercise using the standard Document & Content Management policy template.
 - a. Use the Document & Content Management Policy Template to structure the document.
 - b. The policy should include, at a minimum:
 - Overview, purpose, scope, and objectives
 - Policy applicability, validity, and review process
 - Guidelines aligned with the National Data Management Policy and Standards
 - Detailed policy statements covering:
 - Retention, archival, and disposal of documents
 - Security measures for each type of document
 - Document and content management tool features

- Training and awareness

- Roles and responsibilities
- References

Asset Guidance

The **Document and Content Management Policy Template** is a sample table of contents the Entity can refer to when drafting its policy. It includes the topics required by the standards, as well as additional recommended topics to consider. It also gives a sample of policy statements for one topic from the table of content to help entities draft the policy document.

Illustrative

Table of Contents		2 Document and Content Management Policies
1	Introduction.....#	2.1 Document Retention
1.1	Overview.....#	1. Each document or content item shall be assigned a predefined retention period based on its classification, regulatory requirement, and operational value. Retention periods must be documented and enforced across all systems.
1.2	Purpose.....#	2. Retention schedules shall be reviewed and approved by the Data Governance Lead and Legal Team to ensure alignment with national regulations and organizational policies. Changes to retention schedules must be tracked and version controlled.
1.3	Scope & Applicability.....#	3. No document shall be retained beyond its approved retention period unless legally required or approved by the Document Owner. All expired documents must be flagged for review and scheduled for disposal in accordance with defined disposal protocols.
1.4	Objectives.....#	4. Records designated for permanent or long-term retention must be archived in secured and accessible repositories, with metadata clearly indicating archival status and justification.
2	Document and Content Management Policies.....#	5. All document retention and disposal actions shall be logged, including timestamps, document IDs, user IDs, and reasons for disposal or extended retention, ensuring auditability and accountability.
2.1	Document Retention.....#	6. Documents required for legal, regulatory, or audit purposes must be protected from modification or deletion until their retention obligations are fulfilled. Legal hold procedures must be in place to override standard retention in such cases.
2.2	Document Archival.....#	*** (Sample policy statements for a topic) ***
2.3	Document Disposal.....#	
2.4	Security Measures.....#	
2.5	Document and Content Management Tool Features.....#	
2.6	Training and Awareness.....#	
3	Periodic Policy Review and Updates.....#	
3.1	Revision Frequency.....#	
3.2	Revisions.....#	
3.3	Archival Procedure.....#	
4	Roles within the Scope of this Policy.....#	
5	Related Legislation, References, and Documents.....#	
6	Document Control.....#	

ii. **Apply Clear and Actionable Language:** Ensure the policy is practical, enforceable, and accessible to all stakeholders.

- Use direct, concise language tailored to the Entity's context.
- Ensure each policy statement is tied to a strategic or operational outcome.
- Emphasize responsibilities, process expectations, and compliance triggers.

iii. **Prepare the Draft for Preliminary Review:** Finalize the draft as a working version for internal feedback.

- Share with the collaborative working group.
- Confirm the draft addresses all previously identified policy gaps.
- Prepare a feedback summary log for tracking suggestions in the next step.



Key Message / Information

Draft the policy using clear and concise language that reflects the Entity's specific needs while accommodating diverse operational scenarios. Each policy statement should be directly tied to broader business objectives, demonstrating how it supports strategic goals and organizational priorities. Emphasize actionable and enforceable language to enable consistent implementation and ensure compliance.

2.1.E
(1/2)

Initial Review for Draft Document & Content Management Policy: Once the policy draft is complete, the Entity must conduct an internal review to validate alignment with the National Data Standards, legal and regulatory obligations, and strategic objectives. This review ensures the policy is robust, compliant, and ready for broader publication steps.

- i. **Conduct Governance and Strategy Review:** The draft is reviewed by key stakeholders for policy integrity and relevance.
 - a. The Data Management & Governance Section Head and Data Strategy Expert assess the draft for:
 - Strategic alignment with the Entity's data governance objectives
 - Compliance with National Data Policy and Standards
 - Consistency with related internal policies (e.g., data privacy, quality)
 - b. Confirm the policy structure follows the approved template and includes all required content areas.
- ii. **Validate Legal, Regulatory, and Operational Compliance:** Ensure the policy supports risk management and audit readiness.
 - a. Identify any areas requiring clarification or legal alignment.
 - b. Ensure the policy does not conflict with regulatory or operational obligations.
 - c. Highlight areas where governance enforcement or change management will be required.
- iii. **Capture and Document Feedback:** Record feedback from reviewers in a structured format to inform final refinements.
 - a. Document all comments and suggestions in a feedback log.
 - b. Prioritize revisions based on severity (e.g., compliance issues vs. language improvement).
 - c. Share the feedback log with the Data Governance Specialist for implementation in 2.1.F.



Key Message / Information

This review phase ensures the draft policy is credible, compliant, and strategically sound—before formalization or publication.

2.1.F
(1/2)

Incorporate Feedback: Following the internal review, the Entity must revise the draft Document & Content Management Policy to reflect feedback received from governance, strategy, legal, and operational stakeholders. This step ensures the final version is complete, accurate, and ready for formal approval and publication.

- i. **Review and Prioritize Feedback Log:** Work through the feedback log collected in 2.1.E in a structured and transparent way.
 - a. Categorize feedback by type (e.g., compliance, structure, clarity, alignment).
 - b. Prioritize revisions based on criticality, starting with compliance and strategy gaps.
 - c. Flag any unresolved or disputed comments for follow-up discussion with the Data Management & Governance Section Head.

2.1.F
Cont.
(2/2)

- ii. **Apply Revisions to the Draft Policy:** Update the policy draft to reflect accepted changes.
 - a. Revise content in the official policy document, maintaining formatting consistency.
 - b. Track major changes using version control or change highlights.
 - c. Ensure all policy components (e.g., roles, responsibilities, review cycle) are fully addressed.
- iii. **Finalize the Policy Document for Approval:** Prepare the updated policy for formal submission.
 - a. Confirm that all feedback has been addressed or closed.
 - b. Update metadata such as version number, revision date, and approval status.
 - c. Share the final version with the Data Management & Governance Section Head for submission into the Entity's governance approval workflow.

RACI Matrix - Document & Content Management Policy Creation

Indicative

Sr No.	Activity	Data Management & Security Director	Data Management and Governance Section Head	Data Governance Specialist	Collaborative Working Group	Data Strategy Expert	Legal Team
2.1.A	Build Collaborative Working Group	A	R	C	I	I	
2.1.B	Assess Current Document & Content Management Policies		A	R	C	C	
2.1.C	Determine Document & Content Management Policy Updates		A	R	C	C	
2.1.D	Develop/Update Document & Content Management Policy		A	R	C	C	C
2.1.E	Initial Review for Draft Document & Content Management Policy	A	R	I	C	R	C
2.1.F	Incorporate Feedback		A	R	C		

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

Based on this Activity, the Entity can



Build Collaborative Working Group of SMEs



Draft Document & Content Management Policy

2.2 Document & Content Management Policy Publication

This activity will guide the Entity on the steps to publish its data policies.

Process – Document & Content Management Policy Publication

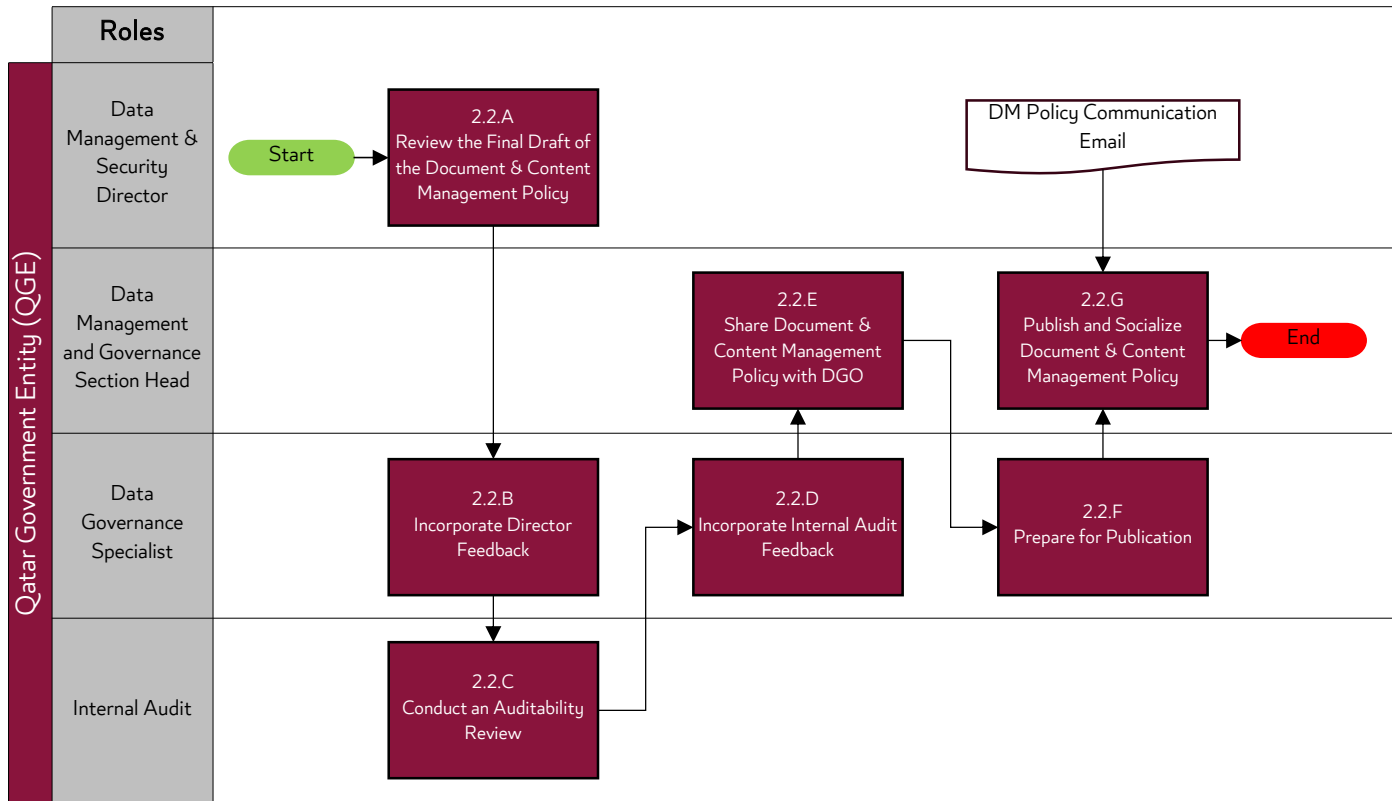


Figure 2: Document & Content Management Policy Publication Process Map

Legend: ■ Process Step ◆ Decision ● Process Start ● Process End □ Document ■ Off-Page Reference

2.2.A (1/2)

Review the Final Draft of the Document & Content Management Policy: Before proceeding to formal approval and publication, the Entity must conduct a final review of the completed Document & Content Management Policy. This step ensures that the policy aligns with the Entity's data management strategy, governance principles, and business objectives, and that any remaining gaps are identified and addressed.

- i. **Confirm Strategic and Operational Alignment:** The Data Management & Security Director reviews the final draft to ensure policy alignment with enterprise priorities. Assess whether the policy:
 - Reflects the Entity's data governance framework and strategic direction
 - Supports operational effectiveness and clear role accountability
 - Aligns with internal governance principles (e.g., privacy, quality, integration)
- ii. **Identify Gaps, Misalignments, or Ambiguities:** Ensure the policy content is comprehensive and implementation-ready.
 - a. Flag missing elements, conflicting statements, or unclear policy language.
 - b. Identify any inconsistencies with related documents.
 - c. Provide written feedback on areas requiring revision or clarification.

2.2.A
Cont.
(2/2)

- iii. **Document Review Outcome and Next Steps:** Ensure feedback is structured and ready for incorporation in the next phase.
- a. Share feedback with the Data Governance Specialist in a structured format.
 - b. Record major comments for traceability (e.g., in a review tracker or comment log).
 - c. Confirm that feedback will be addressed in 2.2.B before publication proceeds.

**Key Message / Information**

This review step ensures the policy is accurate, aligned, and strategically sound before it enters the final approval and publication process.

2.2.B

Incorporate Director Feedback: Following the strategic review by the Data Management & Security Director, the Data Governance Specialist must revise the draft policy to reflect the provided feedback. This step ensures the policy addresses all strategic and governance-related concerns before moving into auditability review.

- i. **Review and Categorize Feedback:** Organize the feedback received from the director review for systematic implementation.
- Categorize comments (e.g., structural, content, compliance-related)
 - Prioritize critical feedback, especially those that impact alignment with strategic direction or compliance.
 - Clarify ambiguous feedback, if needed, through direct engagement with the reviewer.
- ii. **Apply Revisions to the Policy Draft:** Update the policy content to incorporate accepted feedback.
- a. Edit the draft to address feedback while preserving clarity and consistency.
 - b. Ensure changes strengthen strategic alignment, enforceability, and policy coherence.
 - c. Update document versioning and maintain a changelog of revisions made.
- iii. **Prepare the Policy for Auditability Review:** Ready the revised document for submission into the internal review and audit process.
- a. Confirm that all priority feedback has been addressed and documented.
 - b. Finalize the revised version for handover to the next stage.
 - c. Maintain a summary of revisions to support auditability and approval traceability.

2.2.C

Conduct an Auditability Review: Before final approval, the Entity must ensure the policy meets audit readiness criteria. This includes confirming that the policy is version-controlled, aligned with internal regulatory and operational standards and procedures, and compliant with documentation standards required for future audits and inspections. Feedback is gathered to address gaps in accountability, compliance, or performance tracking, if necessary.

2.2.D

Incorporate Internal Audit Feedback: Integrate feedback and recommendations from the internal audit review to address any remaining compliance, accountability, or documentation gaps. This step ensures the policy meets all auditability requirements and is fully prepared for final approval and formal publication.

2.2.E

Share Document & Content Management Policy with DGO: The Entity must submit the finalized draft of the Document & Content Management Policy to the DGO for formal review and feedback. This step ensures the policy aligns with national governance frameworks, regulatory expectations, and recognized data management best practices.

- i. **Submit the Finalized Policy to the DGO:** The policy is formally submitted through the appropriate channel for DGO review.
 - a. Send the finalized draft via the designated email or submission platform (as required at the respective point in time).
 - b. Confirm version number, submission date, and the responsible point of contact.
- ii. **Provide Supporting Context and Summary:** The submission must include a brief explanation to facilitate DGO review.
 - a. Summarize the policy scope, purpose, and any recent updates.
 - b. Highlight key areas where the policy aligns with national standards or fills previously identified governance gaps.
- iii. **Track the Submission and Prepare for Follow-Up:** Maintain traceability and readiness to act on feedback.
 - a. Log the submission in the Entity's governance repository or tracking system.
 - b. Note expected response timelines and plan for feedback incorporation in Step 2.2.F.



Key Message / Information

Engaging the DGO in the policy review process reinforces national alignment and promotes consistency across government-wide document and content management initiatives.

2.2.F
(1/2)

Prepare for Publication: Once all feedback has been incorporated, the Entity must finalize the policy for formal publication. This step ensures the document is properly versioned, archived, and ready to be communicated and distributed across the organization.

- i. **Finalize Policy Content and Format:** Ensure the policy is complete and ready for publishing.
 - a. Confirm all internal and DGO feedback has been fully addressed.
 - b. Apply final formatting, ensure clarity and consistency, and validate that the structure follows the approved policy template.
 - c. Update metadata fields including version number, status, effective date, and next review cycle.

2.2.F
Cont.
(2/2)

- ii. **Archive and Register the Final Version:** Secure the policy in Entity records and ensure traceability.
 - a. Save the finalized document in the Entity's governance repository or policy management system.
 - b. Maintain version history and a changelog, including approval and feedback documentation.
 - c. Confirm access permissions are in place ahead of publication and communication.
- iii. **Notify Stakeholders of Upcoming Publication:** Alert relevant teams that the policy is finalized and will be published in 2.2.G.
 - a. Share a summary message with data owners, stewards, and governance leads.
 - b. Prepare communication materials (e.g., email, announcement note) for rollout.

**Key Message / Information**

Preparing the policy for publication ensures it is complete, traceable, and properly maintained, enabling a smooth transition to Entity-wide communication and adoption.

2.2.G
(1/2)

Publish and Socialize the Document & Content Management Policy: Once finalized, the Entity must publish the policy in an accessible location and actively communicate its purpose, scope, and expectations to relevant stakeholders. This step ensures the policy is not only available, but also understood, adopted, and applied consistently across the organization.

- i. **Publish the Policy in the Official Repository:** Ensure centralized access and version control.
 - a. Upload the final policy to the Entity's internal policy repository or governance portal.
 - b. Tag the document with metadata such as owner, version, status, effective date, and next review date.
 - c. Confirm appropriate access permissions are configured.
- ii. **Communicate Policy Availability and Key Messages:** Promote awareness and usage of the policy across roles and departments.
 - a. Use the Policy Communication Email Template to inform staff of the policy release.
 - b. Include the policy's purpose, scope, and summary of key expectations.
 - c. Tailor communications by role if necessary (e.g., Stewards, Data Owners, IT, Legal).
- iii. **Reinforce Policy Adoption Through Awareness Channels:** Ensure the policy is understood and referenced in practice.
 - a. Present the policy in onboarding, training sessions, or governance briefings.
 - b. Link the policy in supporting materials such as guidelines, templates, or dashboards.
 - c. Gather informal feedback or usage indicators to monitor engagement.

 Asset Guidance

The **Data Management Policy Communication Email Template** is a sample announcement email the Entity can use to notify staff about the publication of the policy and provide key information.

Illustrative

Subject: [IMPORTANT] New [Domain Name] Policy Published – Please Review

Dear [Recipient Name/Team],

We are pleased to announce the publication of the new [Domain Name] Policy, which is now in effect as of [Date]. This policy is designed to [briefly explain the purpose, e.g., "ensure the effective management of metadata and data catalog operations across the entity"] and aligns with the National Data Standards.

What is the Policy About?

The [Domain Name] Policy governs the management, oversight, and compliance of [specific domain] activities across the entity. It outlines critical guidelines and procedures, including:

- [Key Point 1, e.g., "Data Management and Organizational Structure"]
- [Key Point 2, e.g., "Version control and security measures"]
- [Key Point 3, e.g., "Metadata quality and governance"]

This policy has been developed in collaboration with the Data Committee and relevant stakeholders, ensuring compliance with the national data management standards.

How Does This Affect You?

- **Action Required:** Please review the policy and ensure that your team is aligned with its requirements. The policy affects [mention departments or roles impacted, e.g., "all data stewards, IT staff, and department heads"]. Compliance with this policy is essential to ensure adherence to the National Data Management Standards, which are critical to the entity's data governance and operational success.
- **Changes to Processes:** [If applicable, briefly describe any changes to current workflows or responsibilities as outlined by the policy.]

Where Can You Access the Policy?

The policy is available on our internal [intranet/portal] and can be accessed through the following link:
[Link to Policy Document]

Next Steps

- **Review Deadline:** Please ensure that you and your team have reviewed the policy by [Date].
- **Training/Workshops:** [If applicable] We will be hosting a [training/workshop] on [Date] to assist teams in understanding and applying the new policy.
- **Ongoing Support:** For questions, feedback, or support, please contact [Support Contact] at [email/phone number].

Thank you for your attention to this important matter and for your cooperation in ensuring compliance with the new policy. Together, we can maintain a strong framework for [mention domain, e.g., "data catalog and metadata management"] across the entity.

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



Key Message / Information

Publishing the policy is not the end of the process. It must be socialized effectively so that stakeholders understand how it applies to their roles and responsibilities.

Process Risks: Develop and Publish Document & Content Management Policy

Risk	Severity	Mitigation
1. Lack of engagement from business SMEs due to other demanding responsibilities.	High	Data Management and Governance Section Head to secure management commitment for the key SMEs required to develop the Document & Content Management policy.
2. No standardized or existing process to publish the policy.	Medium	Data Management and Governance Section Head to coordinate with the compliance office to establish a centralized process and repository for the publication and maintenance of the Document & Content Management Policy.

RACI Matrix - Document & Content Management Policy Publication

Indicative

Sr No.	Activity	DGO	Data Management & Security Director	Data Management and Governance Section Head	Data Governance Specialist	Data Strategy Expert	Internal Audit
2.2.A	Review the Final Draft of the Document & Content Management Policy		A/R	C			
2.2.B	Incorporate Director Feedback		C	A	R		
2.2.C	Conduct an Auditability Review			I	I		A/R
2.2.D	Incorporate Internal Audit Feedback			A	R	C	
2.2.E	Share Document & Content Management Policy with DGO	I	A	R			
2.2.F	Prepare for Publication			A	R	C	
2.2.G	Publish and Socialize Document & Content Management Policy		A	R		C	

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

Based on this Activity, the Entity can



Publish Document & Content Management Policy

3. Document & Content Management Planning



3. Document & Content Management Planning

What is Document & Content Management Planning and why does the Entity need it?

Document & Content Management Planning is a foundational activity that enables the Entity to operationalize its governance strategy for unstructured content through a structured, phased, and maturity-aligned approach. It combines a baseline maturity assessment with practical planning and roadmap development to ensure that content management efforts are actionable, prioritized, and aligned with national standards and internal operational realities.

This activity is essential because effective document governance requires more than just system implementation — it demands a clear understanding of the current state, identification of high-value content and workflows, and the ability to sequence improvements across people, process, and technology in a sustainable manner. The planning process includes two key components:

- **Maturity Assessment:** Evaluates the Entity's current capabilities across document and content management using the data maturity model.
- **Plan and Roadmap:** Translates insights from the above into a detailed roadmap of initiatives, key activities, responsibilities, risks, dependencies, timelines and milestones

Together, these activities ensure that the Entity's approach to document and content governance is not only policy-driven and standards-aligned but also grounded in operational needs. It provides a clear path to strengthening compliance, improving user experience, reducing unmanaged content, and enabling successful platform adoption.

The remaining sections of this chapter will detail the activities of the below process that will guide the Entity on executing the Document & Content Management Planning:

3.1 Document & Content Management Plan

Guiding Principles for Document & Content Management Planning

1. **Align with the Data Strategy:** Ensure that the plan supports the Entity's data strategy and broader digital transformation objectives, with a focus on enabling secure, standardized document and content handling.
2. **Define Clear Ownership:** Establish clear roles and responsibilities for document and content lifecycle management, assigning accountability for compliance, quality, and operational performance.
3. **Integrate Risk and Interdependency Management:** Proactively identify technical, operational, or compliance risks and interdependencies with other digital systems to minimize disruption and align priorities.
4. **Ensure Cost and Timeline Realism:** Align project timelines and resource needs with the Entity's capacity and budget while ensuring milestones are realistic and implementation is achievable across departments.

3.1 Document and Content Management Plan

The Document and Content Management Plan consist of the maturity assessment, as well as the actual plan and roadmap.

3.1.1 Document and Content Management Maturity Assessment

To build an effective roadmap, the Entity must first assess its current state. This activity guides the Entity in retrieving or refreshing its maturity assessment for the Document and Content Management (DCM) domain using the Data Management Current Maturity Assessment Framework and Data Management Maturity Model. The assessment identifies current strengths, gaps, and improvement priorities across governance, processes, and tools, and serves as the foundation for roadmap planning.

Process – Document and Content Management Maturity Assessment

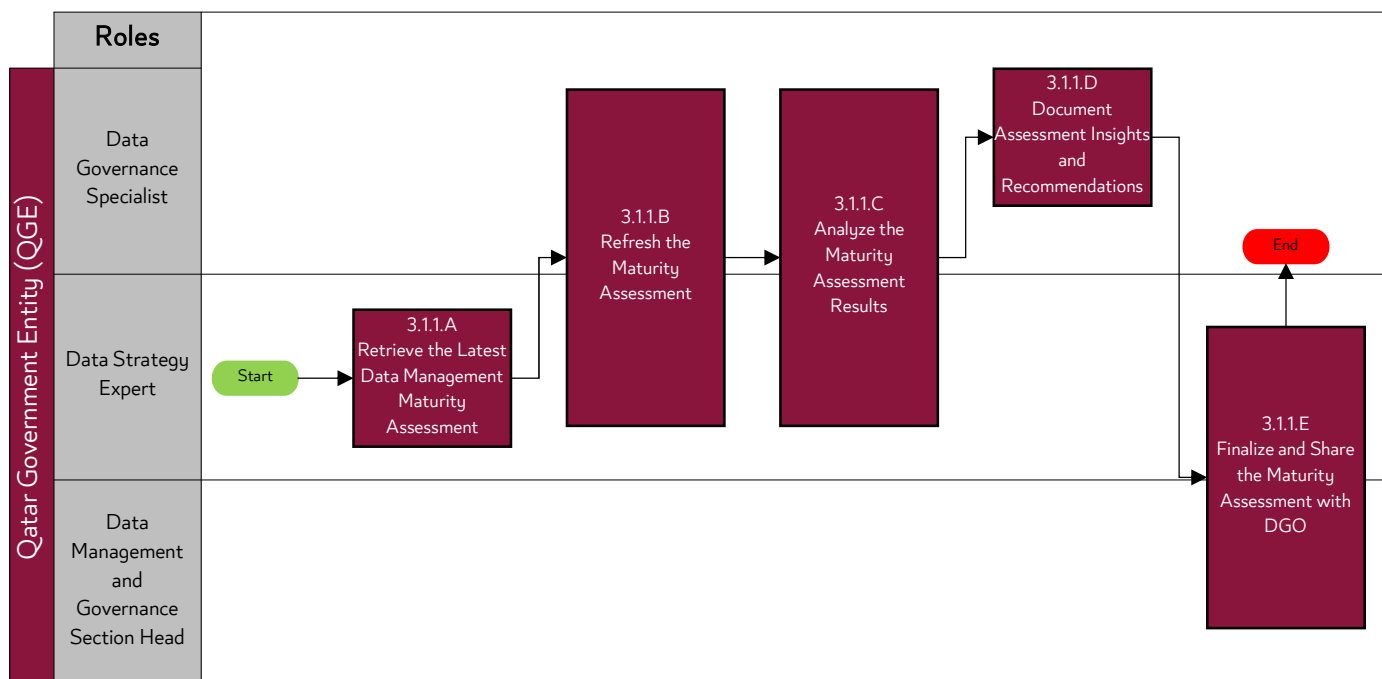


Figure 3: Document and Content Management Maturity Assessment Process Map

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

3.1.1.A (1/2)

Retrieve the Latest Document and Content Management Maturity Assessment: The Entity must retrieve its most recent maturity assessment to establish a baseline understanding of current capabilities across the DCM domain. This step is essential for determining whether an update or reassessment is required and provides the foundation for roadmap planning.

- i. **Request Existing Assessment Report:** The Data Strategy Expert locates and retrieves the latest Document and Content Management maturity assessment.
 - Engage the Data Governance Specialist to obtain the most recent maturity assessment report.
 - Confirm that the report includes maturity ratings across all DCM dimensions.
 - Validate that the report was formally conducted and documented using the approved NPC assessment framework.

3.1.1.A
Cont.
(2/2)

- ii. **Validate the Currency of the Assessment:** The Data Governance Specialist and Data Strategy Expert jointly evaluate whether the existing assessment is still valid and representative of current capabilities.
 - Confirm that the assessment was completed within the past 12 months.
 - Assess whether any significant organizational, tooling, or process changes have occurred since the report.
 - If the report is outdated or misaligned with the Entity's current state, outline that a refresh will be required.
 - Note any open or unaddressed recommendations that may still be relevant and require integration into the new roadmap.



Key Message / Information

Ensure that the maturity assessment covers both business and technical dimensions. If the assessment is fragmented or was conducted informally, treat it as insufficient and proceed to a formal refresh.

A current and validated maturity assessment is essential to building a grounded and targeted improvement roadmap. Without it, any planning activity risks being disconnected from the entity's operational reality and compliance posture.

3.1.1.B
(1/2)

Refresh the Document & Content Management Maturity Assessment (If Required): If the Entity's existing DCM maturity assessment is outdated, incomplete, or unavailable, a full reassessment must be conducted using the **Data Management Current Maturity Assessment Framework** and **Data Management Maturity Model** (referenced in Activity 2.2 within the Data Management Strategy and Governance domain guidelines). This ensures that the planning efforts in the roadmap are grounded in an accurate and current view of the Entity's document and content management capabilities.

- i. **Initiate the Refresh Process:** The Data Management and Governance Section Head triggers the reassessment and mobilizes key stakeholders.
 - Formally launch the maturity refresh process by assigning ownership to the Data Strategy Expert.
 - Confirm participation of relevant stakeholders including Data Owners, Data stewards, IT, and business users.
 - Communicate the scope and purpose of the reassessment to all contributors.
- ii. **Apply the NPC Maturity Assessment Framework:** The Entity must use the **Data Management Maturity Model** to evaluate DCM current-state capabilities.
 - Review and respond to each of the assessment dimensions (Organization, DCM Strategy, DCM Processes, Policies & Standards, etc.) using the 1–5 scale.
 - Ensure contributors refer to actual practices, tools, and governance documentation, and not perceived maturity.
 - Encourage team discussions and workshops to calibrate responses and promote honest evaluation.

3.1.1.B
Cont.
(2/2)

- iii. **Consolidate Input and Finalize Scores.** Leveraging the **Data Management Current Maturity Assessment Framework**, the Data Governance Specialist consolidates all responses, supporting evidence, and justifications.

- Validate consistency across responses and resolve conflicting input where necessary.
- Assign a final maturity level (1–5) for each dimension, including rationale.
- Prepare or update the maturity heatmap for the DCM domain, and document relevant observations.



Key Message / Information

Encourage transparency and use collaborative working sessions to resolve subjectivity and misalignment between technical and business contributors.

3.1.1.C
(1/2)

Analyze the Maturity Assessment Results: Once the DCM maturity assessment has been completed or refreshed, the Entity must analyze the results to understand current strengths, weaknesses, and capability gaps. This analysis forms the foundation for identifying high-priority improvement areas and preparing a focused roadmap.

- i. **Review Maturity Scores Across the DCM Dimensions:** The Data Governance Specialist and Data Strategy Expert jointly evaluate the final maturity scores to identify trends and performance patterns.

- Review assigned maturity levels for all DCM dimensions using the 1–5 scale.
- Identify areas of high maturity that reflect institutionalized and standardized practices.
- Identify low-performing areas (e.g., Document & Content Classification, Document Scanning, etc) that could hinder effective governance or interoperability.

- ii. **Conduct Thematic Gap Analysis:** Group maturity results into logical clusters (e.g., governance, tooling, processes) to derive broader insights.

- Categorize assessment results by functional theme:
 - Governance and ownership
 - DCM processes (technical/business)
 - Tools and features
- Identify cross-cutting gaps that appear across multiple dimensions (e.g., lack of workflow automation affecting both tool features and resources needed).
- Highlight dependencies. For example, weak role clarity (low score in “Organization”) may contribute to poor processes in place (low score in “DCM Processes”).

- iii. **Identify Quick Wins and Structural Gaps:** Segment findings based on the level of effort and impact to prioritize next steps.

3.1.1.C
Cont.
(2/2)

- **Quick wins:** improvements that can be implemented with minimal effort.
- **Structural gaps:** issues that require strategic investment or change management (e.g., tool implementation, entity-wide policy enforcement).
- Recommend areas that should be prioritized in the roadmap due to compliance implications or high strategic value (e.g., Implementing a DCM tool).



Key Message / Information

This analysis step is critical in converting maturity data into actionable insight. The quality of the roadmap depends on how well the Entity understands the underlying causes and impacts of its current maturity gaps.

3.1.1.D
(1/2)

Document Assessment Insights and Recommendations: The Entity must consolidate the results of the DCM maturity assessment into a structured executive-level slide. This summary is intended to present a high-level overview of the current maturity state, key findings, and prioritized opportunities for improvement. It will serve as a key input for roadmap planning and internal/external alignment.

i. **Populate the NPC Maturity Summary Slide:** The Data Governance Specialist prepares a summary slide (as referenced in the Data Management Current Maturity Assessment Framework in Activity 2.2 within the Data Management Strategy and Governance domain guidelines) that captures the summary maturity of the DCM domain.

a. **Maturity Score (Gauge):**

- Calculate the overall average maturity score across all DCM dimensions.
- Use the NPC's 1–5 scale and visually represent the result in the dial/gauge format.
- Select the appropriate maturity level label (Initial, Limited, Evolving, etc.).

b. **People, Process, Technology Ratings:**

- Assign indicative scores across People, Process, and Technology based on maturity dimension grouping:
 - People: e.g., Organization
 - Process: e.g., DCM Processes, Content Discovery, Document Scanning
 - Technology: e.g., DCM Tools

c. **Key Insights & Findings:**

- Summarize major pain points or maturity gaps discovered.
- Highlight inconsistencies in governance, lack of tooling, low coverage, or siloed practices.
- Use brief, high-impact bullet points appropriate for leadership-level review.

ii. **Identify Key Improvement Opportunities:** This section translates findings into action-oriented strategic recommendations.

3.1.1.D
Cont.
(2/2)

- Define the (e.g., 2-4) highest-value opportunities for improvement.
- Ensure these align with major maturity gaps (e.g., introducing stewardship, adopting a tool, formalizing change control).
- Frame opportunities in language suited for executive endorsement and roadmap alignment.

iii. **Validate with Key Stakeholders:** Before finalization, the summary slide must be reviewed by the Governance Section Head and Data Strategy Expert.

- Circulate the draft slide for review and feedback.
- Confirm that insights and opportunities are clearly and accurately captured.
- Refine language and formatting to ensure clarity, precision, and alignment with the rest of the NPC reporting pack.



Key Message / Information

Use concise, action-oriented phrasing; each bullet point should communicate a real insight or decision driver. Avoid vague recommendations and tie each suggestion to a specific weakness and pathway to resolution.

3.1.1.E

Finalize and Share the Maturity Assessment with DGO: If the DCM maturity assessment was refreshed, then the Entity must consolidate the findings and formally share the updated assessment (as part of the broader data management maturity assessment) with the DGO for alignment.

i. **Consolidate DCM Final Materials for Submission:** The Data Strategy Expert prepares the formal assessment package for DGO review.

- DCM domain level maturity scores
- DCM maturity heatmap
- DCM assessment insights and recommendations

ii. **Submit Assessment Package to the DGO:** The Data Management & Governance Section Head oversees submission and initiates engagement with the DGO.

- Send the materials to the official DGO point-of-contact through the designated submission channel.
- Request a formal review and optionally ask for advisory feedback or validation of scoring.

iii. **Incorporate DGO Feedback and Finalize Record:** Once the DGO has reviewed the submission, incorporate any clarifications or adjustments required.

- Address DGO comments or requested edits in the assessment summary slide or supporting documents.
- Finalize all materials and archive the submission internally.
- Ensure the validated version is reflected in the Entity's central data governance records.

RACI Matrix – Document & Content Management Maturity Assessment

Indicative

Sr No.	Activity	DGO	Data Management and Security Director	Data Management and Governance Section Head	Data Strategy Expert	Data Governance Specialist	Data Owner
3.1.1.A	Retrieve the Latest Data Management Maturity Assessment		A	I	R	C	I
3.1.1.B	Refresh the Maturity Assessment (If Required)		A	C	R	R	C
3.1.1.C	Analyze the Maturity Assessment Results		A	C	R	R	C
3.1.1.D	Document Assessment Insights and Recommendations		A	C	C	R	
3.1.1.E	Finalize and Share the Maturity Assessment with DGO	I/C	A	R	R	C	

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

Based on this Activity, the Entity can



Refresh the Data Management Maturity Assessment



Analyze the Maturity Assessment Results

3.1.2 Document & Content Management Plan & Roadmap

The Entity should establish a Document & Content Management Plan, that will be used and monitored to implement and activate document and content management initiatives across the Entity. The plan shall include, at a minimum:

- List of activities and milestones
- Owners and stakeholders
- Interdependencies, assumptions, and risks
- Implementation timeline and cost

Process – Document & Content Management Plan & Roadmap

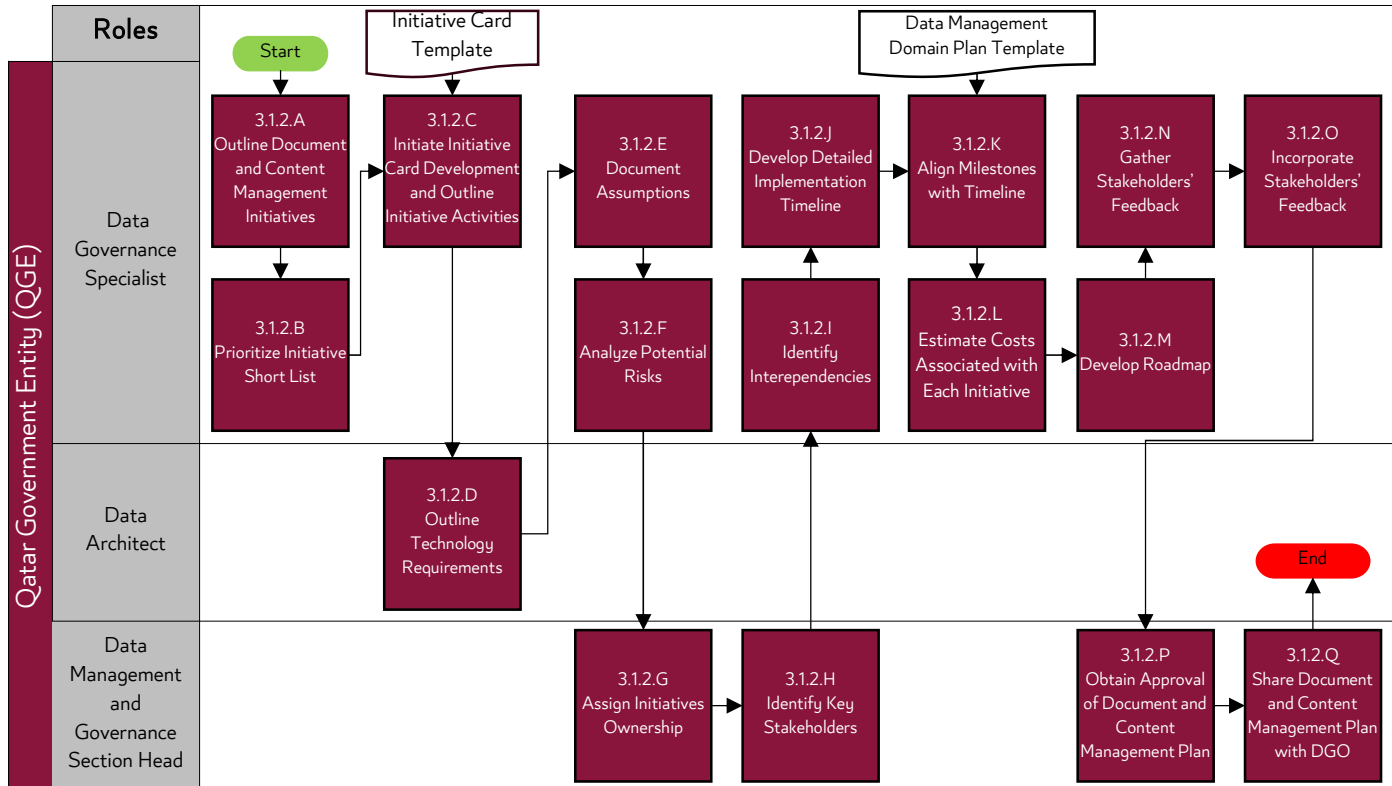


Figure 4: Document & Content Management Plan & Roadmap Process Map

Legend: ■ Process Step ◆ Decision ● Process Start ● Process End □ Document ■ Off-Page Reference

3.1.2.A Outline Document & Content Management Initiatives: Identify and document a comprehensive list of initiatives to improve the Entity's document and content management capabilities. This should include both quick wins and long-term projects. Examples include digitizing paper-based records, implementing version control, enhancing metadata tagging, migrating to a centralized DCM Tool, and developing content publication workflows. Ensure each initiative aligns with the Entity's broader data strategy and supports operational efficiency, regulatory compliance, and secure content management.

3.1.2.B Prioritize Initiative Short List: Use the long list of document and content management initiatives to develop a prioritized shortlist based on business impact, strategic alignment, and implementation feasibility. Focus on initiatives that improve document accessibility, version control, workflow automation, or content retention. Highlight quick wins—such as centralizing frequently accessed documents or implementing document tagging—that can deliver immediate value with minimal investment. Prioritization ensures that resources are allocated to high-value efforts while maintaining momentum through early successes.

3.1.2.C

Initiate Initiative Card Development and Outline Initiative Activities: Develop initiative cards for each prioritized initiative outlined in the short list, capturing essential activities and steps required to guide implementation. For each initiative, outline the key activities by breaking them down into specific steps and sub-activities that need to be completed in sequence (where applicable). Include descriptions of each step to provide clear guidance on execution, along with any necessary details on tools, techniques, or methodologies that may be required.

Asset Guidance

An **Initiative Card Template** provides a structured format to document key information related to prioritized initiatives, such as initiative overview, key activities, sponsor, owner, stakeholders, timeline, key milestones, budget, technology requirements, dependencies, assumptions, risks, and milestones. The initiative cards provide a structured overview of proposed projects, allowing stakeholders to quickly understand each initiative's purpose, expected impact, and resource requirements.

Illustrative

OVERVIEW xxx		SPONSOR xxx	STAKEHOLDERS xxx
		OWNER xxx	
KEY ACTIVITIES		TIMELINE	BUDGET (IN QAR)
Key Activity - Sub-activity X - Detailed Steps - Sub-activity Y - Detailed Steps Key Activity - Sub-activity X - Detailed Steps - Sub-activity Y - Detailed Steps		xxx	QAR xxx
		EXPECTED BENEFITS	
		• xxx	
		KEY MILESTONES	
		A. xxx B. xxx C. xxx	
		TECHNOLOGY REQUIREMENTS	
		• xxx	

OVERVIEW xxx		SPONSOR xxx	STAKEHOLDERS xxx																																																																																																									
		OWNER xxx																																																																																																										
KEY ACTIVITIES		TIMELINE																																																																																																										
<table border="1"> <thead> <tr> <th>#</th> <th>Milestones & Key Activities</th> </tr> </thead> <tbody> <tr> <td>A.</td> <td>Milestone</td> </tr> <tr> <td>1.</td> <td>Key Activity</td> </tr> <tr> <td>B.</td> <td>Milestone</td> </tr> <tr> <td>2.</td> <td>Key Activity</td> </tr> <tr> <td>C.</td> <td>Milestone</td> </tr> <tr> <td>3.</td> <td>Key Activity</td> </tr> </tbody> </table>		#	Milestones & Key Activities	A.	Milestone	1.	Key Activity	B.	Milestone	2.	Key Activity	C.	Milestone	3.	Key Activity	<table border="1"> <thead> <tr> <th>#</th> <th>M1</th> <th>M2</th> <th>M3</th> <th>M4</th> <th>M5</th> <th>M6</th> <th>M7</th> <th>M8</th> <th>M9</th> <th>M10</th> <th>M11</th> <th>M12</th> </tr> </thead> <tbody> <tr> <td>A.</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>1.</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>B.</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2.</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>C.</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>3.</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		#	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	A.													1.													B.													2.													C.													3.												
#	Milestones & Key Activities																																																																																																											
A.	Milestone																																																																																																											
1.	Key Activity																																																																																																											
B.	Milestone																																																																																																											
2.	Key Activity																																																																																																											
C.	Milestone																																																																																																											
3.	Key Activity																																																																																																											
#	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12																																																																																																
A.																																																																																																												
1.																																																																																																												
B.																																																																																																												
2.																																																																																																												
C.																																																																																																												
3.																																																																																																												
DEPENDENCIES		ASSUMPTIONS & RISKS																																																																																																										
• xxx		• xxx																																																																																																										

3.1.2.D ***Outline Technology Requirements:*** Identify and document the technology requirements necessary to support each prioritized document and content management initiative. This includes outlining the required tools, software, and systems needed to ensure successful implementation and adoption across the Entity.

3.1.2.E ***Document Assumptions:*** Record assumptions regarding resource availability, stakeholder engagement, and initiative complexity to ensure transparency and guide decision-making.

3.1.2.F ***Analyze Potential Risks:*** Clearly identify and assess risks associated with document and content management initiatives. This includes:

- Technical risks such as incompatibility with legacy systems, integration challenges with existing platforms, or DCM Tool performance limitations.
- Operational risks such as low user adoption due to lack of awareness or resistance to new workflows.
- Financial risks such as cost overruns from delayed implementations or underestimated resource needs.

3.1.2.G ***Assign Initiatives Ownership:*** The Data Management and Governance Section Head will be the owner of all document and content management initiatives. This designation ensures that the initiatives have a dedicated leader who can oversee progress and resolve roadblocks that may arise.

3.1.2.H ***Identify Key Stakeholders:*** Identify individuals and departments with a vested interest in document and content management, including business units, IT teams, records managers, legal advisors, and compliance officers. These stakeholders play a vital role in defining document workflows, retention requirements, metadata needs, and system features. Engaging the right stakeholders early ensures cross-functional alignment, accelerates decision-making, and promotes adoption of the document and content management plan across the Entity.

3.1.2.I ***Identify Interdependencies:*** Analyze how document and content management initiatives may impact or be influenced by existing or planned activities across the Entity. This includes:

- Reviewing how document digitization, archival, or publishing projects might intersect with data governance, IT modernization, or legal compliance initiatives
- Identifying overlapping teams, tools, or workflows involved in multiple initiatives to prevent duplication of effort
- Ensuring coordination between business units, IT, legal, and records management teams to align priorities and resource allocation

3.1.2.J

Develop Detailed Implementation Timeline: Break down each activity in an initiative into actionable steps with start and end dates, ensuring the timeline is realistic and achievable. Each step should have a clear description of the required task, dependencies on other activities, and allocated resources. Ensure that the timeline accounts for potential delays or risks identified earlier, so adjustments can be made without derailing the project.

3.1.2.K

Align Milestones with Timeline: Set specific checkpoints or milestones throughout the implementation to assess progress. These milestones allow the evaluation of whether the initiative is proceeding as planned and provide opportunities for course corrections.

Asset Guidance

The **Data Management Domain Plan Template** helps the Entity capture an overview of each identified initiative, detail its sub-activities, owners, stakeholders, and activity timeframe.

Illustrative

Data Management Initiative Plan Template								
The following table is a template capturing a brief overview of the domain relevant initiatives								
Field	Description							
Initiative ID	A unique identifier for each initiative to facilitate tracking and reference							
Initiative Title	the name of the initiative							
Initiative Description	A short description of the initiative, outlining its objectives and expected outcomes							
Cost	Estimated financial resources required for the initiative, including both direct and indirect costs							
Start Date	The date when the initiative is scheduled to begin							
End Date	The date by which the initiative is expected to be completed							
Interdependencies	Any other identified initiatives or projects that this initiative depends on for successful execution							
Assumptions	Conditions assumed to be true for the initiative's success (e.g., resource availability)							
Risks	Potential risks that could affect the initiative's success							

Initiative ID	Initiative Title	Initiative Description	Cost	Start Date	End Date	Interdependencies	Assumptions	Risks

Initiative ID	Initiative Title	Sub-activities	Owner	Stakeholder(s)	Status	Activity Timeframes		Roadmap			
						Start Date	Due Date	0	1	2	3
								1 Jan	8 Jan	15 Jan	###
DMSG-001					In Progress	1 Jul	30 Aug				
DMSG-002					Completed	1 Jul	31 Jan				
DMSG-003					Not Started	30 Mar	31 Jul				

3.1.2.L

Estimate Costs Associated with Each Initiative: Consider expenses related to tools, technology, personnel, and training required for effective implementation. Break down costs based on the needs of each task, such as acquiring software, hiring additional staff, or providing necessary training for existing teams. This step ensures the budget is well-planned, realistic, and includes all critical aspects to enable smooth implementation of the initiatives.

3.1.2.M

Develop Roadmap: Create an overall roadmap that outlines timelines, phases, and key milestones for implementing the prioritized document and content management initiatives. Sequence the initiatives based on dependencies, resource availability, and alignment with organizational goals. The roadmap should also include projected timelines for each initiative, allowing stakeholders to monitor progress and allocate resources effectively over time.

3.1.2.N

Gather Stakeholders' Feedback: Present the draft plan to all relevant parties, inviting input and suggestions to enhance its effectiveness. This feedback process helps surface any potential issues or overlooked areas, improving the plan's effectiveness and ensuring all voices are heard. Engaging stakeholders early also builds buy-in and commitment to the plan's success.

3.1.2.O

Incorporate Stakeholders' Feedback: Actively gather and incorporate constructive feedback from key stakeholders to refine the plan and ensure it aligns with their needs and expectations. This collaborative approach helps to address concerns early, fine-tune the details, and strengthen the overall effectiveness of the plan.

3.1.2.P

Obtain Approval of Document and Content Management Plan: After incorporating all feedback, the Data Management and Security Director will be presented with the finalized Document and Content Management Plan for review and approval. This ensures alignment with the Entity's priorities and secures the necessary support for successful implementation. Once approved, the plan can be formally adopted and published.

3.1.2.Q

Share Document and Content Management Plan with DGO: Submit the finalized Document and Content Management Plan to the National Data Governance Office (DGO) for review. The DGO will review the plan and provide recommendations, allowing the Entity to ensure their plan aligns with the broader national data program agenda and best practices.

RACI Matrix – Document and Content Management Plan

Indicative

Sr No.	Activity	DGO	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	Data Architect	Data Stewards	Data Strategy Expert
3.1.2.A	Outline Document and Content Management Initiatives		A	C	R		C	C
3.1.2.B	Prioritize Initiative Short List		A	C	R		C	C
3.1.2.C	Initiate Initiative Card Development and Outline Initiative Activities			A	R			C
3.1.2.D	Outline Technology Requirements			A	C	R	C	C
3.1.2.E	Document Assumptions			A	R		C	C
3.1.2.F	Analyze Potential Risks			A	R	C		C
3.1.2.G	Assign Initiatives Ownership		A	R	I			
3.1.2.H	Identify Key Stakeholders		A	R	C	C	C	
3.1.2.I	Identify Interdependencies			A	R	C		C
3.1.2.J	Develop Detailed Implementation Timeline			A	R	C		C
3.1.2.K	Align Milestones with Timeline			A	R	C		C
3.1.2.L	Estimate Costs Associated with Each Initiative			A	R		C	C
3.1.2.M	Develop Roadmap			A	R			C
3.1.2.N	Gather Stakeholders' Feedback			A	R			
3.1.2.O	Incorporate Stakeholders' Feedback			A	R			C
3.1.2.P	Obtain Approval of Document and Content Management Plan		A	R				
3.1.2.Q	Share Document and Content Management Plan with DGO	C/I	A	R				

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

Based on this Activity, the Entity can



Outline Document and Content Management Initiatives



Develop and Review Document and Content Management Plan

4. Document & Content Management Assessment & Design



4. Document & Content Management Assessment & Design

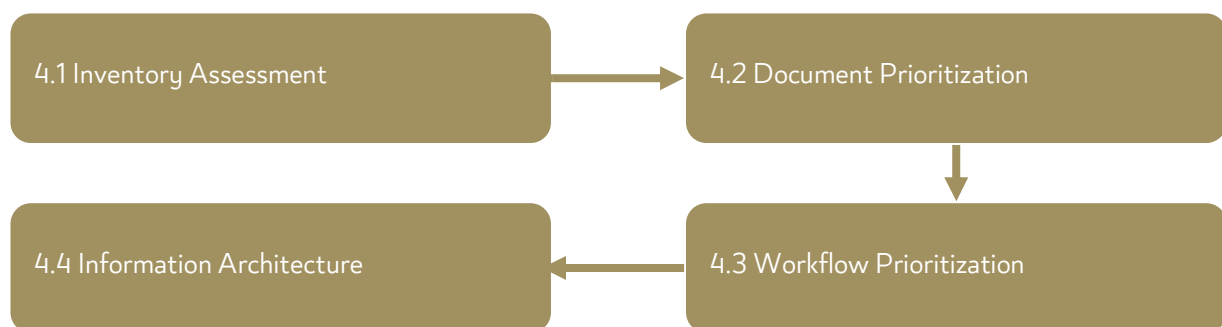
What is a Document & Content Management Assessment & Design and why does the Entity need it?

The Document & Content Management Assessment & Design process provides a structured approach for understanding, prioritizing, and organizing an Entity's documents and content in preparation for structured management and future automation. It translates policy into action by enabling the Entity to assess its current state, identify critical content and workflows, and design an information architecture that supports long-term content governance.

This process ensures that the Entity has clear visibility into where content resides, what types of documents exist, and which workflows are essential to daily operations or regulatory compliance. It allows departments to focus their efforts on high-impact assets and processes, and prepares the foundation for metadata tagging, workflow configuration, and tool implementation.

Through activities such as inventory assessment, document prioritization, workflow mapping, and architecture design, the Entity can reduce redundancy, improve lifecycle control, and optimize user access to key content. These activities enable better decision-making, more consistent governance, and stronger alignment with national standards.

The remaining sections of this chapter will detail the below activities that guide the Entity through executing the Document and Content Management Assessment & Design



Guiding Principles for Document & Content Management Assessment & Design

1. **Design for Actionability:** Ensure all outputs of the assessment (e.g., inventory, prioritization, architecture) are usable inputs for planning, tool configuration, and compliance tracking.
2. **Focus on High-Value Content:** Prioritize documents and workflows that are operationally critical, regulatory in nature, or high-risk — not everything needs to be inventoried or automated at once.
3. **Drive Cross-Departmental Participation:** Empower departments to contribute directly to content mapping and workflow definition, ensuring the assessment reflects the real landscape.
4. **Keep Implementation in Sight:** Design with the future DCM Tool and governance needs in mind — ensuring that structure, metadata, and user flows align with how the system will operate.

4.1 Inventory Assessment

The objective of this activity is to identify, document, and evaluate all document and content management systems currently in use within the Entity. This provides a foundational understanding for planning architecture, improving compliance, and ensuring lifecycle management of all documents and content types.

Process – Inventory Assessment

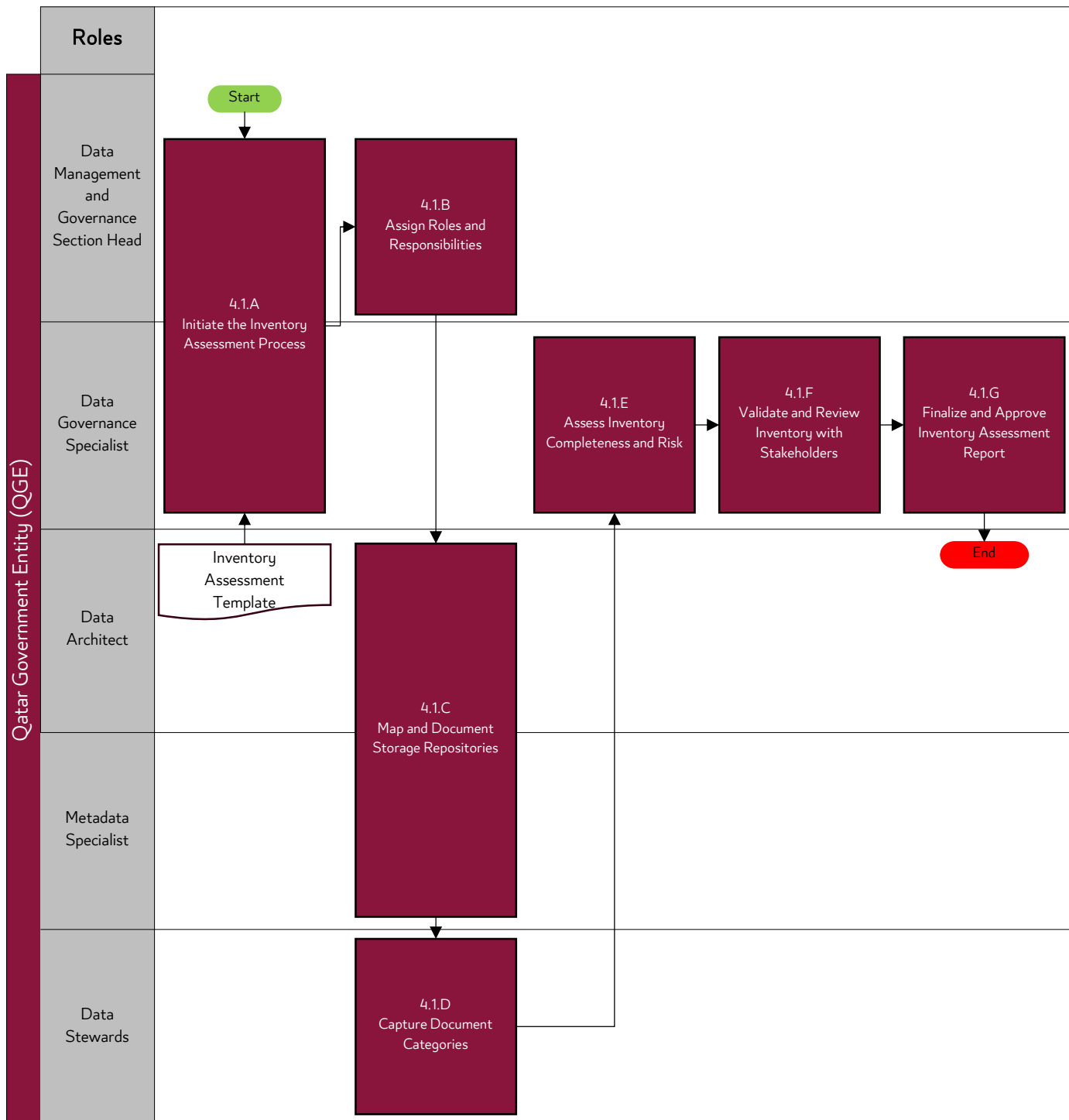


Figure 5: Inventory Assessment Process Map

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

Initiate the Inventory Assessment Process: The Data Management and Governance Section Head initiates the inventory assessment by defining its purpose, boundaries, and the resources required.

- i. **Define Assessment Objectives and Scope:** Clarify the intent, goals, and parameters of the assessment so that all contributors are aligned.

- a. **Clarify inventory goals:**

- Establish a baseline of all systems used for document and content management
- Enable downstream processes such as prioritization, retention planning, metadata enrichment, and risk remediation
- Identify legacy, redundant, or high-risk systems for remediation

- b. **Define the scope of systems to include:**

- Include any digital system, shared drive, web platform, or archive used to store documents, images, videos, or web content
- Cover current production systems and legacy systems that still contain content
- Emphasize that both on-premises and cloud-based platforms should be listed

- c. **Align stakeholders with the purpose of the activity:**

- Communicate that this is not a system audit or compliance check, but instead a foundational exercise
- Emphasize the role of this assessment in preparing for the DCM Tool implementation (Section 5.1)
- Reassure departments that the goal is not to assign blame but to capture the real landscape

- ii. **Develop Inventory Assessment Plan:** Create a structured plan that outlines timelines, responsibilities, and tools to be used.

- a. **Set timeline and phases:**

- Define a clear start and end date for the assessment
- Break the timeline into phases (e.g., kickoff, data gathering, review, consolidation)
- Specify deadlines for each department to submit their inputs

- b. **Identify the tools and templates to be used**

- Confirm use of the standardized Inventory Assessment Template provided by the Entity Data Office
- Prepare a sample filled-out version to help departments understand what good input looks like
- Share a review checklist so contributors can validate their inputs before submission

c. Allocate resources for support and monitoring

- Identify a Data Governance Specialist or support contact for questions
- Establish a shared email or help channel for real-time clarification requests
- Assign one focal point per department to receive updates and reminders

iii. **Communicate and Launch Assessment:** Begin the inventory assessment by providing departments with instructions and formally kicking off the effort.

a. Send the kickoff communication:

- Draft and issue a formal message from the Data Management and Governance Section Head
- Explain the importance of the activity and who is responsible in each department
- Include the start and end dates, links to templates, and help contacts

Asset Guidance

The **Change Management Communication Plan Email Template** is a sample email template the Entity can leverage to announce the assessment.

Illustrative

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]

4.1.A
Cont.
(3/3)

b. Distribute the required tools and instructions:

- Share the blank Inventory Assessment Template with each department
- Include a sample filled-in version for guidance

c. Offer live support and onboarding:

- Host a short onboarding session or virtual Q&A workshop
- Record the session and share the video with departments that cannot attend
- Encourage departments to submit their first draft early for feedback before final submission

Asset Guidance

The **Inventory Assessment Template** can be leveraged by the Entities to evaluate the current state of their document and content management systems.

Illustrative

Inventory Assessment						
This template can be leverage by entities to evaluate the current state of their document and content management systems						
Field	Description				Example	
System Name	Name of the document and content management system in use				SharePoint 2016	
System Type	Type of system (DMS, CMS, Shared Drive, Media Asset Manager, etc.)				Content Management System (CMS)	
Department	Department using the system				Finance	
Coverage Scope	Type of documents and content managed (e.g., policies, videos, web pages)				HR policies, training videos, press releases	
Format Type	Formats supported (e.g., PDF, MP4, HTML, JSON)				PDF, MP4, HTML	
Volume Estimate (GB)	Estimated storage volume				250	
Number of Users	Count of users accessing the system				40	
Access Control Mechanisms	Current access control and authorization method				LDAP, Role-based Access	
Version Control (Y/N)	Whether versioning is enabled				Yes	
Backup Mechanism	Backup method and frequency				Weekly incremental backup	
Integration with Other Systems	Systems integrated with the content/document platform				ERP, CRM	
Pain Points / Limitations	Challenges such as lack of tagging or support for large media				No tagging support for video content	
Comments	Additional notes				Requires metadata enrichment features	

System Name	System Type	Department	Coverage Scope	Format Type	Volume Estimate (GB)	Number of Users

Access Control Mechanisms	Version Control (Y/N)	Backup Mechanism	Integration with Other Systems	Pain Points / Limitations	Comments

4.1.B
(1/2)

Assign Roles and Responsibilities: The Data Management and Governance Section Head, with oversight from the Data Management & Security Director, assigns responsibilities for executing the inventory assessment and ensures coordination across departments.

i. Define Responsible Roles: Allocate inventory responsibilities across key data roles.

a. Assign core technical and governance roles:

- Appoint a Metadata Specialist to coordinate data collection for system attributes such as versioning, access control, and integrations
- Appoint a Data Architect to validate the completeness and technical accuracy of system metadata (e.g., formats, storage, infrastructure)
- Designate a Data Governance Specialist to monitor progress and ensure consistency

A

b. Assign business-facing coordination roles:

- Assign a Data Steward in each department to serve as the point-of-contact for collecting inputs
- Ensure each Data Steward understands their role in coordinating with colleagues and consolidating inputs
- Communicate expectations for Data Stewards, including timelines, support channels, and review processes

c. Define responsibilities at a high level:

- Clarify that Metadata Specialists and Data Architects are responsible for technical completeness
- Confirm that Data Owners must validate and approve the final information submitted for their systems
- Ensure all roles understand that they must collaborate to produce one unified inventory per department

ii. Assign departmental responsibilities: Formalize the assignment of inventory execution tasks to each participating business unit or department.**a. Communicate role assignments to departments:**

- Issue a role assignment memo to all department heads, copied to assigned Data Stewards and Data Owners
- Specify who is responsible for completing the inventory and who will review/approve it

b. Establish lines of accountability and escalation:

- Designate one Data Steward per department as the primary person responsible for completing the template
- Identify the Data Owner for each department who will validate and sign off on submitted inputs
- Assign the Data Governance Specialist as the escalation contact for late, missing, or unclear submission

4.1.C
(1/2)

A

Map and Document Storage Repositories: The Metadata Specialist and Data Architect jointly lead the process of consolidating and reviewing all physical and digital repositories used by the Entity for storing documents and unstructured content. This is based on the Inventory Assessment Templates submitted by departments.

- i. **Identify systems in use:** Use the Inventory Assessment Templates submitted by departments to compile and confirm the list of systems used to manage documents and content.

a. **Extract system entries from submitted templates:**

- Open each department's submitted template and review all entries under System Name and System Type
- Make note of systems that appear across multiple departments or are reused (e.g., SharePoint, Intranet)
- Ensure each system entry is linked to a department and clearly describes the document or content types it manages

b. **Cross-check system names and purposes:**

- Validate that each system has a clear business function and owner listed
- Flag entries with vague system names (e.g., "Old Files") or incomplete fields for follow-up
- Ensure only document and content related systems are included — exclude analytics platforms or business apps that don't serve as repositories

c. **Confirm coverage across all departments:**

- Identify departments that submitted no entries or only partial listings
- Look for signs of underreporting by comparing entries with known infrastructure (e.g., mapped drives, portals)
- Flag any missing or low-detail submissions for stakeholder follow-up in Step 4.1.F

- ii. **Leverage the Inventory Assessment Template:** Use the standard template fields to ensure all submitted data is complete, comparable, and ready for consolidation.

a. **Complete required system fields:**

- Check that each system includes System Name, System Type, Department, and Coverage Scope
- Verify that Format Type, Volume Estimate (GB), Number of Users, and Frequency of Access are filled and plausible
- Identify and flag placeholder entries (e.g., "TBD", "Unknown") for clarification

b. **Capture governance and control attributes:**

- Review Version Control, Access Control Mechanism, and Backup Mechanism fields for all systems

4.1.C
(2/2)

- Confirm that departments have noted the backup frequency and access method (e.g., “Role-based login via AD”)
- Flag entries where security details are vague or missing

c. Describe integrations and known limitations:

- Ensure the Integrations field lists any connections to other systems or platforms
- Review the Pain Points / Limitations field for insights into usability challenges, missing features, or compliance risks
- Use the Comments field to capture any noteworthy edge cases or department concerns

iii. **Validate and consolidate repository metadata:** After verifying the completeness and accuracy of submitted data, compile all entries into one Entity-wide master inventory.

a. Review for accuracy and internal consistency:

- Ensure each system entry is internally coherent and matches expected technical standards
- Standardize naming conventions (e.g., use “Shared Drive” instead of “Z:\” or “Team Folder”)
- Flag contradictory information (e.g., “Has backup: No” and “Backup type: Weekly”)

b. Coordinate technical validation with IT:

- Share questionable or unclear entries with IT for confirmation on system type, hosting, and integrations
- Validate backup mechanisms and access controls where systems are managed by central IT
- Confirm integration fields (e.g., API usage) with relevant technical staff

c. Compile the master inventory file:

- Merge all validated department templates into one consolidated file
- Remove duplicates, correct inconsistencies, and ensure uniform column headers across all entries
- Store the file in a secure shared location and apply version control
- Mark the file as “Working Master” until reviewed and finalized in 4.1.G
- Use this file as the input for subsequent activities, including ROT analysis (4.1.E) and prioritization (4.2)

Capture Document Categories: The Data Stewards, with input from Data Owners, analyze each documented system in the master inventory and describe the high-level types of documents and content stored within them. This provides a functional overview of what types of assets are managed and helps prepare for prioritization in Activity 4.2.

i. **Identify document and content categories:** Classify and describe the types of documents stored in each system using the "Coverage Scope" and related fields in the template.

a. **Categorize content types by function or business use:**

- Review the "Coverage Scope" field in each system entry
- Classify content into high-level types such as policies, contracts, forms, videos, reports, project files, records, media assets, or newsletters
- Add missing descriptions if only vague categories are listed (e.g., change "files" to "employee records and training documents")

b. **Identify formats used for each content type:**

- Review the "Format Type" column and check whether it matches the listed content types (e.g., policies are usually PDF or DOCX)
- Identify systems storing mixed formats (e.g., scanned images, spreadsheets, audio recordings) and ensure they are clearly described
- Flag uncommon or unsupported formats (e.g., .flv, .tiff, .msg) for future consideration in the DCM Tool planning

c. **Validate the classification with departments:**

- Share back questionable or generic entries (e.g., "documents," "miscellaneous") with the department for clarification
- Ask department data stewards to approve or refine document category labels before finalizing
- Encourage departments to be specific but not overly detailed — this is a high-level content grouping, not a document-level inventory

ii. **Identify content structure gaps and limitations:** Analyze the completeness and usability of content stored in each system, especially for areas that may present challenges in future structuring or automation.

a. **Detect unstructured or loosely organized systems:**

- Look for systems where content types are broadly defined or undefined (e.g., "Various folders by year")
- Flag systems where there is no folder hierarchy, metadata tagging, or classification applied to documents
- Identify systems that rely on filename conventions alone (e.g., "Invoice_2022_Approved_v3") instead of metadata

4.1.D
Cont.
(2/2)

b. Highlight usability and discoverability issues:

- Identify systems where departments have noted challenges such as:
 - “Can’t find documents easily”
 - “No consistent folder naming”
 - “Documents are duplicated across drives”
- Document these issues as flags for future enhancement and DCM Tool configuration work

4.1.E
(1/2)

Assess Inventory Completeness and Risk: The Data Governance Specialist performs a risk and ROT assessment using the master inventory. This step focuses on identifying systems with governance, compliance, or operational weaknesses, and flagging repositories with signs of redundant, obsolete, or trivial (ROT) content.

A

- i. **Identify ROT-prone systems:** Analyze metadata, comments, and pain points across the master inventory to find systems that may store outdated, redundant, or low-value content.

a. Detect unmaintained or obsolete systems

- Look for systems described with terms like “archive,” “legacy,” or “backup copy”
- Identify systems marked as rarely used, such as those with “Last Accessed: unknown” or “Monthly or less”
- Flag entries where departments noted phrases like “no longer updated” or “no clear owner”

b. Flag repositories with unstructured or unmanaged content:

- Note systems lacking folders, metadata tagging, or any classification logic
- Highlight descriptions such as “miscellaneous files,” “project leftovers,” or “scanned PDFs” without labeling
- Pay special attention to systems that mix content types with no lifecycle control (e.g., old + current + duplicates in one location)

c. Create a ROT risk summary:

- Tag systems in a new column in the master file with a “ROT Risk” flag (Yes / No / Unclear)
- Record a justification for each flag in a new column (e.g., “Contains old versions and backups from 2019”)
- Use this summary to support future cleanup and content reduction planning in the DCM Tool phase

- ii. **Evaluate governance, compliance, and security risks:** Assess whether each system is suitable for managing official content based on lifecycle, control, and sensitivity handling capabilities.

a. Identify governance and control weaknesses

4.1.E
Cont.
(2/2)

- Flag systems without version control, audit history, or owner assignment
- Look for shared drives or folders with no defined access restrictions
- Note systems used across multiple teams without centralized oversight

b. Detect compliance and retention risks:

- Identify systems storing documents with legal or regulatory value that lack backup or defined retention policies
- Cross-reference any sensitive content (e.g., HR, Legal, Financial) with their security classification — flag gaps
- Highlight storage platforms where no metadata tagging or review scheduling exists
- Add concise risk notes (e.g., “Open access folder for payroll records; no backup; used weekly”)

4.1.F
(1/2)

Validate and Review Inventory with Stakeholders: The Data Governance Specialist leads a structured review of the master inventory file with key oversight and operational stakeholders. This step ensures that ROT flags and risk assessments are accurate, that critical systems are not missed, and that the inventory is ready for approval and planning.

i. Coordinate Stakeholder Validation: Facilitate reviews with cross-functional roles to confirm the completeness and quality of the inventory, and to address risk concerns.

a. Identify the relevant stakeholders for review:

- Include the Information Security and Risk Management Section Head to review access control, backup methods, and security risks
- Include the Internal Audit function to confirm inventory traceability and documentation quality
- Involve Legal and Compliance representatives to validate retention risks, sensitive content handling, and documentation obligations
- Notify the IT Team for clarification on technical configuration or integration questions, if any remain

b. Share the inventory :

- Distribute the consolidated master inventory file to all reviewers
- Include ROT risk flags and other risks along with explanations

c. Conduct structured review sessions or workshops:

- Schedule one or more virtual or in-person review meetings with all relevant stakeholders
- Walk through flagged systems one by one, focusing on those marked as High Risk or ROT-prone
- Encourage reviewers to confirm or revise the ROT risk and risk comments, add missing justifications, or recommend reclassification

A

4.1.F
Cont.
(2/2)

- ii. **Resolve discrepancies and finalize flags:** Use reviewer input to refine, correct, or escalate flagged entries in the inventory.
 - a. **Clarify unclear or conflicting submissions:**
 - Revisit systems tagged as “Unclear” in ROT Risk or where governance fields were incomplete
 - Contact department-level Data Stewards for clarification if required
 - Update fields directly in the master inventory to reflect corrected or confirmed information
 - b. **Finalize ROT and risk designations:**
 - Update the ROT risk and other risks based on consensus during the review
 - Refine justification notes to reflect agreed-upon rationale (e.g., “Obsolete backup of project
 - Apply final labels for systems to be retained, reviewed later, or marked for potential decommissioning
 - c. **Confirm stakeholder sign-off:**
 - Send a follow-up confirmation request or sign-off memo to participating reviewers
 - Ask stakeholders to confirm in writing (email or approval log) that they reviewed and agreed with the assessment
 - Maintain a record of this review as an attachment to the final inventory in the document repository

4.1.G

Finalize and Approve Inventory Assessment Report: The Data Governance Specialist prepares and submits the final version of the inventory assessment report for formal approval by the Data Management and Governance Section Head. This report serves as the official baseline for content planning, cleanup, and DCM Tool implementation preparation.

- i. **Secure formal approval and integrate into planning:** Submit the inventory for final endorsement and use it to update the Entity’s Document and Content Management Plan.
 - a. **Submit report for sign-off:**
 - Send the master inventory to the Data Management and Governance Section Head
 - Include a formal approval memo or email with a request for sign-off
 - b. **Update the Document and Content Management Plan:**
 - Add inventory-driven actions to the roadmap (e.g., system cleanups, metadata standardization, archiving candidates)

A

RACI Matrix – Inventory Assessment

Indicative

Sr No.	Activity	Data Management and Security Director	Information Security and Risk Management Section Head	Data Management and Governance Section Head	Data Governance Specialist	Metadata Specialist	Data Architect	Data Owners	Data Stewards	Internal Audi	Data Compliance Specialist
4.1.A	Initiate the Inventory Assessment Process	A		R	R						
4.1.B	Assign Roles and Responsibilities	A		R	I	I	I	I	I		
4.1.C	Map and Document Storage Repositories			A		R	R				
4.1.D	Capture Document Categories			A				C	R		
4.1.E	Assess Inventory Completeness and Risk			A	R						
4.1.F	Validate and Review Inventory with Stakeholders		C	A	R					C	C
4.1.G	Finalize and Approve Inventory Assessment Report			A	R						

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

Based on this Activity, the Entity can



Initiate the Inventory Assessment Process



Finalize and Approve Inventory Assessment Report

4.2 Document Prioritization

This activity guides the Entity in selectively identifying and prioritizing the most operationally and strategically important documents and content types for structured management within the Document and Content Management Tool. Prioritization enables the Entity to focus its digitization, migration, classification, and retention efforts on high-impact assets first that support critical functions, compliance, and service delivery.

Process – Document Prioritization

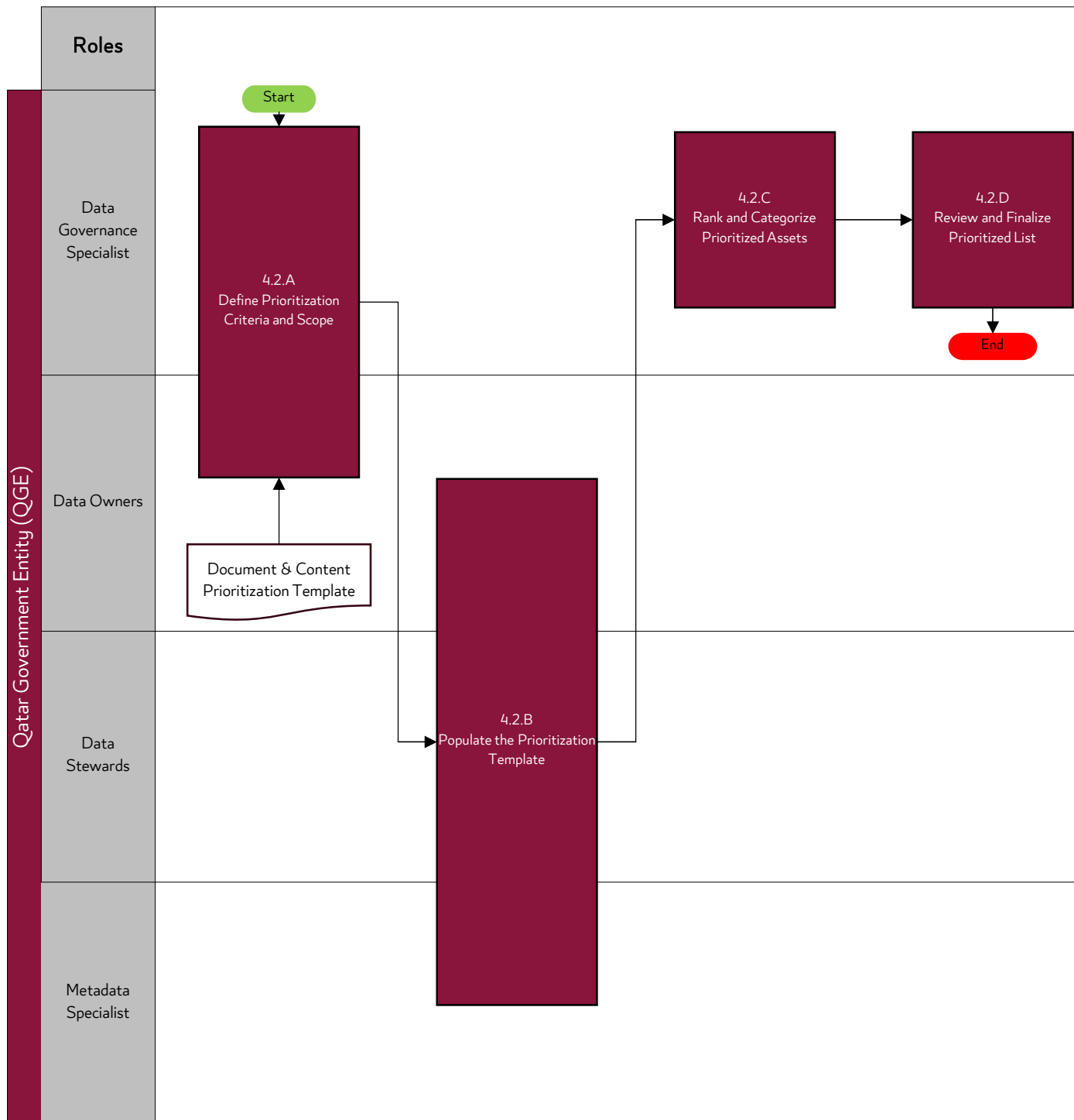


Figure 6: Document Prioritization Process Map

Legend:

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

Define Prioritization Criteria and Scope: The Data Governance Specialist, in coordination with Data Owners, defines how departments will select which documents or content assets to prioritize for structured management. The goal is to narrow the focus to high-value, high-risk, or high-impact assets.

- i. **Establish Prioritization Criteria:** Develop clear, practical rules to help departments identify the most important content to include.

- a. **Define threshold criteria for prioritization:**

- Select documents or content items that are critical to business operations or public service delivery
- Include items required to meet legal, regulatory, or audit obligations (e.g., HR records, financial statements, licensing documents)
- Prioritize assets frequently accessed by staff or external users (e.g., internal policies, manuals, procedures)
- Include sensitive content (e.g., contracts, personal data) that requires strong access controls
- Capture known pain points, such as documents without version control, or stored in non-compliant locations

- b. **Create a short eligibility checklist for departments:**

- Prepare a simple “Should This Be Prioritized?” list with Yes/No questions such as:
 - Does this content support a critical business process?
 - Is this document legally required to be retained?
 - Is the current storage location unstructured or insecure?
 - Is this content regularly accessed, reused, or shared?
- Include this checklist in the guidance package sent to departments with the Document & Content Prioritization Template (detailed in 4.2.B)

- c. **Provide examples of high-priority assets**

- **Example 1:** Employee onboarding templates stored on a shared drive with no access control
- **Example 2:** Compliance records for annual audits with undefined retention timelines
- **Example 3:** Citizen-facing web content that must go through a defined publishing process

- ii. **Define Scope of Review:** Clarify the limits of this activity and communicate realistic expectations to departments.

- a. **Set limits on how many items each department should prioritize:**

4.2.A
(2/2)

- Focus on high-value areas such as HR, Legal, Finance, Operations, Planning, and Public Services
- Exclude trivial, obsolete, or low-use materials for this round

b. Focus on high-value departments and business domains:

- Ask departments in high-risk areas (e.g., Legal, HR, Finance, Audit) to participate first or with more items
- Encourage shared services departments (e.g., IT, Procurement) to coordinate with business owners before listing shared documents

c. Confirm review approach with Data Owners:

- Schedule short calls or messages with Data Owners to review prioritization criteria
- Answer any questions about what qualifies as “priority” in their context
- Send a confirmation email summarizing what’s expected from each department

4.2.B
(1/3)

Populate the Prioritization Template: The Data Stewards, with input from Data Owners and support from the Metadata Specialist, document each selected high-priority document or content asset using the standardized Document & Content Prioritization Template. The goal is to consistently capture relevant details for planning future structuring, retention, access control, and automation.

i. Complete the Required Fields: Enter detailed metadata for each prioritized content asset using the provided template.

a. Gather input from content owners:

- Meet with content creators or process owners who work with the documents daily
- Ask them to describe what the asset is, who uses it, and how often it is accessed
- Collect any missing details that the Data Steward cannot answer alone

b. Fill in all fields in the prioritization template:

- Use the unique Item ID to label each row (e.g., “DOC-001”)
- Populate Document/Content Title, Department, and Business Process Supported
- Complete Asset Type (Document, Video, Web Page, etc.) and Format Type (DOCX, PDF, MP4, etc.)
- Indicate the Sensitivity Classification (Restricted, Internal, Public, etc.)
- Specify Frequency of Access (Daily, Monthly, Rarely, etc.)
- Note whether there is a Legal/Regulatory Requirement (Yes/No)
- Enter the required Retention Period (e.g., “5 years,” “Permanent”)
- Assign a Priority Level (High / Medium / Low) based on 4.2.A criteria
- Use the Comments field for any additional explanation or context

A

4.2.B
(2/3)

c. Use clear and specific language:

- Avoid vague entries like “used often” — instead write “used weekly by Finance team for reconciliation”
- Do not leave any fields blank — use “Not Applicable” if truly irrelevant
- Ensure each row refers to a specific document or distinct content item — not a general category

ii. **Validate input quality:** Review entries for accuracy, completeness, and consistency before submission.

a. Conduct internal peer review:

- Ask a second Data Steward to double-check the entries
- Cross-check priority levels against the eligibility criteria from 4.2.A
- Confirm that formats and classifications are consistent (e.g., avoid mixing “Internal” and “Confidential” arbitrarily)

b. Coordinate with the Metadata Specialist for technical alignment:

- Ask the Metadata Specialist to review entries involving uncommon formats, mixed content types, or complex workflows
- Verify if selected content types will require special metadata fields in the future (e.g., web content vs. videos)

c. Finalize and submit Team-level entries:

- Save the completed template using the agreed naming convention (e.g., “HR_DocPrioritization_v1.xlsx”)
- Submit the finalized version to the Data Governance Specialist via a designated folder or channel
- Confirm submission and keep a local copy in case further clarification is needed in later steps

4.2.B
Cont.
(3/3) **Asset Guidance**

The **Document & Content Prioritization Template** can be leverage by the Entity to identify and prioritize key documents and content assets.

Illustrative

Document & Content Prioritization					
This template can be leverage by entities to identify and prioritize key documents and content assets for management, digitization, or migration					
Field	Description				Example
Item ID	Unique identifier for each document or content item				DOC-001
Document/Content Title	Title of the document or content asset				Social Media Policy
Department	Department responsible				Marketing
Business Process Supported	Business workflow that uses or generates this content				Internal Communications
Asset Type	Type of content (e.g., Document, Image, Video, Web Page)				Document
Format Type	Format of the asset				DOCX, MP4, HTML
Sensitivity Classification	Data classification level				Internal
Frequency of Access	How often the asset is accessed or used				Monthly
Legal/Regulatory Requirement	Whether retention is mandated by law or regulation				Yes
Retention Requirement	Required duration before disposal/archive				5 Years
Priority Level	Priority for digitization, migration, or management (High, Medium, Low)				High
Comments	Additional notes				Needed for compliance audit
Item ID	Document/Content Title	Department	Business Process Supported	Asset Type	Format Type
Sensitivity Classification	Frequency of Access	Legal/Regulatory Requirement	Retention Requirement	Priority Level	Comments

4.2.C
(1/3)

Rank and Categorize Prioritized Assets: The Data Governance Specialist consolidates all department-level prioritization templates into a single master file and performs analysis to rank the assets by priority level, identify cross-departmental trends, and detect any participation or content gaps.

i. **Consolidate department submissions into a master file:** Combine all validated departmental templates into one structured, entity-wide prioritization list.

a. **Collect and merge all department-level templates:**

- Confirm receipt of each department's completed Document & Content Prioritization Template
- Ensure each file uses the standardized format and naming convention (e.g., "Legal_DocPrioritization_v1.xlsx")
- Follow up with departments that submitted incomplete templates or missed the submission
- Copy all entries into a centralized master spreadsheet

b. **Apply quality checks across the merged file**

- Remove duplicates (e.g., same document listed by multiple departments)

A

- Verify that the Priority Level, Sensitivity Classification, and Retention Requirement fields are filled for every row
- Use filters to identify blank, inconsistent, or illogical values and flag them for clarification in 4.2.D

ii. **Group items by priority level:** Organize the consolidated list into High, Medium, and Low categories to guide resource allocation and planning.

a. **Sort all assets by Priority Level:**

- Use the “Priority Level” column to group entries as High, Medium, or Low
- Count the total number of assets in each category and calculate percentage distribution
- Highlight High priority assets for inclusion in upcoming DCM Tool configuration or workflow planning

b. **Analyze the characteristics of each group:**

- For each group, assess patterns in Format Type, Sensitivity Classification, and Retention Requirement
- Check whether High-priority assets are concentrated in certain departments or content types
- Identify formats that may pose technical challenges for the DCM Tool implementation (e.g., videos, custom HTML)

c. **Flag inconsistencies in prioritization:**

- Look for assets marked as “High Priority” with minimal usage or no legal retention requirement — validate these in Step 4.2.D
- Detect departments that marked nearly everything as “High” or “Low” — request justification if needed
- Note any “Medium” or “Low” assets that appear mission-critical or sensitive and may warrant review

iii. **Analyze content distribution and participation gaps:** Evaluate how well the prioritized asset list covers departments, content types, and business needs.

a. **Summarize distribution by department:**

- Count how many assets each department submitted and how many were High priority
- Identify departments with unusually low participation or generic entries (e.g., all “Forms,” all “Misc Docs”)
- Highlight departments with no participation — escalate if they are high-risk functions (e.g., HR, Legal)

4.2.C
Cont.
(3/3)

b. Review distribution by content type and process:

- Analyze trends across Business Process Supported (e.g., most documents supporting “Procurement” or “Audit”)
- Look for underrepresented but important domains (e.g., no documents tied to citizen-facing services)
- Identify opportunities to standardize document types or naming across departments

c. Document findings and prepare for validation:

- Add summary tabs or charts to the master prioritization file to show distribution and gaps
- Prepare a short list of unclear entries, missing departments, or questionable classifications to raise in 4.2.D
- Save the master prioritization file as “DocPrioritization_Master_v1.xlsx” and apply version control

4.2.D
(1/2)

Review and Finalize Prioritized List: The Data Governance Specialist leads the review of the consolidated prioritization file with stakeholders to validate unclear entries, resolve discrepancies, and finalize the master list of high-priority documents and content assets for downstream structuring and DCM Tool planning.

A

i. **Conduct Stakeholder Validation:** Present the analyzed master list to department heads, legal, compliance, and technical stakeholders for review and clarification.

a. Flag entries for department review:

- Highlight rows with vague or generic titles (e.g., “Docs_2022” or “Misc Files”)
- Point out assets marked High priority but missing business process, retention, or sensitivity classification
- Flag inconsistent classifications (e.g., documents marked “Confidential” with “No” under legal requirement)

b. Share the draft master prioritization file:

- Distribute the consolidated master file (from 4.2.C) to all departments that participated
- Include summary statistics by department and a list of flagged entries needing clarification

c. Facilitate review sessions or feedback windows:

- Give departments a 3–5 day window to submit updates or corrections
- Host optional 1:1 calls with departments to walk through their entries
- Ask departments to provide written confirmation once their entries are finalized

4.2.D
(2/2)

ii. **Refine and approve the finalized list:** Use the validation feedback to clean and close out the prioritization activity.

a. **Apply updates and corrections to the master file:**

- Revise priority levels, add missing metadata, or correct inaccurate classifications as requested
- Normalize inconsistent formatting or naming (e.g., unify document titles or business process terms)
- Track changes in a separate tab or log for auditability

b. **Resolve outstanding issues with stakeholders:**

- Escalate unresolved questions (e.g., unclear retention or legal obligation) to Legal, Compliance, or the Data Owner
- Remove duplicate or invalid entries that were mistakenly included
- Clarify ownership or process alignment if the same content is listed by multiple departments

c. **Finalize and version-control the master file:**

- Save the approved file
- Apply metadata such as approval date, version, owner, and review cycle
- Store the file for later use in activity 5.1 (Tool Implementation)

RACI Matrix – Document Prioritization

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	Metadata Specialist	Data Owners	Data Stewards	Internal Audi	Data Compliance Specialist
4.2.A	Define Prioritization Criteria and Scope		A	R		R			
4.2.B	Populate the Prioritization Template		A	I	R	R	R		
4.2.C	Rank and Categorize Prioritized Assets		A	R					
4.2.D	Review and Finalize Prioritized List	I	A	R	C	C	C	C	C

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

Based on this Activity, the Entity can



Define Document & Content Prioritization Criteria



Review and Finalize Prioritized List of Documents & Content

4.3 Workflow Prioritization

This activity enables the Entity to identify, assess, and prioritize document and content related workflows for automation within the Document and Content Management Tool. Prioritization is based on criteria such as business impact, manual burden, and feasibility of automation. The goal is to focus automation efforts on workflows that significantly improve efficiency, reduce risk, and support timely publishing or service delivery.

Process – Workflow Prioritization

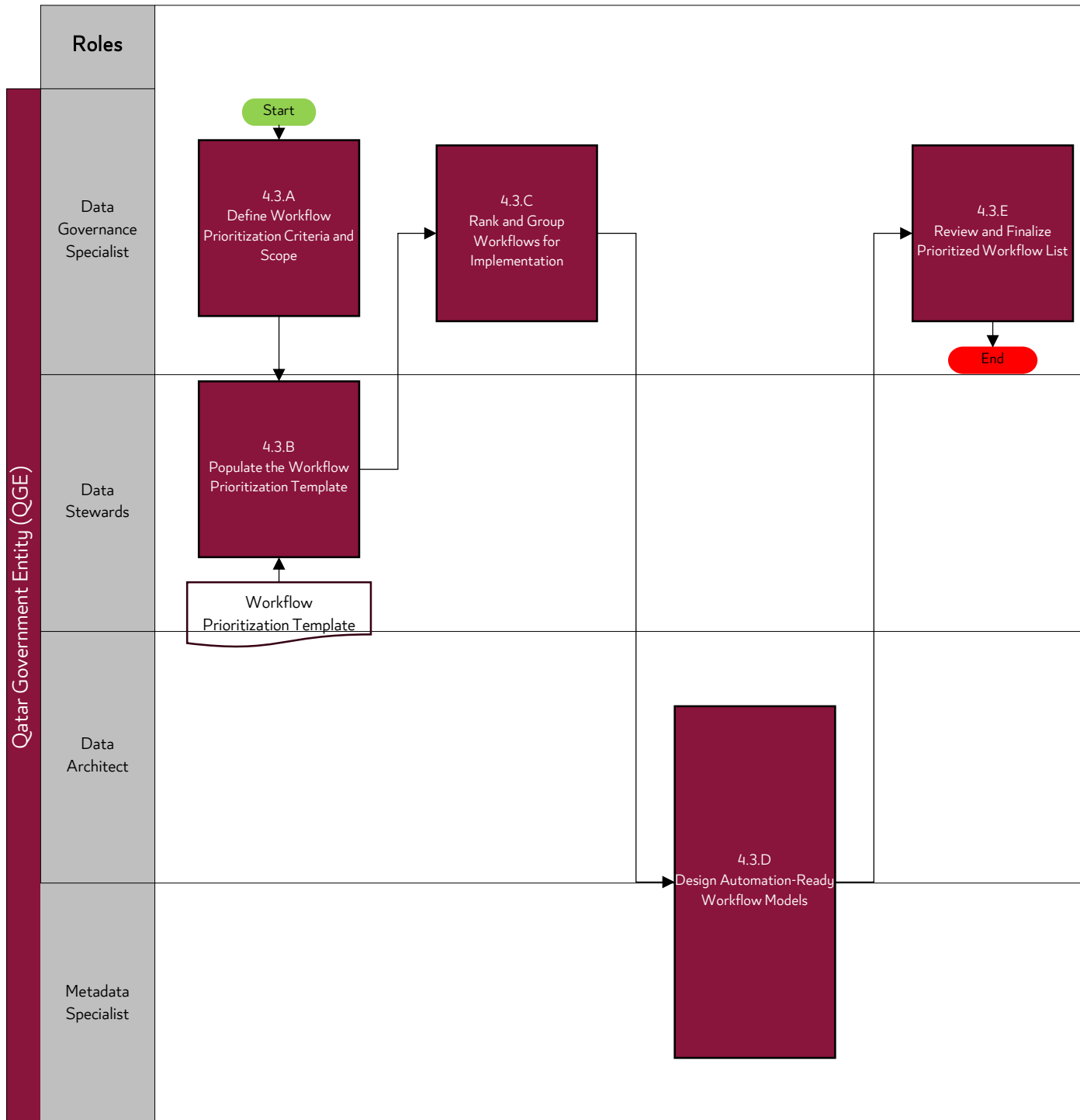


Figure 7: Workflow Prioritization Process Map

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

4.3.A
(1/2)

A

Define Workflow Prioritization Criteria and Scope: The Data Governance Specialist, in collaboration with Departmental Focal Points, defines how departments will identify document and content related workflows for prioritization. The focus is on selecting high-value workflows that can be feasibly automated in the future DCM Tool, based on business impact and implementation readiness.

i. **Establish workflow evaluation criteria:** Provide departments with clear guidelines to help them identify workflows that should be prioritized for potential automation.

a. **Define key evaluation factors:**

- Prioritize workflows with high operational impact (e.g., delays in this workflow slow down service delivery or audits)
- Focus on workflows with medium to high manual effort that could benefit from automation
- Consider workflows with frequent execution (e.g., daily, weekly, or high volume monthly processes)
- Include workflows that involve multiple roles or departments, requiring structured routing and approvals

b. **Create a checklist to guide departments:**

- Provide “Should This Workflow Be Prioritized?” prompts such as:
 - Is this workflow critical to delivering services or meeting regulatory deadlines?
 - Does it involve multiple manual approvals or handovers?
 - Is it often delayed, duplicated, or error-prone due to lack of structure?
- Include these prompts as part of the instruction sheet for the Workflow Prioritization Template (detailed in 4.3.B)

c. **Provide examples of qualifying workflows:**

- **Example 1:** Content publishing approval (e.g., internal policy or press release review)
- **Example 2:** Records retention review and disposal approval
- **Example 3:** Contract template usage and routing for approval

ii. **Define scope of departmental participation:** Limit the scope of review to workflows that are realistically automatable and clearly tied to document or content handling.

a. **Request department-level workflow nominations:**

- Ask each department to identify document/content-related workflows they rely on regularly
- Focus on workflows that involve preparing, reviewing, approving, or publishing a document or media asset

4.3.A
Cont.
(2/2)

- Instruct departments to avoid generic business workflows unrelated to content (e.g., meeting scheduling)

b. Clarify what is out of scope:

- Exclude one-time or irregular processes that aren't repeatable (e.g., annual event planning)
- Exclude workflows that happen entirely outside the DCM Tool
- Exclude overly broad or vague submissions (e.g., "email approvals") for clarification later in 4.3.E

c. Confirm expectations and submission timelines:

- Share a deadline and instructions for completing the Workflow Prioritization Template
- Provide a support contact in case departments need clarification or help documenting their workflows

4.3.B
(1/3)

Populate the Workflow Prioritization Template: The Data Stewards, with support from Departmental Focal Points and oversight from the Data Governance Specialist, document candidate workflows using the standardized Workflow Prioritization Template. The goal is to consistently capture critical information needed to analyze, rank, and plan automation-ready document and content workflows.

i. **Complete workflow metadata:** Capture all required details in the workflow prioritization template to describe each workflow clearly and accurately.

a. Gather input from process owners:

- Meet with individuals who manage or participate in the workflow (e.g., approvers, publishers, document creators)
- Ask them to describe the workflow in plain language from beginning to end
- Clarify key attributes such as how often it occurs, how long it takes, and who is involved

b. Fill in all fields in the template for each workflow:

- Assign a unique Workflow ID (e.g., "WF-001") and provide a descriptive Workflow Name
- Specify the Department and the Business Process Supported (e.g., "Content Approval", "Document Archival")
- Enter the Frequency of Use (Daily, Weekly, Monthly, etc.) and Number of Users Involved
- Estimate the current Manual Processing Time (e.g., "3 Days," "5 Hours")

A

4.3.B
(2/3)

- Assess the Complexity Level of automating the process (Low / Medium / High)
- Describe the Impact on Operations if the workflow is delayed or mismanaged
- Indicate the Content/Document Type Involved (e.g., Policy, Video, Case File)
- Specify the Publishing Channel (e.g., Website, Intranet, Email, Archive)
- Assign a Priority Level (High, Medium, Low) based on 4.3.A criteria
- Use the Comments field to provide context or highlight known pain points

Asset Guidance

The **Workflow Prioritization Template** can be leveraged by entities to identify and rank workflows that are candidates for automation.

Illustrative

Workflow Prioritization Template	
This template can be leveraged by entities to identify and rank workflows that are candidates for automation within a Document and Content Management System	

Field	Description	Example
Workflow ID	Unique identifier for the workflow	WF-001
Workflow Name	Name or title of the workflow	Content Publishing Approval
Department	Department that owns or runs the workflow	Communications
Business Process	Process supported	Press release review and approval
Frequency of Use	How often the workflow is executed	Weekly
Number of Users Involved	How many people typically participate	10
Manual Processing Time	Time required to complete manually	3 Days
Complexity Level	Complexity to digitize or automate (Low, Medium, High)	Medium
Impact on Operations	Business impact of delays or inefficiency	High
Content/Document Type Involved	Type of asset handled in the workflow (e.g., Video, Web Page, Policy Doc)	Web Page
Publishing Channel	Where the final asset is published or delivered (e.g., Website, Intranet, Newsletter)	National Portal
Priority Level	Priority for automation or optimization (High, Medium, Low)	High
Comments	Additional notes	Approval delays impact timeliness

Workflow ID	Workflow Name	Department	Business Process	Frequency of Use	Number of Users Involved	Manual Processing Time

Complexity Level	Impact on Operations	Content/Document Type Involved	Publishing Channel	Priority Level	Comments

- ii. **Validate submitted entries:** Review department submissions for completeness, clarity, and technical feasibility.

a. **Conduct peer review by Data Stewards:**

- Review the populated workflow prioritization template for consistency and proper formatting
- Flag workflows with unclear steps, missing users, or unrealistic complexity ratings
- Ensure workflows are document or content related, and not general task lists or business activities

b. **Perform technical alignment checks with the Metadata Specialist:**

- Ask the Metadata Specialist to review workflows involving unusual content types or external publishing platforms
- Check whether automation features like notifications, versioning, or metadata tagging are feasible
- Note any workflows that would require integration with other systems (e.g., legal approvals tied to contract management software)

4.3.B
Cont.
(3/3)c. **Finalize and submit workflows:**

- Save the completed template using the agreed naming format (e.g., “Finance_WorkflowPrioritization_v1.xlsx”)
- Submit the finalized file to the Data Governance Office via the designated workspace or shared folder
- Keep a local backup and notify the Data Governance Specialist once the submission is complete

4.3.C
(1/2)

Rank and Group Workflows for Implementation: The Data Governance Specialist consolidates all department-level workflow submissions into a single master file, analyzes the entries based on priority and feasibility, and categorizes them to guide structured planning for future DCM Tool-based workflow automation.

i. **Consolidate department workflow submissions:** Combine all submitted Workflow Prioritization Templates into a single master file for analysis.

a. **Collect and review department-level templates:**

- Confirm receipt of all departmental submissions
- Verify that templates use the standardized format and include all required fields
- Follow up with departments that submitted partial templates or missed the deadline

b. **Compile workflows into a central master file**

- Copy all validated rows into one consolidated Excel workbook
- Standardize column headers and field values (e.g., ensure all Priority Levels use “High / Medium / Low”)
- Retain a column for “Department” to preserve traceability and support department-level reporting

c. **Clean and normalize the consolidated data**

- Remove duplicate entries (e.g., same workflow submitted by different teams)
- Resolve inconsistencies in terminology across submissions (e.g., “Policy Approval” vs. “Policy Sign-off”)
- Apply version control and label the master file appropriately (e.g., “WorkflowPrioritization_Master_v1.xlsx”)

ii. **Analyze value and feasibility for implementation:** Evaluate each workflow’s potential to be implemented efficiently and effectively based on impact vs. complexity.

a. **Plot workflows on a quick-win matrix:**

A

4.3.C
(2/2)

- **Use two axes:** Business Impact (High/Medium/Low) and Automation Complexity (High/Medium/Low)
- **Identify “Quick Wins”:** High Impact + Low Complexity (e.g., policy approval with defined roles and few steps)
- **Identify “Strategic Priorities”:** High Impact + Medium/High Complexity (e.g., records disposal workflows with legal controls)

b. Highlight automation barriers and special considerations:

- Mark workflows requiring integration with other systems (e.g., ERP, contract management)
- Flag processes involving complex branching logic, parallel approvals, or unique file types
- Note content types or publishing channels that might be unsupported in the future DCM Tool (e.g., video workflows)

c. Document readiness and grouping for future waves:

- Add a “Readiness Rating” column (e.g., Ready / Needs Redesign / Too Complex)
- **Propose grouping workflows into implementation waves:**
 - **Wave 1:** Quick Wins
 - **Wave 2:** Medium Complexity, Medium Impact
 - **Wave 3:** High Complexity
- Save this plan as a working draft for validation in Step 4.3.E

4.3.D
(1/2)

A

Design Automation-Ready Workflow Models: The Data Architect and Metadata Specialist, in collaboration with business units, prepare structured designs for the highest-priority workflows. These designs describe how content moves through people, systems, and approvals, and ensure that key details are captured for future DCM Tool automation planning.

i. **Define Workflow Steps and Logic:** Document the internal flow of each top-priority workflow in a structured, step-by-step format.

a. Create a visual or tabular map of each workflow:

- Use flowcharting tools (e.g., Visio, Lucidchart, or Excel) to show the progression of the workflow
- For each step, include who performs the task, what they do, and what document or data is involved
- Identify the entry point (trigger) and exit point (final status or output) of the workflow

4.3.D
(1/2)**b. Use a standard modeling method such as BPMN:**

- Represent activities, roles, decisions, and document transitions using simple shapes and connectors
- Highlight approval steps, conditions, or branches (e.g., “If rejected, return to initiator”)
- Include swimlanes to distinguish responsibilities across departments or users

c. Document workflow metadata and system actions:

- Specify whether each step involves document upload, tagging, status change, or routing
- Note actions such as “send email notification,” “assign task,” or “lock version”
- Use consistent terminology for metadata fields referenced in the workflow (e.g., “Status = Final”)

ii. Identify input and output requirements: Capture what types of documents are processed by the workflow and what metadata, outputs, or approvals are expected.**a. Link each workflow to the prioritized content it supports (from 4.2):**

- Identify the Document Type(s) involved (e.g., Policy, Contract, Case File)
- Cross-reference each workflow with related items in the Document Prioritization Master File (if applicable)

b. Define required metadata and document status at key stages:

- Identify what metadata must be applied or updated at each step (e.g., “Tag with ‘Approved by Legal’”)
- Document status changes throughout the process (e.g., “Draft” → “In Review” → “Published”)
- Specify which metadata fields are optional vs. mandatory

c. Clarify business rules and triggers:

- Define conditions that affect the flow (e.g., “Auto-approve if no comment within 3 days”)
- Note escalation paths, rejections, or rerouting rules
- Include decision logic that may need to be implemented later in the DCM Tool workflow engine

iii. Assess technical alignment and configuration needs: Prepare for implementation by assessing the feasibility of automation in the future DCM Tool.**a. Review workflow logic for technical feasibility:**

- Flag steps requiring integrations with external systems (e.g., e-signature platforms, ERP)

4.3.D
Cont.
(2/2)

- Note any content types or publishing channels that are non-standard (e.g., YouTube publishing, mobile apps)
- Mark workflows that involve attachments or structured forms (e.g., web forms, PDFs with metadata)

b. Document configuration implications for future implementation:

- Identify roles that will need to be configured in the DCM Tool (e.g., Reviewer, Approver, Publisher)
- Note requirements for task notifications, versioning behavior, and access control at each step
- Include any assumptions or limitations (e.g., “Assumes content already exists in DCM Tool”)

c. Store workflow models for use in Section 5.1:

- Save each model in a shared location using a clear naming convention (e.g., “HR_PolicyApproval_WorkflowModel_v1”)
- Keep a table of all modeled workflows with links to each file and status of design review
- Leverage these models during the DCM Tool configuration phase

4.3.E
(1/2)

Review and Finalize Prioritized Workflow List: The Data Governance Specialist leads a structured review of all designed workflow models and the consolidated prioritization file. The goal is to validate the logic, metadata dependencies, and implementation feasibility of each workflow with key stakeholders and finalize the list of workflows to be considered for DCM Tool configuration.

A

i. Conduct Stakeholder Review: Organize cross-functional feedback sessions to review workflow models, address inconsistencies, and confirm priorities.

a. Identify and invite relevant reviewers:

- Include Department Heads or workflow owners to confirm accuracy of documented processes
- Include IT to validate technical feasibility and system compatibility
- Include Legal, Compliance, or Risk Officers for workflows involving sensitive or regulated content

b. Present each workflow model and key metadata:

- Walk through visual or tabular models step by step, including roles, decisions, and content flow
- Highlight document types involved, required metadata, and publishing channels
- Discuss business rules, escalation paths, and conditions defined in each model

c. Capture feedback and validation input:

- Use a feedback tracker or review log to document requested changes, missing steps, or approval delays
- Mark workflows as “Approved,” “Needs Revision,” or “Pending Clarification”
- Ask reviewers to submit follow-up comments or approvals in writing (email or tracked comments)

ii. Refine and approve finalized workflow list: Incorporate feedback, close open questions, and formally finalize the workflow designs and their assigned priority.**a. Apply changes based on stakeholder input:**

- Edit workflows to reflect agreed role changes, process simplifications, or additional routing steps
- Update metadata fields or logic where reviewers suggested corrections
- Standardize naming conventions, swimlane formatting, or notation styles if inconsistent

b. Confirm final priority and readiness status:

- Revisit workflows marked “Medium” or “High” priority during review and adjust based on updated business value
- Categorize workflows into proposed implementation waves for use in Section 5.1

c. Finalize and archive the approved workflow models:

- Save each finalized workflow model file in a structured shared location
- Mark this deliverable as ready for handoff to the technical team or vendor for use in tool configuration and workflow engine design

RACI Matrix – Workflow Prioritization

Indicative

Sr No.	Activity	Data Management and Governance Section Head	Data Governance Specialist	Metadata Specialist	Data Architect	Data Stewards	Department Focal Point	IT Team	Data Compliance Specialist
4.3.A	Define Workflow Prioritization Criteria and Scope	A	R				C		
4.3.B	Populate the Workflow Prioritization Template	A				R	C		
4.3.C	Rank and Group Workflows for Implementation	A	R						
4.3.D	Design Automation-Ready Workflow Models	A		R	R		C		
4.3.E	Review and Finalize Prioritized Workflow List	A	R					C	C

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

Based on this Activity, the Entity can



Define Workflow Prioritization Criteria



Design Workflow Models

4.4 Information Architecture

This activity focuses on designing a future-ready information architecture that will guide the structured organization, classification, and navigation of documents and content across the Entity. It enables consistency, compliance, discoverability, and usability of documents, and ensures alignment with metadata, taxonomy, and governance practices. While implementation will occur after DCM tool selection (Section 5.1), the design established here will serve as a blueprint for configuration.

Process – Information Architecture

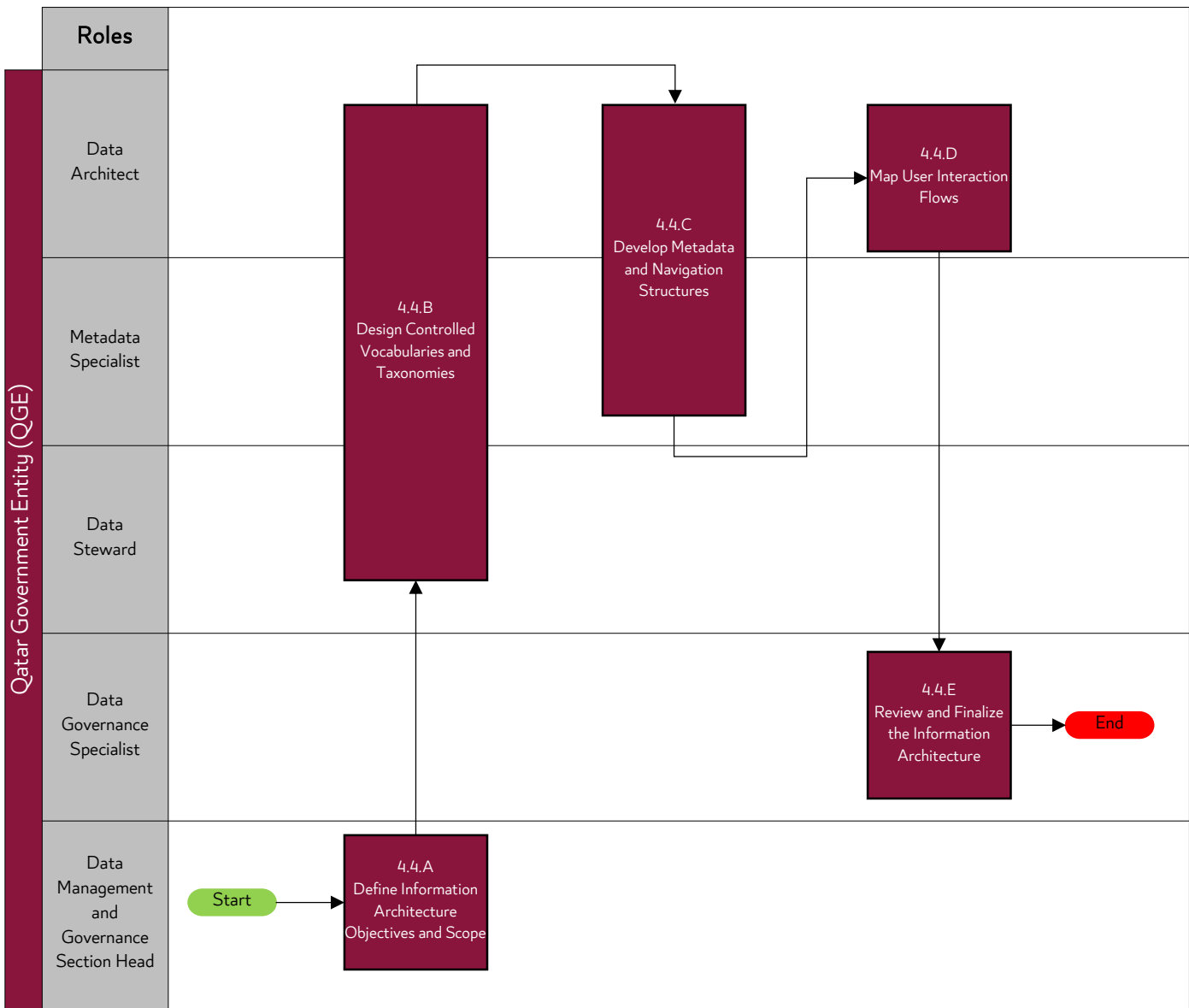


Figure 8: Information Architecture Process Map

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

Define Information Architecture Objectives and Scope: The Data Management and Governance Section Head leads the definition of the information architecture's purpose, business alignment, and coverage boundaries. This activity sets the strategic direction for how content will be organized, classified, and made accessible across platforms.

i. **Establish architecture goals:** Clarify what the Entity's information architecture is intended to achieve and how it supports both governance and usability.

a. **Align the architecture with business and user needs:**

- Ensure that the architecture supports content discovery, usability, and operational efficiency
- Emphasize that structured organization will improve findability, reduce duplication, and streamline publishing
- Link the architecture design to pain points raised during inventory and workflow assessment (e.g., inconsistent folder names, poor search)

b. **Support governance and compliance goals:**

- Reinforce the need for metadata, structure, and tagging to enable version control, audit trails, and access controls
- Reference legal and regulatory obligations (e.g., retention, classification, security) that require content to be well-structured
- Highlight the role of consistent vocabularies and taxonomies in enabling lifecycle governance

c. **Ensure readiness for downstream DCM Tool implementation:**

- Clarify that the architecture being designed will serve as a blueprint for metadata tagging, content migration, and workflow configuration
- Emphasize that this is a design activity, not a system configuration step
- Ensure business owners understand their involvement now will shape how content appears and functions later

ii. **Define content scope and coverage boundaries:** Determine what types of content and which platforms will be governed by this architecture.

a. **Identify the types of content to be included:**

- Include all unstructured and semi-structured content types managed by the Entity:
 - Policies
 - Reports
 - Images
 - Web pages
 - Videos
 - Records

4.4.A
Cont.
(2/2)

- Focus on content that will be migrated into, or actively managed by the future DCM Tool
- Exclude highly technical system files or databases unless directly tied to content delivery

b. Define the systems and repositories in scope:

- Include systems already captured in the inventory assessment (4.1), such as DMS, CMS, ECM, shared drives, and archives
- Ensure platforms like intranet portals or external web content managers are included if they host official content
- Exclude platforms unrelated to document or content storage (e.g., ERP, CRM) unless they publish content downstream

c. Set boundaries for what will be designed in this cycle:

- Focus on core architectural elements: controlled vocabularies, taxonomies, navigation structures, and user flows
- Defer more technical specifications to future configuration in Section 5.1
- Set expectations that refinements can be made during or after the DCM Tool implementation once feedback is gathered

4.4.B
(1/2)

Design Controlled Vocabularies and Taxonomies: The Metadata Specialist, with support from the Data Steward and Data Architect, defines and documents the core semantic structures that will be used to classify and label documents and content across platforms. These structures are foundational to consistent metadata tagging, improved search, and lifecycle governance.

i. Define controlled vocabularies: Create a centralized set of approved terms that ensure consistency in how content is labeled and retrieved.**a. Develop authoritative term lists for key fields:**

- Create drop-down lists for document types (e.g., Policy, Guideline, Report, Contract)
- Define standard options for sensitivity classification (e.g., Restricted, Internal, Public)
- Standardize lifecycle stages (e.g., Draft, In Review, Approved, Archived)

b. Resolve terminology inconsistencies:

- Identify synonyms, abbreviations, or department-specific language used inconsistently across systems (e.g., “Procedure” vs. “SOP”)

A

4.4.B
(2/2)

- Define “preferred terms” and map variants to them using a synonym ring or authority list
- Work with departments to approve a harmonized vocabulary that reflects shared meaning

c. **Align vocabularies with enterprise and national standards:**

- Cross-reference terms with those in the Entity’s business glossary
- Reuse terminology from existing reference data sets (e.g., sector names, content categories, legal classifications)
- Document vocabulary definitions, owners, and update frequency

ii. **Design content taxonomies and ontologies:** Structure content in a way that supports classification, browsing, and semantic relationships across systems.

a. **Build hierarchical taxonomies to group content logically:**

- Define parent-child structures for major document groups (e.g., “Finance” > “Budget Reports” > “Q1 Reports”)
- Group content by business function, topic, format, or content lifecycle
- Avoid overly granular levels — aim for intuitive, navigable structures

b. **Define simple ontologies to capture semantic relationships:**

- Map connections between content types (e.g., “Policy informs Procedure”, “Report summarizes Performance Data”)
- Identify workflows where multiple content types are related (e.g., form → submission → approval → publication)
- Use these relationships to support future metadata linking or contextual navigation in the DCM Tool

c. **Prepare classification guides for end users:**

- Document how taxonomies and vocabularies will be applied when tagging or uploading content
- Provide examples of correct term usage for different content types
- Create visual maps or trees to show the overall structure for stakeholder review

4.4.C
(1/2)

A

Develop Metadata and Navigation Structures: The Data Architect and Metadata Specialist jointly design the navigation structures that will be used to describe, organize, and access documents and content across platforms. These structures ensure consistency, enhance search and usability, and support lifecycle and compliance needs.

i. **Define metadata maps:** Develop the set of metadata attributes that will be used to tag and manage content consistently across systems.

a. **Identify required metadata attributes for all content types:**

➤ Define core fields such as:

- Title
- Owner
- Department
- Creation Date
- Document Type
- Sensitivity Classification
- Format
- Status
- Retention Period

➤ Include workflow-related fields such as:

- Version Number
- Approval Status,
- Review Date

➤ Use standardized terms from the vocabularies and taxonomies defined in 4.4.B

b. **Distinguish between required and optional metadata fields:**

- Mark fields like Title, Document Type, and Sensitivity Classification as mandatory
- Identify optional fields that enhance governance (e.g., Keywords, Linked Policies, Reference Number)
- Document rules for field completion (e.g., “Must be filled before publishing” or “Auto-filled from dropdown”)

c. **Create metadata configuration guides:**

➤ For each metadata field, define:

- Field name and description
- Allowed values or format (e.g., text, date, dropdown list)
- Field type (Required, Optional, Conditional)

4.4.C
Cont.
(2/2)

- ii. **Design navigation maps:** Define how users will browse or filter content within the DCM Tool or other systems using folders, menus, and metadata-based logic.

a. **Develop logical folder and access structures:**

- Propose folder structures grouped by business function (e.g., HR > Policies, Legal > Contracts)
- Create separate areas for published content, drafts, and archived material
- Ensure folder names are consistent with taxonomy and vocabulary terms

b. **Enable faceted navigation based on metadata:**

- Design metadata-based filtering options (e.g., by Department, Format, Sensitivity Classification, Year)
- Group filters logically to support intuitive use (e.g., “Filter by Status” alongside “Filter by Owner”)
- Map metadata fields to UI elements (e.g., dropdowns, filters, tags) for search and browsing

c. **Create user-friendly navigation guides:**

- Draft visual representations (site maps, folder trees) of how content will be organized and accessed
- Label major content “hubs” or categories that will serve as entry points for users
- Share draft navigation guides with departments for usability feedback in 4.4.E

4.4.D
(1/2)

Map User Interaction Flows: The Data Architect, with input from data stewards and business users, defines how staff and external users interact with documents and content during their lifecycle. These interaction flows guide how the future DCM Tool will be configured to support common tasks like uploading, reviewing, approving, and publishing.

- i. **Define content lifecycle user journeys:** Document the key user interactions from document creation to archival, covering various roles and actions.

a. **Identify typical user scenarios:**

- Draft and finalize a document
- Review and approve a document
- Search for and retrieve historical records
- Publish content to the intranet or public-facing portal
- Archive or dispose of obsolete content

b. **Identify typical user scenarios:**

- Associate tasks with defined roles (e.g., Author, Reviewer, Approver, Publisher, Records Manager)

A

- Associate tasks with defined roles (e.g., Author, Reviewer, Approver, Publisher, Records Manager)
- Indicate how different roles interact with metadata fields (e.g., who applies “Approved” status or tags retention period)
- Use swimlane diagrams or annotated tables to show who does what and when

c. Define touchpoints and actions for each role:

- For each role, define what they see, click, or complete (e.g., “Submit document for approval”, “Select classification tag”, “Publish to portal”)
- Identify the metadata they are responsible for completing or verifying
- Document pain points (e.g., unclear folders, version confusion, too many review loops) to improve in future DCM Tool design

ii. Prepare system-ready interaction logic: Translate user flows into technical expectations that can guide configuration in the DCM Tool during implementation.

a. Capture metadata-dependent actions:

- Define triggers based on metadata (e.g., “If Status = Approved, send to Publisher”)
- Note which fields are system-populated (e.g., Modified Date) vs. user-filled (e.g., Keywords)
- Identify where validation rules are needed (e.g., Sensitivity Classification cannot be blank)

b. Define notifications and approvals:

- List points in the flow where automatic notifications should occur (e.g., “Reviewer notified when draft is submitted”)
- Specify approval routing (e.g., “Legal must approve before Publishing”)
- Document escalation rules or reminders for tasks not completed on time

c. Store and catalog interaction flows for implementation:

- Save all user interaction flow diagrams or documents in a shared planning folder
- Tag each file with the content type or department it supports
- Link each interaction flow to the relevant workflows defined in 4.3 and content types prioritized in 4.2

4.4.E
(1/2)

A

Review and Finalize the Information Architecture: The Data Governance Specialist facilitates a structured review of the designed information architecture components with relevant stakeholders. The goal is to ensure alignment with business needs, governance expectations, and technical feasibility — and to formally package the architecture as an approved input for DCM Tool implementation.

- i. **Conduct stakeholder review:** Engage key stakeholders to validate that the architecture meets usability, governance, and system-readiness expectations.

- a. **Identify and invite the right reviewers:**

- Include Department Heads or key business users for content usability and classification validation
- Include IT and Metadata Specialists for metadata compatibility and system constraints
- Include Legal and Compliance Officers for review of sensitivity classification, and lifecycle tags
- Include the Records Management and Risk teams to validate archival and retention elements

- b. **Share architecture deliverables in advance:**

- Distribute a review pack including:
 - Controlled vocabularies
 - Taxonomy and metadata
 - Navigation structure diagrams
 - User interaction flow maps
- Include a comments tracker to gather structured input

- c. **Facilitate structured review sessions:**

- Host virtual or in-person walkthrough sessions to review key components
- Capture concerns, suggestions, or clarification requests
- Mark each component as “Approved,” “Needs Revision,” or “Escalation Required”

- ii. **Finalize and document the approved architecture:** Incorporate feedback, resolve remaining gaps, and formally close the design activity.

- a. **Apply final updates to architecture components:**

- Revise vocabularies, taxonomy labels, or folder structures based on stakeholder input
- Clarify metadata fields or approval routing points in user interaction flows
- Align terminology, formatting, and structure across all diagrams and documents

- b. **Compile the architecture into a version-controlled package:**

- Save all finalized artifacts into a structured and labeled digital folder

4.4.E
(2/2)

- Apply appropriate metadata tags to the final files (e.g., department, review date, lifecycle = Approved)

c. Archive and prepare for handoff to implementation team:

- Store the approved package in the Entity's document repository under formal version control
- Submit a copy to the implementation team for use in Section 5.1 (Tool Configuration and Planning)
- Schedule a revisit cycle (e.g., every 12–18 months or post-DCM Tool go-live) for maintenance and updates

RACI Matrix – Information Architecture

Indicative

Sr No.	Activity	Data Management and Security Director	Data Architecture and Analytics Section Head	Data Management and Governance Section Head	Data Governance Specialist	Metadata Specialist	Data Architect	Data Owners	Data Stewards
4.4.A	Define Information Architecture Objectives and Scope	A		R	C	C	C		C
4.4.B	Design Controlled Vocabularies and Taxonomies			A		R	R	C	R
4.4.C	Develop Metadata and Navigation Structures			A		R	R	C	C
4.4.D	Map User Interaction Flows		A				R		R
4.4.E	Review and Finalize the Information Architecture			A	R	C	C		C

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

Based on this Activity, the Entity can



Initiate the Inventory Assessment Process



Finalize and Approve Inventory Assessment Report

5. Document & Content Management Implementation



5. Document & Content Management Implementation

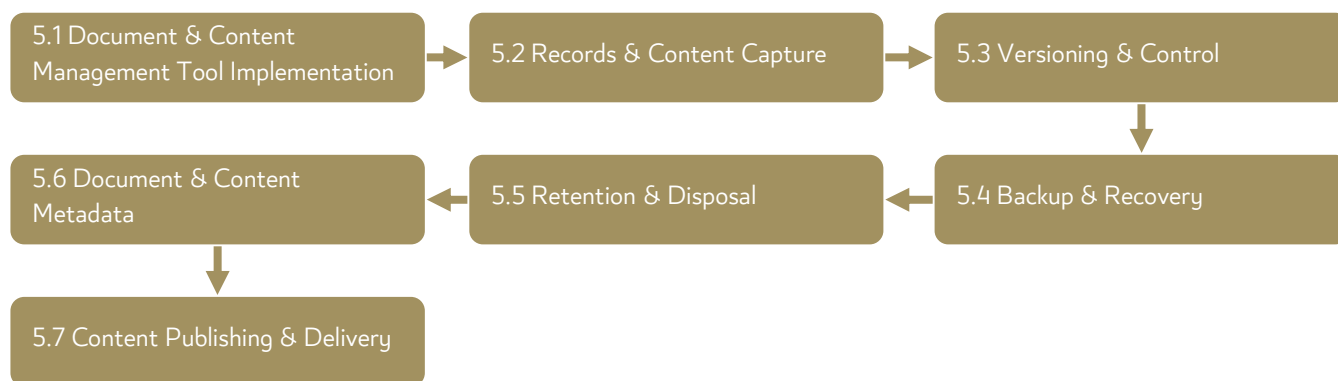
What is Document & Content Management Implementation and why does the Entity need it?

The Document & Content Management Implementation process enables the Entity to operationalize its policy and design work by configuring the document and content management tool, capturing content effectively, enforcing governance, and preparing for long-term automation. This process builds directly on the outputs of the assessment and design phase and translates them into practical, system-driven outcomes.

Through structured implementation activities, the Entity ensures that documents and content are stored securely, tagged consistently, versioned reliably, retained appropriately, and published through the correct channels. Metadata, workflows, access rules, and retention schedules are embedded into the system to support day-to-day operations, audit readiness, and compliance with national standards.

Implementation activities include tool selection and configuration, content capture, versioning, backup, retention enforcement, metadata tagging, and publishing setup. Each activity is designed to improve control, increase transparency, and streamline access to content across departments and user groups.

The remaining sections of this chapter will detail the activities that guide the Entity through executing the Document & Content Management Implementation process.



Guiding Principles for Document & Content Management Implementation

1. **Build on What's Designed:** Use the structures, metadata, workflows, and content priorities defined in the assessment phase as the direct inputs to tool configuration and implementation.
2. **Automate Where It Matters:** Focus automation on high-impact workflows and lifecycle events such as approvals, versioning, retention, and publishing — avoid overcomplicating low-risk areas.
3. **Protect What's Critical:** Prioritize the capture, backup, and retention of documents classified as critical to compliance, service continuity, or strategic value.
4. **Tag with Purpose:** Ensure metadata tagging is not a checkbox exercise — it should actively drive classification, searchability, retention, access control, and reporting.

5.1.A
(1/2)

A

Define Tool Implementation Objectives and Governance: The Data Management and Governance Section Head, in collaboration with the IT Team, defines the purpose, outcomes, and governance structure for the DCM Tool implementation.

- i. **Set clear implementation objectives:** Clarify what the Entity expects to achieve from DCM Tool implementation and how it supports governance.
 - a. **Define core DCM Tool goals:**
 - Enable structured storage, access, and retrieval of content
 - Enforce version control, metadata tagging, retention, and access permissions
 - Support document lifecycle governance, collaboration, and workflow execution
 - b. **Align DCM Tool with organizational priorities:**
 - Link the tool to digital transformation, operational efficiency, and service delivery goals
 - Address gaps identified in the inventory and prioritization assessments
 - Reinforce its importance in supporting compliance, transparency, and audit readiness
 - c. **Use previous outputs to define scope:**
 - Base DCM Tool design decisions on outcomes from Sections 4.1–4.4
 - Align implementation with the structured content, workflows, and architecture already developed
 - Ensure all departments understand the role of their input in shaping system capabilities
- ii. **Establish implementation roles and oversight:** Define accountability and coordination structures to guide selection, configuration, and rollout.
 - a. **Assign executive and technical leadership:**
 - Designate the Data Management and Governance Section Head as business owner
 - Assign the IT Team as the implementation owner
 - Designate the Data Governance Specialist as the project manager
 - b. **Form a cross-functional implementation team:**
 - Include key roles: Metadata Specialist, Data Architect, and department focal points
 - Define role-specific responsibilities for tool review, metadata mapping, workflow configuration, and testing
 - Establish a dedicated communication channel and shared workspace

5.1.A
(1/2)

c. Define governance and decision protocols:

- Set a meeting cadence (e.g., weekly or biweekly working sessions)
- Establish a decision log to track critical approvals and issues
- Involve executive sponsors (e.g., Director) in escalation and milestone reviews

A

5.1.B

Define Functional and Technical Requirements: The IT Team and Metadata Specialist, with support from the Data Architect and Data Governance Specialist, define the core features, integration needs, and compliance controls required in the DCM Tool based on the national data standards and the Entity's internal needs.

A

VA

i. Define functional requirements: Identify the capabilities needed to support content lifecycle management across departments.

a. List advanced features aligned to the national data standards:

- Document versioning, including histories of changes
- Secured document access
- Global search and discovery on the registered documents
- Collaboration capabilities

b. List very advanced features aligned to the national data standards:

- OCR (Optical Character Recognition) functionality to analyze imported images
- Document indexing
- Documents workflows development
- Workflow automation
- Web Content Management System (WCMS): an application designed for storing and managing web content utilized by the Entity's portals and internet sites

ii. Define technical and integration requirements: Ensure the DCM Tool can function within the Entity's existing IT environment and support future growth.

a. Identify system compatibility requirements:

- Ensure browser compatibility, mobile responsiveness, and accessibility compliance
- Confirm language support (e.g., Arabic, English)
- Define storage expectations (e.g., cloud-based, on-premises, or hybrid options)

b. Define integration needs with existing platforms:

- Connectivity with identity management systems (e.g., Active Directory)
- Publishing/export options to intranet portals or public websites

5.1.C
(1/2)

A

Shortlist and Evaluate Tool Options: The Data Governance Specialist, in coordination with the IT Team, leads the evaluation of DCM Tool options using the DCM Tool Selection Criteria Template.

- i. **Prepare the evaluation framework:** Use a structured and objective approach to compare tools based on feature availability, advancement level, and pricing.
 - a. **Use the provided Tool Selection Criteria Template:**
 - Complete the table fields: Tool Feature, Weight, Advancement Level, and Tool 1–X comparison
 - Understand scoring for functionality (1–4) and pricing (1–4)
 - Assign weights to features based on their importance to the Entity
 - b. **Include all nationally required features:**
 - **Advanced features:** Version control, secured access, global search, collaboration
 - **Very Advanced features:** OCR, indexing, workflow automation, WCMS integration
 - Ensure features align with national Document & Content Management standards
 - c. **Weight and rank features logically:**
 - Assign higher weights to advanced features and must-haves (e.g., versioning, secured access)
 - Apply moderate weights to very advanced features that support long-term scalability
- ii. **Shortlist eligible tools:** Narrow the candidate pool to tools that meet the requirements outlined in the National Data Standards.
 - a. **Conduct a pre-screening of available solutions:**
 - Review documentation, demos, or vendor responses to confirm features
 - Eliminate tools lacking key functionality or integration readiness
 - Select 3–5 tools for formal scoring
 - b. **Assign evaluation roles:**
 - IT assesses infrastructure, security, and integration
 - Business teams assess usability, and workflows
 - Governance teams assess lifecycle, retention, and classification controls
 - c. **Set up a shared workspace for tool comparison:**
 - Centralize brochures, vendor responses, and completed scoring templates
 - Apply naming conventions (e.g., “Tool_Evaluation_DCM_v1”)

5.1.C
Cont.
(2/2)

iii. **Score and compare tools using the template:** Evaluate tools and generate weighted scores to support a data-driven selection.

a. **Complete the Tool Selection Criteria Template:**

- Populate features in alignment with the standards as well as additional features
- Apply pricing and feature scores based on the criteria
- Use built-in formulas to generate weighted total scores

b. **Review scores with stakeholders:**

- Discuss results in a working session
- Highlight tools that exceed minimum standards and score highly on key features
- Document any open questions or items requiring vendor follow-up

c. **Identify top 2–3 tools for final review and demonstrations:**

- Select highest-scoring tools for vendor demos or sandbox testing
- Prepare a summary of shortlisted tools with scoring results for presentation in Step 5.1.D

Asset Guidance

The **DCM Tool Selection Criteria Template** helps the Entity document mandatory and additional DCM tool features, list various tool options, specify feature and cost weightings based on importance, and guide the Entity through the decision-making process.

Illustrative

Document and Content Management Tool Selection Criteria Template						
The following tables provides a structured template to guide the evaluation and selection of a document and content management tool						
Field	Description					
Tool feature	The specific tool feature required based on the domain's standards (e.g., version control).					
Tool feature weight	The weighted percentage assigned to the tool feature based on importance to the respective entity.					
Feature level of Advancement [Tool name 1,2,3,X]	The level of advancement of the feature as per the standards (Foundational, Advanced, or Very Advanced). Whether the suggested tool has the feature described (Yes/No).					
Features Scoring	Description					
1 - Low	Limited functionality, insufficient to meet key requirements					
2 - Medium	Basic functionality, meets most requirements but with some limitations					
3 - High	Strong functionality, meets all requirements effectively with minor gaps					
4 - Very High	Comprehensive functionality, meets all requirements with advanced features and flexibility					
Pricing Scoring	Description					
1 - Low	High cost solution					
2 - Medium	Moderate cost solution					
3 - High	Budget friendly solution					
4 - Very High	Low cost solution					
Tool Feature	Tool Feature Weight	Feature level of Advancement	[Tool name 1]	[Tool name 2]	[Tool name 3]	[Tool name X]
Cost	20%	Advanced	4			
Document Versioning	10%	Advanced	4			
Secured Document Access	10%	Advanced	2			
Global Search and Discovery	10%	Advanced	2			
Collaboration Capabilities	10%	Advanced	3			
OCR	8%	Very Advanced	3			
Document Indexing	8%	Very Advanced	4			
Workflow Development	8%	Very Advanced	2			
Workflow Automation	8%	Very Advanced	4			
WCMS	8%	Very Advanced	4			
Total:			82%	0%	0%	0%

Select and Approve the Tool: The Data Management and Governance Section Head, in consultation with the IT Team, leads the final evaluation and selection of the preferred Document & Content Management Tool. The goal is to ensure that the chosen tool is not only feature-compliant and cost-effective, but also aligned with business needs, future scalability, and the national data standards.

- i. **Conduct detailed evaluation of shortlisted tools:** Review the top-scoring tools from 5.1.C using live demos, sandbox environments, and stakeholder feedback.

a. **Organize vendor demonstrations:**

- Invite shortlisted vendors to demonstrate their platform's core capabilities
- Request that vendors show how the tool supports version control, metadata tagging, search, retention, and workflow features
- Encourage participants to ask questions and test common use cases (e.g., uploading and tagging a file, starting an approval workflow)

b. **Facilitate hands-on testing or sandbox reviews:**

- Provide internal staff (IT, business users, metadata owners) with limited access to test environment if available
- Use predefined evaluation scenarios (e.g., "Can the tool classify a document with three metadata tags and submit it for approval?")
- Collect user feedback on usability, interface clarity, speed, and responsiveness

c. **Capture and compare feedback across stakeholder groups:**

- Use a simple feedback form or scoring sheet for all demo attendees
- Document any critical gaps or risks identified during testing
- Update the Tool Selection Summary with user preferences, risks, and final impressions

- ii. **Finalize tool selection decision:** Consolidate findings and prepare a formal recommendation for leadership approval.

a. **Consolidate all evaluation artifacts:**

- Combine final scoring results, demo feedback, pricing comparisons, and technical evaluations
- Prepare a Tool Recommendation Report with the following sections:
 - Overview of shortlisted tools
 - Evaluation criteria and scoring results
 - Strengths and weaknesses of each tool
 - Recommended tool and rationale
 - Estimated cost and licensing model
 - Key implementation considerations

5.1.D
Cont.
(2/2)**b. Present recommendation to executive stakeholders:**

- Share the Tool Recommendation Report with the Data Management & Security Director
- Host a review session (if needed) to present findings and answer questions
- Use this session to formally request approval of the selected tool

c. Secure documented approval:

- Obtain written or email approval from the designated authority (e.g., Executive Sponsor or Steering Committee)
- Record the decision and approval date in a decision log or project file
- Inform all vendors and internal stakeholders of the selected tool and next steps

5.1.E
(1/2)

Develop Tool Implementation Plan and Roadmap: The Data Governance Specialist, in coordination with the Data Management and Governance Section Head and IT Team, develops a detailed plan and timeline for implementing the selected Document & Content Management Tool. This includes defining phases, resources, risks, and dependencies to ensure the project is achievable, aligned to strategic needs, and prepared for structured execution.

i. Define implementation phases and activities: Break down the implementation into clear, manageable phases aligned with business priorities and technical readiness.**a. Structure the implementation across key phases:**

- **Phase 1:** Configuration of advanced features (e.g., metadata fields, access controls, folder structures)
- **Phase 2:** Migration of prioritized content and onboarding of core departments
- **Phase 3:** Workflow setup and automation for approved use cases
- **Phase 4:** configuration of remaining features, followed by Entity-wide rollout

b. Map each activity to a defined time window:

- Create a timeline or Gantt chart with key tasks, durations, and milestones
- Link configuration, migration, testing, training, and go-live events to specific dates or quarters
- Allocate time for feedback, adjustments, and post-launch stabilization

c. Align each phase with previous QDKC outputs:

- Use the developed information architecture from 4.4 to drive Phase 1 configuration
- Use prioritized documents from 4.2 for Phase 2 migration
- Use workflow designs from 4.3 for Phase 3 automation setup

A

5.1.E
Cont.
(2/2)

- ii. **Assign roles, responsibilities, and resource requirements:** Ensure the implementation team is staffed, supported, and empowered to deliver the plan.

a. **Confirm project team structure and responsibilities:**

- Assign the data governance specialist to lead day-to-day coordination
- Ensure the Metadata Specialist, and Data Architect are available for their respective configuration tracks
- Include departmental representatives to validate configuration and test migrated content

b. **Define system administration and vendor coordination roles:**

- Assign a Technical Lead to oversee system installation, performance, and upgrades
- Identify a primary contact for vendor communication (e.g., licensing, support, escalations)
- Define who will manage user roles, permissions, and change requests post go-live

c. **Estimate required resources and effort:**

- Identify internal hours required per role per phase
- Define any external support needs (e.g., vendor-led configuration, migration scripting)
- Secure an implementation budget (if not already included in procurement approval)

- iii. **Identify risks, dependencies, and success metrics:** Anticipate roadblocks, ensure dependencies are addressed, and define how success will be measured.

a. **Document key risks and mitigation actions:**

- **Risk:** Poor department adoption → Mitigation: Early engagement and targeted training sessions
- **Risk:** Integration delays with WCMS → Mitigation: Pilot with limited modules first

b. **Track external and internal dependencies:**

- Ensure departments can allocate reviewers and testers in time for validation phases
- Align go-live with periods of low operational risk (e.g., avoid fiscal year-end, audit cycles)

c. **Define success indicators for each phase:**

- **Phase 1:** Metadata fields functional, folders configured, security applied
- **Phase 2:** 100% of prioritized documents migrated successfully
- **Phase 3:** Workflows tested and used by target users
- **Phase 4:** Users trained, WCMS integration complete, and adoption rates >80% in core departments

5.1.F
(1/2)

A

VA

Configure the Tool Using Designed Structures: The IT Team, in close coordination with the Metadata Specialist, and Data Architect, configures the Document & Content Management Tool based on the Entity's approved information architecture, and prioritized content and workflows. This configuration ensures the system aligns with the national data standards and supports governance, usability, and automation.

- i. **Configure metadata fields and tagging logic:** Set up the metadata fields in alignment with the outputs of Section 4.4 to support consistent classification, governance, and search.
 - a. **Create all required metadata fields in the system:**
 - Add core fields (e.g., Title, Document Type, Sensitivity Classification, Department, Status, Retention Period, Criticality Level)
 - Configure field types (e.g., dropdowns, date pickers, free text) and set mandatory fields
 - b. **Implement metadata validation and dependencies:**
 - Configure rules (e.g., "Retention Period" is required if "Legal Requirement = Yes")
 - Set field-level validation (e.g., no special characters in Title, predefined formats for Document ID)
 - Ensure system supports dynamic metadata updates based on user role or document status
 - c. **Enable metadata-based filtering and search:**
 - Map metadata fields to filters in the search UI (e.g., "Filter by Department", "Filter by Year")
 - Ensure metadata fields are indexed and searchable
 - Test sample queries using metadata filters to ensure discoverability
- ii. **Set up folder structures and navigation views:** Build the digital navigation structure based on the information architecture developed in 4.4.
 - a. **Configure folder hierarchies by business domain:**
 - Create folders grouped by department or content type (e.g., "HR > Policies", "Legal > Contracts")
 - Separate folders by document lifecycle where needed (e.g., "Drafts", "Approved", "Archived")
 - Apply permissions at folder level to restrict access based on sensitivity or business role
 - b. **Enable faceted navigation using metadata:**
 - Configure dynamic navigation panels based on metadata (e.g., "Browse by Format", "Browse by Year")
 - Link content hubs to specific workflows or publishing actions (e.g., "Submit for Approval")
 - Test that navigation paths are intuitive and match the folder trees defined in 4.4.C

5.1.F
Cont.
(2/2)**c. Establish default views for users:**

- Define department-specific landing pages or dashboards
- Pre-configure views for “My Documents”, “Pending Approvals”, or “Recently Modified”
- Ensure role-based customization is enabled (e.g., publisher vs. contributor view)

iii. Configure workflows and access controls: Implement document-related workflows and access models based on approved designs from 4.3 and 4.4.**a. Set up automated workflows for top-priority processes:**

- Use the finalized workflow models from 4.3.D and 4.3.E
- Configure sequential or parallel approval steps, automated routing, escalation rules, and task assignments
- Map each workflow to a document type or trigger condition

b. Define roles, permissions, and document-level access controls:

- Assign user roles (e.g., Viewer, Contributor, Reviewer, Publisher) based on department and job function
- Apply access controls based on metadata (e.g., “Confidential” = restricted to management roles)
- Enable document check-in/check-out, audit history, and edit logs

c. Establish access request and approval workflows

- Implement a structured access request process where users submit requests specifying desired role, justification, and content scope
- Route requests to the appropriate Content Owner, Department Focal Point, or Tool Administrator for approval
- Log all approvals in an Access Control Register, capturing timestamp, approving authority, and access duration (if temporary)
- Schedule periodic access reviews with department heads to validate that permissions are current and appropriate
- Revoke or adjust access when users change roles, projects, or leave the Entity
- Ensure audit logs capture all changes to access rights for compliance reporting

5.1.G
(1/3)

Test and Validate Tool Functionality: The IT Team, in collaboration with the Data Governance Specialist, Metadata Specialist, and departmental testers, conducts structured testing of the configured Document & Content Management Tool.

i. Develop test scenarios and acceptance criteria: Define test cases that reflect real business scenarios and verify that system features meet configuration and governance requirements.**a. Create role-based test scripts:**

- Develop step-by-step test cases for each user role (e.g., Contributor, Reviewer, Approver, Publisher)

A

- Include core activities: uploading content, tagging metadata, routing for approval, changing document status, performing search
- Use content examples from the prioritized documents list (4.2) to ensure realism

b. Define clear acceptance criteria per feature:

- **Example:** “Document must not be published unless ‘Approved’ status is applied”
- **Example:** “Only users with Reviewer role can edit metadata fields marked as restricted”
- Document expected results, actual results, and test status (Pass/Fail) in a Test Results Log

c. Prepare test environment with realistic data:

- Populate the system with test content tagged using real metadata from 4.4
- Ensure access roles and workflows mirror the final configuration
- Label test files clearly (e.g., “TEST - Legal Review Workflow”) to avoid confusion with real content

ii. Conduct end-to-end testing with stakeholders: Execute tests with functional users to confirm that configurations meet expectations.

a. Coordinate user testing across departments:

- Select 1–2 testers per key department to run through their assigned workflows
- Host a kick-off briefing to explain testing goals, scripts, and support channels
- Set a clear testing window (e.g., 5 business days) with daily check-ins for blockers

b. Track and document testing outcomes:

- Use a shared test log or issue tracker to capture defects, and usability concerns
- Classify findings as critical, major, minor, or cosmetic
- Record screenshots or error messages where applicable

c. Analyze test results and prioritize fixes:

- Review failed test cases and validate whether the issue is in configuration or user error
- Assign fixes to the responsible team member and retest once resolved
- Confirm all critical and major issues are resolved before go-live

ii. Validate compliance and audit readiness: Ensure that system features support audit trails, access logs, and governance requirements.

a. Confirm versioning and history tracking:

- Upload a test document, make changes, and verify that all versions are tracked
- Check that users can view, compare, and restore previous versions

b. Review access control behavior:

- Attempt to access restricted documents using different roles

5.1.G
Cont.
(3/3)

- Verify that permission levels match configurations and unauthorized access is blocked
- Confirm that access logs are generated and traceable

c. **Validate retention and lifecycle settings:**

- Apply retention metadata and simulate lifecycle actions (e.g., review alerts, archival triggers)
- Confirm that system-generated actions follow configured timelines and logic
- Check that disposal workflows are secure, auditable, and permission-restricted

5.1.H
(1/3)

Train Users and Prepare for Launch: The data governance specialist, with support from the IT Team, and department focal points, plans and delivers a comprehensive training and readiness program to ensure users understand how to navigate, use, and govern content within the new Document & Content Management Tool.

i. **Develop the training plan and materials:** Create tailored training sessions, guides, and support resources for each user group based on their role in the DCM Tool.

a. **Segment training by user role and function:**

- Define user groups: Viewers, Contributors, Reviewers, Approvers, Publishers, and Admins
- Tailor each session to the actions relevant to that role (e.g., contributors learn metadata tagging; approvers focus on review workflows)
- Include general sessions for awareness and governance (e.g., importance of classification, version control, retention)

b. **Prepare training materials and user guides:**

- Develop role-specific quick reference guides and walkthroughs
- Record demo videos showing common actions like uploading, tagging, submitting, and publishing
- Include FAQs and a glossary of the DCM Tool. terms (e.g., “Check-in”, “Disposition”, “Version History”)

c. **Plan training delivery and tracking:**

- Schedule live sessions (in-person or virtual) and assign participants by department or role
- Provide a sandbox environment for hands-on learning during or after sessions
- Track attendance and completion using a training register, and follow up with non-attendees

A

5.1.H
Cont.
(2/3)

- ii. **Communicate launch readiness to departments:** Coordinate internal communications to prepare departments for the transition and clarify expectations.
- a. **Develop a DCM Tool readiness announcement plan:**
 - Create clear, friendly messages that explain what's changing, why it matters, and when it takes effect
 - Use multiple channels: email, intranet, department briefings, posters, or newsletters
 - Brand the launch with a name or tagline (e.g., "SmartDocs is Live – Organize. Tag. Track.")
 - b. **Share support contact points and escalation paths:**
 - Publish the names and emails of the support team and key contacts for each department
 - Set up a shared mailbox or helpdesk channel for triage and user support
 - Document and communicate how users can escalate urgent issues or tool access requests
 - c. **Provide readiness checklists for departments:**
 - Share a simple checklist for each department to confirm readiness (e.g., "Metadata tags verified," "Key staff trained," "Workflow models reviewed")
 - Ask each department to assign a DCM Tool launch contact to coordinate last-mile questions or feedback
 - Set a deadline for checklist submission to confirm go-live readiness

 Asset Guidance

The **Change Management Communication Plan Email Template** is a sample email template the Entity can leverage to announce the new document and content management tool. *Illustrative*

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]

5.1.H
Cont.
(3/3)

- iii. **Finalize launch logistics and change management:** Prepare support plans, stabilization activities, and post-launch monitoring to ensure a smooth transition.

a. **Establish a hypercare support period:**

- Define a 2–4 week “hypercare” window after go-live for prioritized support
- Assign a daily or weekly point-of-contact for triaging issues
- Monitor usage and user-reported problems to identify trends

b. **Confirm access provisioning and onboarding:**

- Ensure all users have system accounts, roles assigned, and test login credentials
- Create a simple onboarding guide for new users post-launch
- Validate that role-based permissions match pre-launch configuration

c. **Document post-launch feedback mechanisms:**

- Set up a form or shared spreadsheet to collect improvement suggestions and usability concerns
- Schedule a feedback review session after 1 month to prioritize configuration adjustments
- Create a lessons-learned log to guide future enhancements or onboarding phases

5.1.I
(1/2)

Go-Live and Post-Implementation Support Planning: The Data Governance Specialist, with support from the IT Team, and designated department focal points, oversees the go-live process and sets up sustainable post-launch support to ensure system stability, adoption, and continuous improvement.

- i. **Execute go-live in a controlled and coordinated manner:** Launch the tool in a phased, well-supported manner to minimize disruption and ensure user success.

a. **Launch in phases or waves (if needed):**

- Go live with high-priority departments and workflows first, then expand in waves
- Confirm readiness for each wave using department checklists and user feedback
- Provide pre-launch reminders and reissue key training resources before each wave

b. **Communicate go-live details to all users:**

- Share the go-live announcement with links to user guides, contact info, and timelines
- Highlight what actions are expected from users on Day 1 (e.g., log in, tag a document, approve a test record)
- Reinforce support contacts and escalation process for any immediate issues

c. **Monitor system and user activity from Day 1:**

- Track login success, task completion, workflow routing, and content access patterns
- Use system audit logs and admin dashboards to monitor real-time usage
- Assign IT and Governance resources to provide hands-on support during first-week “hypercare”

A

5.1.I
(2/2)

- ii. **Establish a post-launch support model:** Transition from project mode to operational governance and support.
 - a. **Assign permanent support roles and responsibilities:**
 - Designate a Document and Content Management Tool Administrator for ongoing configuration changes, user management, and upgrades
 - Assign the Metadata Specialist to maintain taxonomies, vocabularies, and classification rules
 - Define who reviews and approves workflow or permission change requests
 - b. **Set up a content governance process:**
 - Schedule quarterly or semi-annual content governance reviews (e.g., ROT analysis, user feedback review)
 - Assign department leads to oversee content hygiene and compliance at the department level
 - c. **Establish maintenance and escalation paths:**
 - Define how system bugs, enhancement requests, or outages are reported and tracked
 - Maintain a configuration change log for auditability
 - Engage the tool vendor or hosting provider for advanced support and SLA compliance
- iii. **Plan for continuous improvement and system sustainability:** Ensure the tool evolves with business needs and continues to deliver value over time.
 - a. **Schedule structured feedback loops**
 - Run user satisfaction surveys at 1 month, 3 months, and 6 months post-launch
 - Use helpdesk ticket trends to identify common issues and training needs
 - Schedule lessons-learned workshops to inform future onboarding or tool phases
 - b. **Integrate the document and content management tool into strategic planning cycles**
 - Align tool improvement actions with Entity-wide digital transformation or service improvement initiatives
 - Budget for system expansion, licensing, and user training in the next fiscal planning cycle

RACI Matrix – Document & Content Management Tool Implementation

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	Metadata Specialist	Data Architect	Data Owners	Data Stewards	IT Team	Department Focal Point
5.1.A	Define Tool Implementation Objectives and Governance	A	R	C		C		C	C	
5.1.B	Define Functional and Technical Requirements		A	C	R	C			R	
5.1.C	Shortlist and Evaluate Tool Options		A	R					R	
5.1.D	Select and Approve the Tool	A	R	I	I	I	I	I	C	
5.1.E	Develop Tool Implementation Plan and Roadmap	I	A/R	R	C	C	C		C	
5.1.F	Configure the Tool Using Designed Structures		A	I	R	C	I		R	
5.1.G	Test and Validate Tool Functionality		A	R	R				R	
5.1.H	Train Users and Prepare for Launch		A	R					R	C
5.1.I	Go-Live and Post-Implementation Support Planning	I	A	R					R	C

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

Based on this Activity, the Entity can



Select and Approve the Tool



Train Users and Launch the Tool

5.2 Records & Content Capture

A standardized records and content capture process ensures that all documents created, uploaded, or migrated across the Entity's platforms are properly classified, usable, and aligned with governance expectations. This activity focuses on embedding metadata at the point of capture, assessing content quality, eliminating redundancies, and ensuring business relevance.

Effective capture is the first step in enforcing lifecycle governance, enabling search, automating workflows, and ensuring that documents serve their intended operational or compliance purposes. Without proper capture, content becomes fragmented, untraceable, or non-actionable.

Process – Records & Content Capture

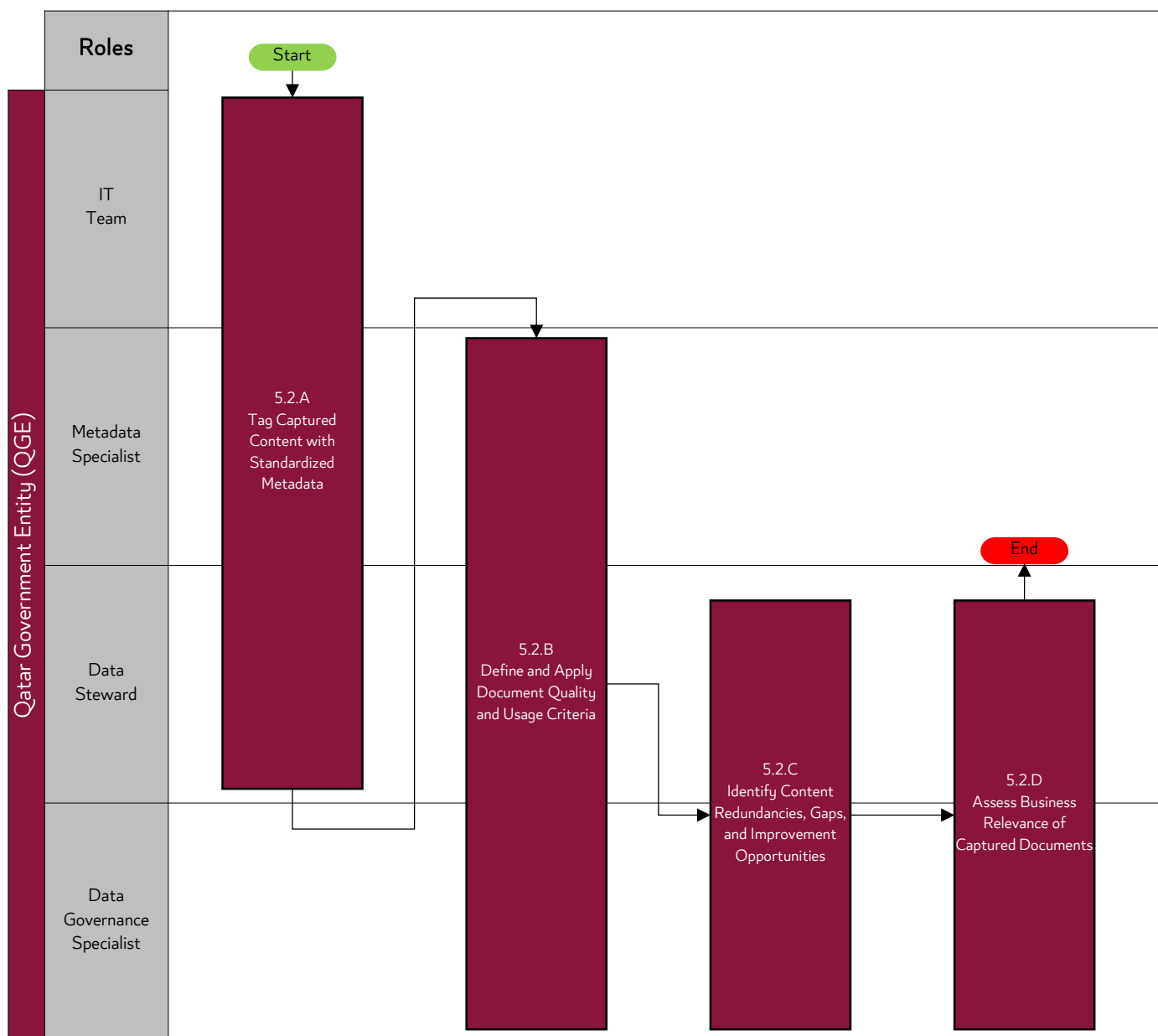


Figure 10 – Records & Content Capture Process Map

Legend: ■ Process Step ◆ Decision ● Process Start ● Process End □ Document ■ Off-Page Reference

5.2.A
(1/2)

A

Tag Captured Content with Standardized Metadata: The Metadata Specialist, in collaboration with the Data Stewards and IT Team, ensures that all captured documents and content are consistently tagged using standardized metadata aligned with the Entity's information architecture. This supports discoverability, classification, access control, and lifecycle governance.

- i. **Apply metadata to newly captured content:** Ensure all documents entering the system are described using predefined metadata attributes.

- a. **Use mandatory metadata fields from Section 4.4:**

- Apply key fields such as Title, Document Type, Department, Owner, Sensitivity Classification, and Retention Period
- Ensure that dropdown values (e.g., Sensitivity Classification = Secret, Internal, Public) follow the controlled vocabularies established in 4.4.B
- Mark required fields as non-optional during content upload or creation

- b. **Automate metadata tagging where possible:**

- Configure default metadata values based on folder or document source (e.g., anything uploaded to "HR > Policies" is auto-tagged as "Document Type = Policy")
- Use system logic to auto-capture metadata like Creator, Created Date, File Format, and File Size
- Implement rules to inherit metadata from parent folders or previously tagged templates

- c. **Support manual tagging for complex content:**

- Provide guided tagging forms for users when uploading documents (e.g., dropdowns, tooltips, required fields)
- Display metadata previews so users can confirm or edit values before final submission
- Log which users entered or edited each metadata field for traceability

- ii. **Tag legacy and backlog documents:** Ensure historical or previously untagged content is retroactively classified for lifecycle governance and retrieval.

- a. **Identify backlog content requiring metadata:**

- Use the results of the inventory assessment (4.1) to identify systems or folders with untagged files
- Prioritize High-priority documents from 4.2 that are stored in shared drives or archives
- Exclude ROT-prone or obsolete content flagged in 4.1.E unless needed for legal or archival reasons

5.2.A
(2/2)**b. Apply metadata in batch or through scripted tools:**

- Use the document and content management tool or migration tools to apply common metadata to files in bulk (e.g., all files in “2022 Reports” = Document Type: Report, Year: 2022)
- Tag files by folder name, file name conventions, or embedded properties where possible
- Maintain an audit log of bulk tagging actions for traceability

c. Assign metadata cleanup tasks to departments:

- Share department-specific tagging assignments for documents identified in their area
- Create a simple status tracker (e.g., Excel sheet) for metadata completion
- Follow up weekly to ensure tagging progress is monitored and finalized

5.2.B
(1/2)

Define and Apply Document Quality and Usage Criteria: The Data Stewards, with support from the Metadata Specialist and Data Governance Specialist, define and apply clear criteria for assessing the quality and usage of captured documents. This ensures that stored content is reliable, relevant, and governed in a manner that supports operational needs and compliance requirements.

A

i. Define document quality criteria: Establish a set of standards that determine whether a document is fit for retention, retrieval, and future automation.

a. Define minimum quality attributes for documents:

- Title is present, accurate, and follows naming conventions
- Document Type is correctly assigned based on vocabulary standards
- Metadata fields (e.g., Sensitivity Classification, Owner, Department) are complete and valid
- File format is standardized and accessible (e.g., PDF, DOCX, not obsolete or system-specific)

b. Define business-level completeness criteria:

- Content is current and final (not draft or duplicate unless appropriately labeled)
- The document includes required approvals, signatures, or legal markers (where applicable)
- Version history is intact or properly tracked via metadata or embedded fields

c. Document the quality checklist for internal use:

- Create a Document Quality Checklist that departments can use to assess and validate documents
- Include visual examples of “Good vs. Poor” quality files for training purposes
- Share the checklist with all departments responsible for bulk uploads or migration

5.2.B
(2/2)

- ii. **Conduct document quality assessments:** Apply the defined criteria to newly captured or existing documents to ensure consistent quality standards.
 - a. **Perform random sampling checks:**
 - Select a representative sample of documents from each department or content type
 - Review them against the Document Quality Checklist
 - Record findings in a Quality Review Log, noting the number of issues per document
 - b. **Engage departments in document validation:**
 - Ask departments to self-review a subset of documents before migration or tagging
 - Provide a lightweight validation form to record quality gaps (e.g., missing metadata, incorrect titles)
 - Schedule spot-check reviews with department focal points for collaborative clean-up
 - c. **Track quality issues and resolution status:**
 - Maintain a log of issues identified (e.g., “20 files in Legal shared drive missing Retention tags”)
 - Assign corrective actions to responsible teams
 - Reassess after corrections are made to confirm quality thresholds are met
- iii. **Assess content usage patterns:** Evaluate how often content is accessed, used, or referenced to inform retention, migration, or prioritization.
 - a. **Use system logs or access reports (where available):**
 - Review metadata such as “Last Accessed,” “Last Modified,” or download counts
 - Tag content with low or no usage for further review in 5.2.C
 - b. **Consult business users on usage value:**
 - Ask content owners: “Is this document still in use?”, “Who uses it and how often?”
 - Mark documents as “Active,” “Archived,” or “Obsolete” based on business input
 - Avoid deleting content unless retention and ownership are confirmed
 - c. **Link usage findings to content governance actions:**
 - Use usage trends to decide whether content should be archived, deleted, or restructured
 - Align findings with the ROT analysis previously flagged in the inventory assessment (4.1.E)

5.2.C
(1/2)

A

Identify Content Redundancies, Gaps, and Improvement Opportunities: The Data Stewards, with support from the Data Governance Specialist, review captured content to identify redundant documents, missing content, and inconsistencies. This helps reduce information clutter, optimize content storage, and ensure that all critical business processes are properly documented and represented in the system.

- i. **Identify redundant or duplicate content:** Detect and flag documents that are repeated, copied across systems, or stored under different names.

- a. **Detect duplicate file names and content patterns:**

- Search for files with identical or near-identical names (e.g., “Final_Report_v2”, “Final_Report_v3”) in the same or multiple systems
- Look for repeated files stored across department folders (e.g., “HR_Policy” in both HR and Legal shared drives)
- Use the document and content management system or a file analysis tools to identify identical file hashes or metadata patterns

- b. **Flag uncontrolled versions or legacy copies:**

- Identify “Draft,” “Backup,” or “Old” copies stored alongside current documents
- Check for uncontrolled versioning — e.g., multiple “Final” versions with no clear owner or archive history
- Mark documents that do not follow version control policies defined during metadata configuration (5.1.F)

- c. **Tag redundant documents for review and action:**

- Add a “Duplicate” or “Review for Deletion” label using metadata or an internal tracker
- Group duplicates by content owner or department for confirmation before removal
- Record recommendations in a cleanup log (e.g., “Keep only v4, delete v1–v3 once confirmed by Finance”)

- ii. **Identify missing or unrepresented content:** Detect critical content types or business areas that are underrepresented or missing from captured records.

- a. **Compare captured content against process and workflow maps:**

- Use the workflows designed in 4.3 to check for missing document types (e.g., “No Case Closure Form found for Legal process”)
- Cross-check document types expected in each department based on 4.2 prioritization
- Review navigation structures (4.4.C) to validate whether all major categories contain content

5.2.C
(2/2)**b. Consult department users to identify gaps:**

- Ask questions like: “Are there key documents that aren’t in the system yet?”
- Identify records still stored in physical form or personal drives that haven’t been uploaded

c. Record missing content and plan for resolution:

- Document all identified gaps in a “Content Gap Log” with department, type, and resolution status
- Schedule follow-ups with departments to locate, digitize, and upload missing documents
- Prioritize gaps tied to compliance, legal, or high-priority workflows

iii. Recommend content cleanup and restructuring actions: Use the insights gathered to improve content structure, usability, and long-term manageability.**a. Propose consolidation of duplicate folders or document sets:**

- Recommend merging folders that hold overlapping content (e.g., “Policy Drafts” and “Policies 2021”)
- Suggest deleting unnecessary backups if clean versions and metadata are available
- Encourage departments to use a shared workspace instead of siloed storage areas

b. Recommend cleanup of outdated or low-quality documents:

- Flag documents with outdated metadata (e.g., “2018 Draft Budget – Missing Owner”)
- Propose archiving or disposing of files marked “Obsolete” or “Inactive” per retention rules
- Document any risks or dependencies before cleanup actions (e.g., “Obsolete but referenced in Audit Report”)
- Assign cleanup tasks to department focal points with expected deadlines
- Maintain a tracker to monitor completion status and notes from business owners

5.2.D
(1/2)

A

Assess Business Relevance of Captured Documents: The Data Governance Specialist, in coordination with Data Stewards, evaluates whether captured documents and content actively support the Entity's business functions, service delivery, or compliance requirements. This step ensures that content retained in the system has a clear purpose and justifies the resources needed to manage it.

- i. **Map documents to business processes and services:** Determine how each document contributes to or supports a functional business activity.
 - a. **Confirm alignment with business service delivery:**
 - Identify documents that are directly tied to public-facing or internal services (e.g., Citizen Application Forms, Staff Onboarding Manuals)
 - Assess whether those documents are current and accessible at the point of need
 - Flag outdated service documents that may cause delays or confusion
 - b. **Create a Document-to-Process mapping register:**
 - Maintain a table linking each key document to the business function or workflow it supports
 - Include fields such as: Document ID, Process Name, Owner, Frequency of Use, and Last Validated Date
 - Use this register to inform future decisions around content retention, migration, or redesign
- ii. **Evaluate documents based on strategic importance:** Assess how each document supports critical objectives such as compliance, auditability, continuity, or institutional knowledge.
 - a. **Identify documents required for regulatory or legal purposes:**
 - Confirm whether the document is cited in any policy, standard, or legal directive
 - Tag documents that must be retained for a defined legal or fiscal period (e.g., "Keep 7 years for audit")
 - Review with Legal or Compliance focal points if retention purpose is unclear
 - b. **Evaluate operational impact:**
 - Determine if the document is essential for continuity during staff turnover or emergencies (e.g., SOPs, escalation paths)
 - Identify key internal documents used in planning, budgeting, or citizen engagement
 - c. **Categorize documents by value tier:**
 - **High-value:** Critical to compliance, decision-making, or service delivery
 - **Medium-value:** Operationally useful but not mission-critical
 - **Low-value:** Historical or reference-only content
 - Use this tiering to inform retention, migration, and digitization decisions

5.2.D
(1/2)

- iii. **Document findings and link to content governance actions:** Capture all business relevance insights and use them to drive prioritization, cleanup, and retention decisions.

a. **Integrate business relevance into lifecycle governance:**

- Use relevance tags to define retention schedules, archival paths, and publishing rights
- Prioritize High-value documents for structured workflows and enhanced access
- Deprioritize or flag Low-value content for future consolidation, archiving, or retirement

RACI Matrix – Records & Content Capture

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	Metadata Specialist	Data Stewards	IT Team
5.2.A	Tag Captured Content with Standardized Metadata	I	A	C	R	R	R
5.2.B	Define and Apply Document Quality and Usage Criteria		A	R	R	R	
5.2.C	Identify Content Redundancies, Gaps, and Improvement Opportunities		A	R		R	
5.2.D	Assess Business Relevance of Captured Documents		A	R		R	

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

Based on this Activity, the Entity can



Define and Apply Document Quality and Usage Criteria



Assess Business Relevance of Captured Documents

5.3 Versioning & Control

A versioning and control process ensures that documents and content managed within the Entity's Document and Content Management Tool are accurate, traceable, and auditable throughout their lifecycle. This includes tracking every change made, preserving historical versions, and supporting secure collaboration between users. Effective version control minimizes risks related to outdated content, unauthorized modifications, or lost changes.

This section outlines the configuration of versioning settings, real-time collaboration features, version recovery tools, and intelligent notification systems that allow users and stakeholders to stay informed and in control of document changes.

Process – Versioning & Control

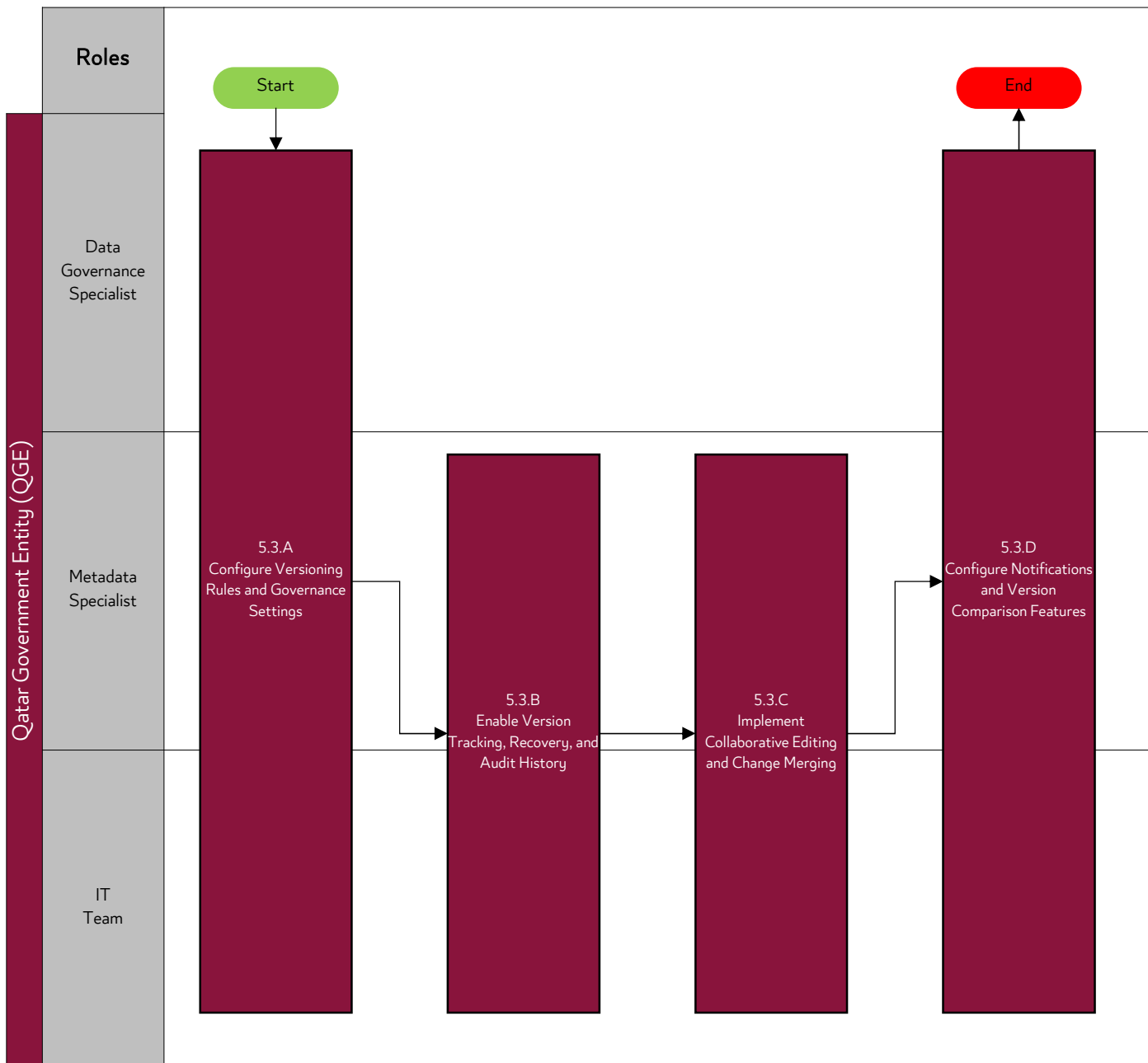


Figure 11 – Versioning & Control Process Map

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

Configure Versioning Rules and Governance Settings: The IT Team, in collaboration with the Metadata Specialist and Data Governance Specialist, defines and configures the rules and policies that govern how document versions are created, labeled, tracked, and retained across the document and content management tool.

- i. **Define versioning governance standards:** Establish the rules and conditions for how versions are created, managed, and labeled.
 - a. **Define versioning triggers and update behaviors:**
 - Create rules for when a new version is automatically generated (e.g., after document approval, status change, or major content update)
 - Specify whether users must manually choose to version, or if the system auto-versions on save
 - Define major vs. minor versions and when each applies (e.g., 1.1 for draft changes, 2.0 for approvals)
 - b. **Standardize version naming and numbering conventions:**
 - Decide on format: e.g., “v1.0”, “v2.3”, “Draft 1”, “Final 3”
 - Ensure consistency across departments by embedding version naming rules in the DCM Tool settings or training guides
 - Align version naming with document status metadata (e.g., “Approved”, “Archived”)
 - c. **Set version retention and archival policies:**
 - Define how many versions to retain for each document type (e.g., retain all for contracts; only final versions for newsletters)
 - Configure archival rules for inactive versions (e.g., move to archive after 12 months of inactivity)
 - Ensure old versions are never deleted manually without proper approval or policy-based disposition
- ii. **Configure system settings for version creation and access:** Translate versioning policies into technical system settings.
 - a. **Enable automatic version creation within the document and content management tool:**
 - Turn on system-level versioning features to track all document updates
 - Allow for both major and minor version creation
 - Ensure the system captures metadata for each version (e.g., editor name, timestamp, change summary)

5.3.A
Cont.
(2/2)

b. Define access and edit rights for different roles:

- Restrict version deletion to administrators or designated content managers
- Allow viewers to see the latest version only, unless explicitly granted access to version history

c. Link versioning with metadata and audit logs:

- Ensure version changes trigger metadata updates (e.g., Modified Date, Version Number)
- Configure audit trails to capture version actions: who made changes, what changed, and when
- Test version creation across user roles to validate permissions and system behavior

5.3.B
(1/2)

Enable Version Tracking, Recovery, and Audit History: The IT Team, in coordination with the Metadata Specialist, configures and validates the Document and Content Management Tool to ensure that all document changes are automatically tracked, historically recorded, and recoverable when needed. This supports transparency, traceability, and lifecycle compliance.

- i. **Enable automated version tracking and change logging:** Ensure that every document update results in a system-tracked version with a full change log.

a. Configure version tracking functionality in the tool:

- Activate automatic version control settings so every saved change creates a new version or checkpoint
- Ensure each version captures: editor name, timestamp, change type, and optional comments
- Allow users to optionally add a change note (e.g., “Added clause 4.2” or “Updated signature section”)

b. Ensure version metadata is visible to authorized users:

- Display version numbers, change timestamps, and author names in the document history panel
- Include metadata tags such as “Version Status,” “Reviewed By,” and “Reviewed On” where applicable
- Maintain versioning consistency across content types, whether text documents, scanned PDFs, or web content

c. Maintain complete historical logs for all documents:

- Store full version history from document creation to final archival or disposal
- Disable manual deletion of older versions unless through an approved governance-controlled process
- Retain version history even when a document is moved, renamed, or reassigned

A

5.3.B
Cont.
(2/2)

- ii. **Enable version comparison and recovery capabilities:** Allow users to restore earlier versions or compare changes between versions when needed.
 - a. **Configure version recovery settings:**
 - Ensure that any user with edit rights can revert to a previous version
 - Log each recovery as a new version to maintain audit integrity
 - Add an option to restore from “last approved” or “last published” version in workflows
 - b. **Validate recovery and comparison features in test scenarios:**
 - Test restoring an older version and confirm metadata updates correctly
 - Confirm that version comparison works across file types used by the Entity (e.g., DOCX, PDF)
 - Verify version rollbacks are restricted to authorized roles only
- iii. **Audit versioning activity for compliance and traceability:** Ensure all versioning events are recorded and auditable for governance and regulatory purposes.
 - a. **Configure versioning logs in the DCM Tool:**
 - Capture events such as version creation, rollback, deletion (if allowed), and comment additions
 - Link versioning logs with user profiles and timestamps for traceability
 - Store logs in tamper-proof format with role-based access controls
 - a. **Integrate versioning data with content governance reporting:**
 - Include versioning metrics in governance dashboards (e.g., # of versions per document, last modified by, rollback frequency)
 - Use these insights to flag unusual behavior (e.g., frequent rollbacks, unapproved edits)
 - Review audit logs during regular governance and compliance reviews

5.3.C
(1/2)

A

Implement Collaborative Editing and Change Merging: The IT Team, in coordination with the Metadata Specialist, enables and tests collaborative editing features within the document and content management tool. These capabilities allow multiple users to edit the same document in real time or near-real time, with changes tracked, merged, and versioned accurately.

- i. **Enable real-time and co-authoring features:** Activate the tool's collaborative functionality to allow multiple users to edit shared documents simultaneously.
 - a. **Turn on co-editing or real-time collaboration mode:**
 - Enable collaborative editing for document types that support it (e.g., DOCX, spreadsheets, HTML-based forms)
 - Verify that real-time changes are saved dynamically and without corruption
 - Test co-authoring across departments to ensure stability in multi-user scenarios
 - b. **Configure user permissions and roles:**
 - Allow only designated roles (e.g., Contributor, Reviewer) to co-edit specific content
 - Prevent unauthorized roles (e.g., Viewers) from modifying content
 - Set rules for when collaboration is allowed (e.g., in Draft status only, not after approval)
 - c. **Display user presence and edit indicators:**
 - Ensure the tool shows who is currently editing a document in real-time
 - Highlight edits made by different users using colored indicators, initials, or time stamps
 - Allow users to see a change log summarizing who changed what and when
- ii. **Track and merge changes from multiple users:** Ensure that edits made by multiple users are tracked, recorded, and merged cleanly to avoid data loss or confusion.
 - a. **Enable change tracking during collaboration sessions:**
 - Activate "Track Changes" features where supported (e.g., insertions, deletions, formatting)
 - Ensure change tracking is stored with the version and not just the file
 - Configure visual cues for tracked edits (e.g., underlines, strikethroughs, margin notes)
 - b. **Configure change merging logic:**
 - Choose how simultaneous edits are merged (e.g., auto-merge, manual resolution, reviewer-based acceptance)
 - Configure system behavior when changes conflict (e.g., notify user, prompt for resolution, create parallel versions)
 - Document how conflicts are handled and include guidance in user training

5.3.C
Cont.
(2/2)c. **Maintain edit history per user:**

- Log individual contributions within each collaborative session
- Display user-specific edit history when needed for audit or rollback
- Allow document owners to view and export detailed change logs

iii. **Train users on collaborative features and monitor adoption:** Provide guidance to departments on how to use collaborative features effectively, and monitor for performance or usability issues.

a. **Provide training and quick reference guides:**

- Develop a one-pager or walkthrough video showing how to open, edit, and save documents collaboratively
- Explain how users can view who is editing, resolve merge conflicts, and revert unintended changes
- Clarify how collaboration ties into versioning and approval workflows

b. **Monitor system performance and edit issues:**

- Track system responsiveness during co-editing, especially with larger files or concurrent users
- Log performance issues, failed saves, or corrupted edits for troubleshooting
- Adjust file size limits, session timeouts, or user concurrency settings based on real-world testing

c. **Review collaboration logs during audits:**

- Include collaborative session logs in the broader document audit trail
- Ensure the system shows who contributed what content, when, and under what permissions
- Flag workflows or documents where collaboration caused frequent conflicts or confusion

5.3.D
(1/2)

Configure Notifications and Version Comparison Features: The IT Team, in coordination with the Metadata Specialist and Data Governance Specialist, configures automated change notifications and version comparison capabilities in the tool.

i. **Enable automated change notifications:** Ensure the system alerts stakeholders when key documents are modified, based on business rules and metadata.

a. **Configure change notification triggers:**

- Define which events trigger alerts (e.g., document edit, approval, rejection, status change, version creation)
- Set rules to trigger notifications only for specific content types (e.g., “Notify Legal team when Contract is modified”)
- Use metadata to narrow scope (e.g., “If Sensitivity = Confidential and Status = Approved → Notify Owner”)

VA

5.3.D
(2/2)

b. Define notification recipients and delivery method:

- Route notifications to document owners, approvers, and relevant stakeholders based on role and metadata
- Allow users to opt in or out of notifications where appropriate
- Deliver alerts via email, system inbox, dashboard widget, or integration with communication tools (e.g., Microsoft Teams)

c. Standardize notification content and frequency:

- **Ensure each notification includes:** document name, triggering event, user who made the change, and link to the file
- Avoid excessive notifications by enabling batching or summary views for frequent editors

ii. **Activate version comparison tools:** Allow users to visually compare two or more document versions to quickly understand what changed.

a. Enable version comparison in the tool interface:

- Activate built-in tools that allow side-by-side or overlay comparisons of two selected versions
- Ensure support for commonly used formats (e.g., DOCX, PDF, XLSX)
- Allow version comparison to be triggered from the version history panel or approval interface

b. Display highlighted changes between versions:

- Highlight additions, deletions, and formatting changes using color-coded markup
- Indicate which user made each change and when (where supported)
- Enable quick toggle between clean and markup views for readability

c. Link version comparison tools to workflows and reviews:

- Allow reviewers to compare versions as part of approval or review workflows
- Provide a "Compare with Previous" button in all task assignments or document review windows
- Ensure that final approvers can confirm that required changes were made by checking version deltas

RACI Matrix – Versioning & Control

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	Metadata Specialist	Data Architect	Data Owners	Data Stewards	IT Team	Department Focal Point
5.3.A	Configure Versioning Rules and Governance Settings	I	A	R	R				R	
5.3.B	Enable Version Tracking, Recovery, and Audit History		A	C	R			C	R	
5.3.C	Implement Collaborative Editing and Change Merging		A	I	R	I	I	I	R	I
5.3.D	Configure Notifications and Version Comparison Features	I	A	R	R	I	I	I	R	I

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

Based on this Activity, the Entity can



Configure Versioning Rules



Implement Collaborative Editing and Version Comparison

5.4 Backup & Recovery

A robust backup and recovery process ensures that critical documents and content stored in the Document and Content Management Tool are protected against data loss, corruption, or system failure. Backup and recovery is not only a technical safeguard—it is a core pillar of content governance that supports business continuity, legal compliance, and information integrity.

This section guides the Entity in classifying critical documents, integrating DCM Tool backups into the broader IT strategy, and ensuring recovery mechanisms are tested and ready for use.

Process – Backup & Recovery

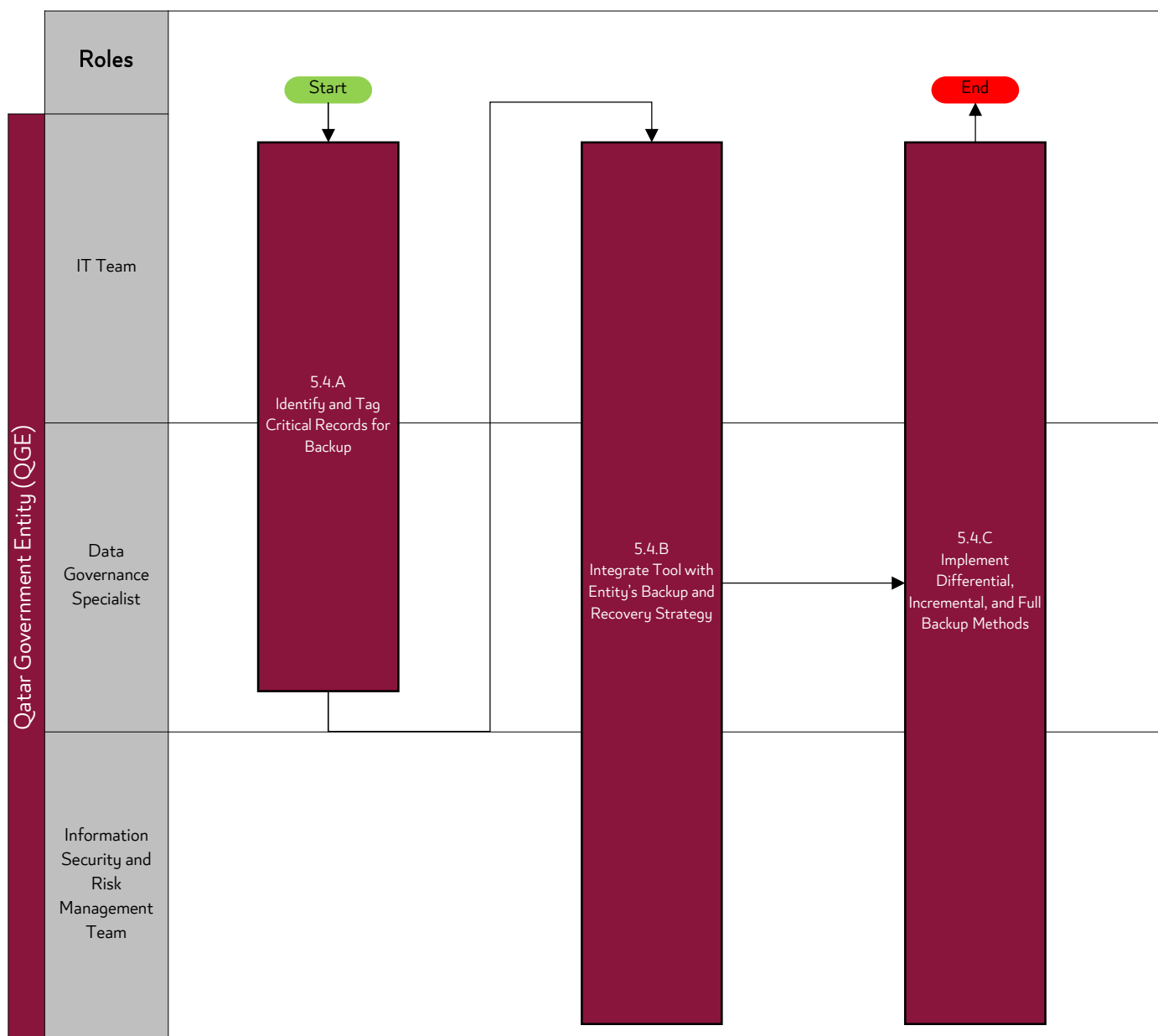


Figure 12 – Backup & Recovery Process Map

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

5.4.A
(1/2)

A

Identify and Tag Critical Records for Backup: The Data Governance Specialist, in coordination with Data Stewards and the IT Team, ensures that all critical documents are clearly tagged and cataloged within the tool to support prioritized backup and recovery. This tagging forms the foundation for a risk-based protection strategy aligned with the Entity's continuity, legal, and regulatory obligations.

- i. **Define what qualifies as a critical record:** Establish a shared understanding of which documents require priority backup and recovery.
 - a. **Develop business and compliance-based criteria:**
 - Records required by law or regulation to be preserved (e.g., audit logs, legal contracts)
 - Documents that support essential operations (e.g., service delivery procedures, policy manuals)
 - Content classified as high-sensitivity (e.g., Top Secret) or mission-critical for continuity (e.g., incident response plans)
 - b. **Align criteria with existing document metadata:**
 - Use metadata fields from 5.1.F such as "Criticality Level," and "Retention Period"
 - Ensure the criteria are consistently applied across departments using dropdowns or checklists in the tool
 - c. **Review criteria with Legal, Risk, and Business Continuity teams:**
 - Validate that the criteria cover regulatory, legal, and operational risks
 - Adjust definitions based on feedback from compliance leads and data owners
 - Secure formal endorsement of the criteria from the Data Governance Office
- ii. **Tag and register critical records in the tool:** Use the defined criteria to identify and label critical documents stored in the system.
 - a. **Apply criticality tags to existing documents:**
 - Run filtered reports based on retention metadata, document type, and sensitivity classification to find likely critical items
 - Work with departments to confirm whether each candidate document is indeed critical
 - Apply a "Criticality level = Critical" metadata tag or flag in the tool for tracking and reporting
 - b. **Maintain a centralized Critical Records Register:**
 - Extract all tagged critical documents into a centralized register (e.g., Excel sheet, DCM Tool dashboard, etc.)
 - Include fields such as Document Name, Department, Owner, Last Modified Date, and Backup Status

5.4.A
Cont.
(2/2)

- Review the register quarterly or annually to ensure completeness and update classifications

c. Use this tagging to drive risk-based backup planning:

- Ensure the Critical Records Register feeds directly into backup prioritization
- Mark any documents missing backup coverage as “At Risk”
- Use this list as a foundation for DR testing, audit checks, and governance reporting

5.4.B
(1/2)

A

Integrate Tool with Entity’s Backup and Recovery Strategy: The IT Team, in coordination with the Data Governance Specialist and the Information Security and Risk Management Section, incorporates the Document and Content Management Tool into the Entity’s enterprise-level backup and disaster recovery plan.

- i. **Define the tool’s role in the Entity’s recovery architecture:** Ensure the Document and Content Management Tool is treated as a mission-critical system with appropriate disaster recovery measures.
 - a. **Include the DCM Tool in the official Business Continuity and Disaster Recovery (BC/DR) framework:**
 - Register the tool in the Entity’s list of systems requiring periodic backup and defined recovery point objectives (RPOs) and recovery time objectives (RTOs)
 - Categorize the tool based on its criticality (e.g., Tier 1 = High availability, fast recovery required)
 - Ensure BC/DR documentation clearly states where backups are stored and who owns the recovery responsibility
 - b. **Document backup and recovery policies specific to the tool (if not defined in the DCM Policy):**
 - Define frequency of backups (e.g., daily full backup, hourly differential backups)
 - Define acceptable data loss thresholds (e.g., no more than 4 hours of lost data)
 - Include procedures for failover, data restoration, and audit confirmation
 - c. **Align recovery plans with content sensitivity and criticality:**
 - Ensure critical documents are included in high-priority backup plans
 - Assign faster RTOs for critical content types (e.g., operational manuals, legal records)
 - Establish role-based access to recovery functions (e.g., only Records Manager can initiate recovery of legal documents)

5.4.B
(2/2)

- ii. **Coordinate with security and risk management protocols:** Ensure the backup and recovery processes meet the Entity's data security and compliance requirements.
- a. **Enforce encryption and secure backup practices**
 - Encrypt backup files both at rest and during transmission
 - Store backups in secure, access-controlled locations (e.g., offsite data centers, government-approved cloud)
 - Maintain a record of all backup destinations and associated access permissions
 - b. **Integrate recovery procedures with risk management activities:**
 - Perform risk assessments for Document and Content Management Tool data loss scenarios (e.g., ransomware, accidental deletion, file corruption)
 - Document mitigation strategies, such as cold storage for long-term records or immutable backups for legal files
 - Link recovery procedures to the Entity's data breach response and incident handling plans
 - c. **Conduct backup configuration reviews as part of governance audits:**
 - Include tool backup settings in regular internal or third-party IT audits
 - Review backup logs to ensure scheduled jobs are completing successfully
 - Maintain an audit trail of backup activity and related incident responses

5.4.C
(1/2)

Implement Differential, Incremental, and Full Backup Methods: The IT Team, in coordination with the Data Governance Specialist and Information Security Team, implements a layered backup strategy for the tool using full, differential, and incremental backups. This ensures efficient, scalable protection for critical and non-critical content while maintaining compliance with recovery expectations.

VA

- i. **Define the Entity's tool backup architecture:** Establish a backup model that balances frequency, system load, and recovery effectiveness.
- a. **Configure full backup routines for baseline integrity:**
 - Schedule full backups of the entire document and content repository on a weekly or biweekly basis
 - Store these backups in at least two separate secure locations (e.g., on-premises and cloud)
 - Ensure full backups capture all metadata, document content, version histories, and permissions
 - b. **Implement differential backups for mid-cycle recovery points:**
 - Schedule daily differential backups to capture changes made since the last full backup
 - Optimize scheduling to occur during low-activity hours (e.g., overnight) to reduce system impact
 - Use differential logs to reduce total backup size while preserving fast restoration

5.4.C
(1/2)

c. Set up incremental backups for high-frequency environments:

- For content that changes hourly or more (e.g., shared folders, collaborative editing zones), enable incremental backups
- Capture only the data changed since the last backup (full or incremental), minimizing resource usage
- Enable fast-roll forward restoration paths using incremental snapshots for high-availability areas



Key Message / Information

The IT team is responsible for monitoring backup activity, resolving any failed backup incidents, and ensuring these configurations are reviewed periodically under the Entity's central IT governance protocols.

RACI Matrix – Backup & Recovery

Indicative

Sr No.	Activity	Data Management and Governance Section Head	Information Security and Risk Management Team	Data Governance Specialist	Metadata Specialist	Data Stewards	IT Team
5.4.A	Identify and Tag Critical Records for Backup	A		R	C	C	R
5.4.B	Integrate Tool with Entity's Backup and Recovery Strategy	A	R	R			R
5.4.C	Implement Differential, Incremental, and Full Backup Methods	A	R	R			R

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

Based on this Activity, the Entity can



Configure Versioning Rules



Implement Collaborative Editing and Version Comparison

5.5 Retention & Disposal

A structured retention and disposal process ensures that documents and content are kept only as long as necessary, then securely and compliantly retired or destroyed. This reduces storage burden, minimizes legal risk, and upholds the principles of lifecycle governance defined in the Entity's Document & Content Management Policy.

This section guides the Entity through validating retention rules, establishing review and approval procedures for disposal, and implementing secure retirement or destruction techniques for all document types.

Process – Retention & Disposal

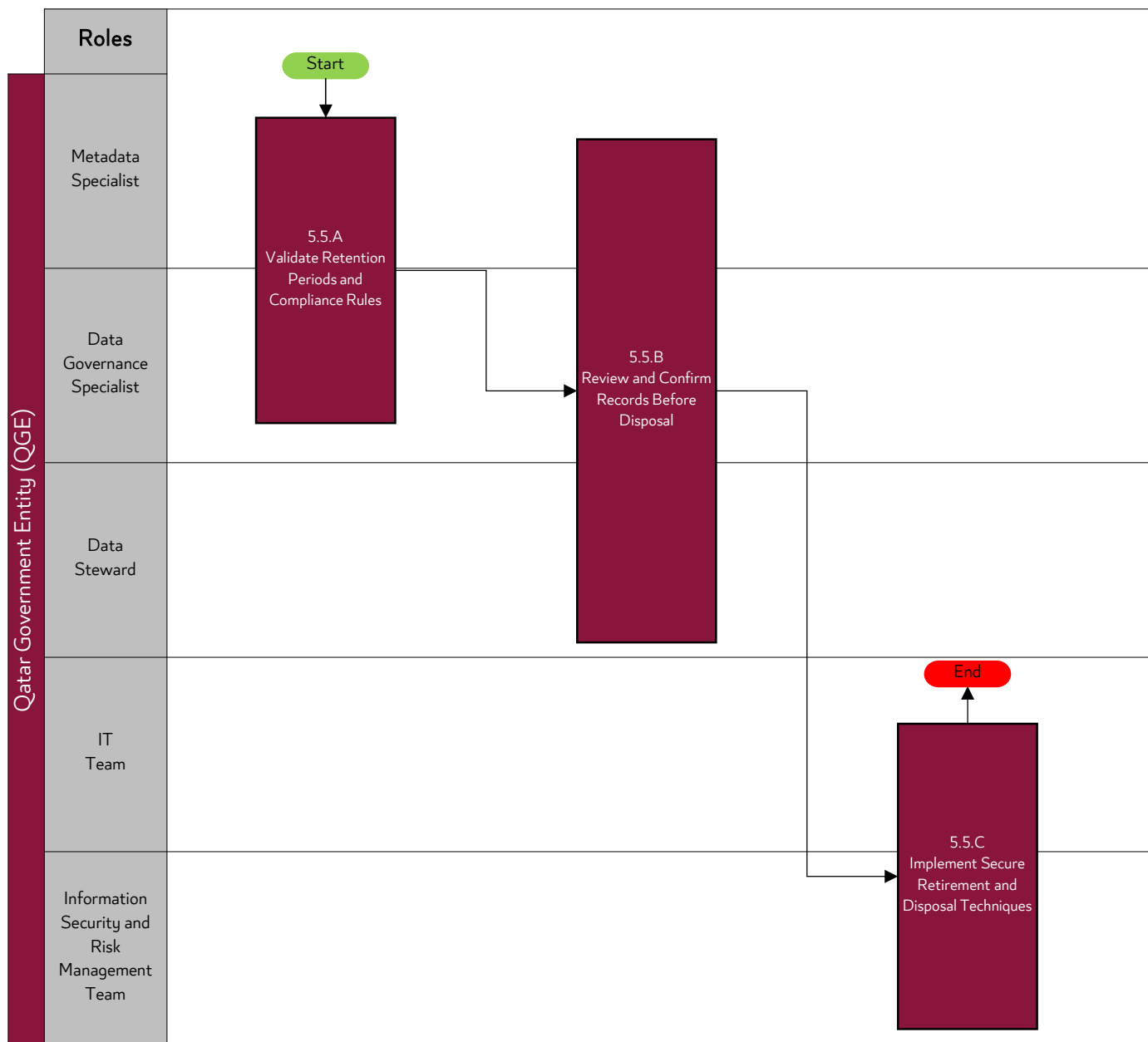


Figure 13 – Retention & Disposal Process Map

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

5.5.A

A

Validate Retention Periods and Compliance Rules: The Metadata Specialist, in collaboration with the Data Governance Specialist, and Legal, reviews and confirms that retention periods applied to all documents are accurate, justified, and aligned with the retention requirements defined in the Entity's Document & Content Management Policy.

- i. **Review retention rules defined in the Entity's policy:** Start by confirming the source of truth for document retention: the Entity's official document and content management policy.
 - a. **Extract retention rules from the approved policy:**
 - Review the Document & Content Management Policy for listed retention categories and durations
 - Capture these rules in a structured table (e.g., Document Type, Retention Period, Legal Basis, Department Owner)
 - Note any conditional rules (e.g., "Keep 7 years after contract end date" or "Permanent for regulatory reports")
 - b. **Validate alignment with national or regulatory standards:**
 - Cross-check retention durations against legal and regulatory mandates relevant to the Entity (e.g., audit, HR, legal, finance laws)
 - Confirm whether certain document types must be held permanently or transferred to archival bodies
 - Engage Legal to approve or revise draft retention durations
- ii. **Apply validated retention rules to document metadata:** Ensure that all documents stored in the tool are tagged with an appropriate retention value based on the verified rules.
 - a. **Create or update the "Retention Period" metadata field:**
 - Populate this field across all document types based on the retention mapping table
 - Ensure values are standardized (e.g., "3 years", "7 years", "Permanent")
 - Tag the associated retention trigger event (e.g., "Date Created", "Contract Expiry Date", "Case Closure Date")
 - b. **Use default retention values where available:**
 - For commonly used document types (e.g., invoices, policies, meeting minutes), apply default retention based on approved rules
 - Enable inheritance where possible (e.g., all documents in "Legal > Contracts" get 7 years by default)
 - Review exceptions or special cases with department focal points before overriding defaults
 - c. **Track retention status in the Document and Content Management Tool:**
 - Configure the system to calculate retention status automatically (e.g., "Active", "Retention Expired", "Pending Disposal Review")
 - Set up reports or dashboards to view how many documents are nearing their retention deadline
 - Ensure retention logic is reviewed annually or when policy updates occur

5.5.B

A

Review and Confirm Records Before Disposal: The Data Governance Specialist and Departmental Data Stewards, reviews documents flagged for disposal to confirm their eligibility and business irrelevance. This step ensures that no document is deleted or retired without clear approval, appropriate documentation, and audit compliance.

- i. **Establish a pre-disposal review process:** Create a standardized workflow for verifying and approving documents before they are disposed of.
 - a. **Define eligibility conditions for disposal:**
 - Retention period has expired based on metadata or trigger date
 - No legal holds or audit dependencies are in effect
 - Document has been reviewed by the content owner and marked for disposal
 - b. **Build a review checklist or form:**
 - Include fields for Document ID, Department, Retention Expiry Date, and Disposal Rationale
 - Require review and sign-off from Data Steward and/or Content Owner
 - Include a field to record any exception (e.g., "Hold due to pending litigation")
 - c. **Integrate review into the Document and Content Management Tool workflow:**
 - Configure the DCM Tool to flag documents whose retention periods have expired
 - Route these items into a "Disposal Pending Review" queue
 - Notify designated reviewers to evaluate and approve each case
- ii. **Document approvals and disposal decisions:** Record all pre-disposal decisions to ensure accountability, auditability, and future traceability.
 - a. **Log who approved or rejected each disposal:**
 - Record the reviewer's name, role, and approval decision
 - Capture the review date, time, and document status at the time of review
 - Store this information in a protected Disposal Approval Log
 - b. **Require documented rationale for every action:**
 - **If approved:** "Retention period expired; confirmed not in use"
 - **If rejected:** "Pending audit closure", "Legal hold in place", or "Reclassified as permanent"
 - Include an optional notes field for reviewer comments
 - c. **Maintain a tamper-proof audit trail:**
 - Lock the approval logs from manual editing
 - Ensure logs are searchable and reportable by audit and compliance teams
 - Retain all approval history for a minimum of 3–5 years, or in accordance with legal policy

5.5.C

Implement Secure Retirement and Disposal Techniques: The IT Team, in collaboration with the Information Security Team, carries out approved retirement and disposal actions using secure, traceable, and policy-compliant methods. These actions ensure that documents are either permanently deleted, archived, or transferred — based on their retention classification and risk profile.

A

- i. **Apply approved retirement or archival methods:** Execute non-destructive retention actions for content that must be stored beyond active use.
 - a. **Move records to nearline or offline storage:**
 - Transfer expired but legally required content to an offline archive or repository
 - Use metadata tagging (e.g., “Archived = Yes”) to clearly mark retired documents
 - Restrict editing or movement of archived documents to designated roles only
 - b. **Transfer to official archival bodies or third parties:**
 - For permanent or historically valuable records, coordinate with national archives or designated archival entities
 - Prepare content in accepted formats and structures (e.g., PDF/A, metadata packages, XML exports)
 - Ensure a formal handoff record is maintained, documenting transfer date, content description, and receiving entity
 - c. **Retain digital and physical archive index logs:**
 - Maintain a list of archived documents, including location, format, access restrictions, and retention reason
 - Store index logs within the document and content management tool or in an external governance tool for reference
 - Ensure index logs are searchable by title, department, and archival category
- ii. **Perform secure deletion or destruction where appropriate:** Use irreversible, policy-approved deletion methods for documents that are no longer required and have passed the review stage.
 - a. **Use approved deletion mechanisms for digital files:**
 - Overwrite file data to prevent recovery (e.g., digital shredding)
 - Log file IDs, deletion date, deletion method, and user who performed the action
 - Prohibit deletion from shared folders or active systems without approval
 - b. **Destroy physical media containing classified content:**
 - Use certified shredding or incineration for paper records
 - Physically destroy external drives or discs containing retired digital documents
 - Follow information security protocols for disposal of classified media
 - c. **Maintain destruction records for audit and accountability:**
 - Log every deletion or destruction event in a Disposal Execution Log
 - Include document ID, method used, date/time, and reviewer/authorizer
 - Retain disposal logs securely for future audit, litigation, or compliance reviews

RACI Matrix – Retention & Disposal

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Information Security and Risk Management Team	Data Governance Specialist	Metadata Specialist	Data Owners	Data Stewards	IT Team	Legal Team
5.5.A	Validate Retention Periods and Compliance Rules	I	A		R	R				C
5.5.B	Review and Confirm Records Before Disposal		A		R		I	R		
5.5.C	Implement Secure Retirement and Disposal Techniques		A	R	C			C	R	

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

Based on this Activity, the Entity can



Validate Retention Periods



Implement Secure Disposal Techniques

5.6 Document & Content Metadata

Document and content metadata provides the foundation for organizing, securing, and governing unstructured information across the Entity's Document Management Tool. It enables content to be classified, searched, filtered, linked, and managed across its full lifecycle.

This section guides the Entity in implementing and enriching metadata within the tool, ensuring all content is tagged in accordance with metadata standards, enriched with key governance attributes such as sensitivity and access history, and configured to support discoverability, retention, and access control across departments.

Process – Document & Content Metadata

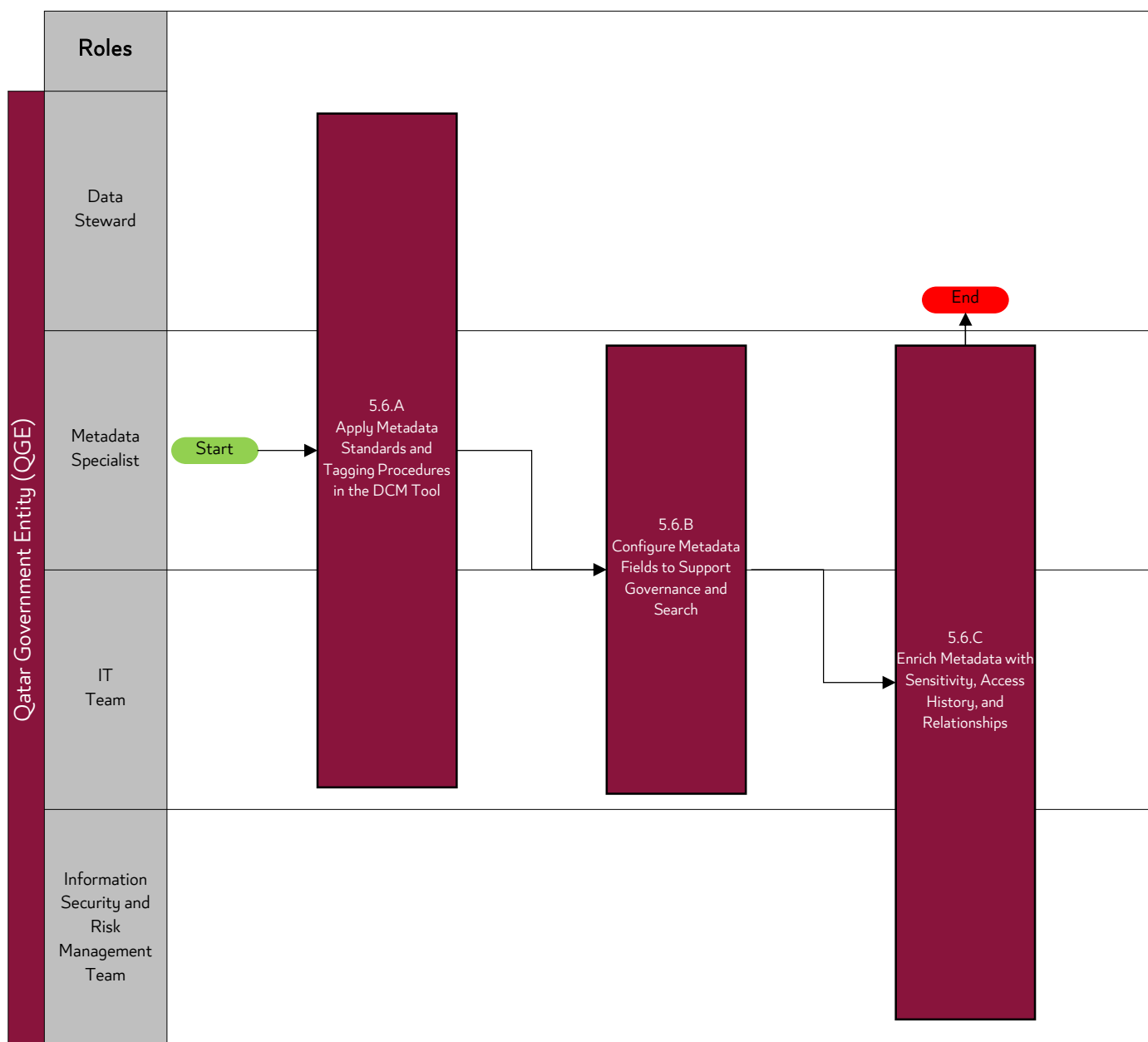


Figure 14 – Document & Content Metadata Process Map

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

5.6.A

Apply Metadata Standards and Tagging Procedures in the DCM Tool: The Metadata Specialist, in collaboration with the IT Team and Data Stewards, ensures that all documents and content stored in the DCM Tool are tagged using metadata structures that align with the Entity's metadata governance standards.

- i. **Align tool metadata fields with Entity-wide data catalog and metadata management policy:** Ensure that metadata tagging within the document and content management tool reflects the approved vocabulary and is aligned to the data catalog and metadata management policy (in addition to terms determined in section 5.1).
 - a. **Reference approved metadata domains and vocabularies:**
 - Use naming conventions and controlled lists defined as part of the data catalog and metadata management domain and the metadata fields outlined in section 5.1
 - Apply consistent values for fields such as Document Type, Department, Status, and Sensitivity Classification
 - Include shared classification terms used across structured and unstructured environments (e.g., "Restricted / Internal / Public")
 - b. **Validate field definitions and allowed values:**
 - For each metadata field, define: name, description, format, and allowed values
 - Example: "Document Type" = Policy, Contract, Report, Form, etc.
 - c. **Ensure tool metadata fields are mapped to governance roles:**
 - Assign ownership for key fields (e.g., Sensitivity Classification = Information Security; Document Type = Content Owner)
 - Define who is responsible for maintaining metadata lists and enforcing tagging
- ii. **Implement standardized tagging procedures for all content:** Ensure that metadata is consistently applied to both new and legacy content.
 - a. **Tag all new content at the point of upload:**
 - Configure mandatory metadata fields in upload workflows (e.g., Document Type, Owner, Department, Retention Period)
 - Provide drop-downs or lookup fields to enforce consistency
 - Prevent publishing or approval unless minimum metadata is completed
 - b. **Apply metadata to legacy content during migration or audit:**
 - Use automated tools to batch-tag legacy documents based on folder, filename, or document properties
 - Assign Data Stewards to manually review and correct metadata where needed
 - Prioritize tagging for high-risk or critical content (identified in Sections 4.2 and 5.4)
 - c. **Include metadata tagging in training and onboarding:**
 - Train content contributors on the purpose of each field and how to apply tags

A

5.6.B
(1/2)

A

Configure Metadata Fields to Support Governance and Search: The IT Team, in coordination with the Metadata Specialist, configures metadata fields in the tool to support classification, filtering, access control, retention, and enterprise-wide content discovery.

- i. **Configure metadata fields for lifecycle and access governance:** Ensure that key governance functions — such as retention enforcement and access restriction — are metadata-driven.

a. **Set up metadata fields to control document lifecycle:**

- Create fields such as “Retention Period,” “Review Date,” “Last Modified,” and “Disposition Status”
- Use metadata to trigger lifecycle workflows (e.g., alert for review, auto-archive, mark for deletion)
- Ensure these fields are integrated with the retention and disposal logic in Section 5.5

b. **Use metadata to support classification and access control:**

- Configure a “Sensitivity Classification” field with values such as Top Secret, Secret, Restricted, Internal, and Public, based on the National Data Classification Policy
- Link each classification level to predefined permission groups or roles (e.g., “Confidential” content = accessible only to Legal, HR, or Management roles)
- Ensure access controls are enforced dynamically in the document and content management tool based on metadata values — users should only see or interact with documents that match their role and clearance level
- Align metadata fields and values with the access request and approval workflows defined in activity 5.1, ensuring consistency between tagging, permissions, and access governance
- Periodically review metadata tagging accuracy as part of access reviews to ensure access decisions remain valid

c. **Make governance metadata fields mandatory where applicable:**

- Require tagging of Retention Period and Sensitivity Classification for all official documents
- Block publishing or workflow advancement if mandatory fields are missing
- Include help text or validation messages to guide correct field completion

- ii. **Configure metadata fields for search, filtering, and navigation:** Ensure that users can efficiently discover and retrieve documents using intuitive, metadata-driven tools.

a. **Enable metadata-based search and filtering:**

- Index metadata fields to allow users to filter by Document Type, Department, Year, Status, etc.
- Support keyword and advanced search with field-based filtering (e.g., “Find all contracts approved by Legal in 2022”)

5.6.B
Cont.
(2/2)

a. Standardize field formats and dropdown options for usability:

- Use dropdowns and pre-approved vocabularies to prevent free text inconsistencies
- Apply consistent formatting for fields like dates, department codes, and document statuses
- Translate or localize field labels where multilingual support is required (e.g., English/Arabic)

5.6.C

Enrich Metadata with Sensitivity, Access History, and Relationships: The Metadata Specialist, in collaboration with the IT Team and Information Security Team, configures the tool to enhance metadata with advanced governance attributes that improve auditability, access monitoring, and document linkage.

i. **Capture and store user access history as metadata:** Track and expose document access records to support transparency, usage analytics, and audit readiness.

a. Enable automatic logging of document access events:

- Record user ID, access timestamp, and access type (viewed, downloaded, edited)
- Store this data as system metadata or in an attached audit trail file

b. Provide a metadata-based view of access history:

- Allow document owners or admins to see a log of who accessed a file and when
- Support access summaries (e.g., “Viewed 14 times in the last 30 days”)

ii. **Establish inter-document relationship metadata:** Enable documents to reference, link to, or inherit properties from related content.

a. Create metadata fields for relationship mapping:

- Examples: “Related Document ID,” “Parent Policy,” “Superseded By,” “Supports Report”
- Use lookup fields or auto-complete to link existing documents within the tool

b. Visualize or group related content:

- Display related documents in the tool’s UI (e.g., “See Also” or “Linked Content” panels)
- Allow users to browse by relationship type (e.g., all SOPs linked to a Policy)
- Preserve relationship links during archiving or content migration

RACI Matrix – Document & Content Metadata

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Information Security and Risk Management Team	Data Governance Specialist	Metadata Specialist	Data Stewards	IT Team
5.6.A	Apply Metadata Standards and Tagging Procedures in the DCM Tool	I	A			R	R	R
5.6.B	Configure Metadata Fields to Support Governance and Search		A			R		R
5.6.C	Enrich Metadata with Sensitivity, Access History, and Relationships	I	A	R		R		R

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

Based on this Activity, the Entity can



Apply Tagging Procedures in the Tool



Enrich Metadata

5.7 Content Publishing & Delivery

A structured content publishing and delivery process ensures that finalized documents and media are published through the correct channels, in the right format, and with the necessary approvals and metadata. This supports accessibility, traceability, and consistent communication — both internally and externally.

This section focuses on defining the Entity's official publishing channels, enforcing a publishing workflow with appropriate formatting and approvals, and applying metadata and keyword tagging to ensure content is searchable and reliably delivered to its intended audience.

5.7.A

Define Official Publishing Channels and Access Points: The Data Governance Specialist, in collaboration with the IT Team and Communications Team, identifies and formalizes the approved publishing channels for disseminating finalized content to internal and external audiences. This ensures consistency, traceability, and appropriate access to official documents.

- i. **Identify and document approved publishing channels:** Create an inventory of internal and external platforms used for official content dissemination.
 - a. **List all publishing destinations used by the Entity:**
 - **Internal:** Intranet, SharePoint hubs, employee portals, internal newsletters
 - **External:** Government websites, public portals, social media (if applicable)
 - **System-native channels:** WCMS or portal-integrated modules within the document and content management tool
 - b. **Define use cases and access scope for each channel:**
 - Specify which audiences are served (e.g., internal staff, external public, partners)
 - Define what content types are published where (e.g., Policies on Intranet, Reports on Open Data Portal)
 - Note any platform-specific formatting or tagging requirements
- ii. **Assign ownership and publishing roles:** Ensure accountability for each channel and clarify who is responsible for publishing.
 - a. **Designate channel owners:**
 - Assign responsibility for managing each publishing platform (e.g., IT for WCMS, Communications for public site)
 - Ensure owners are responsible for uptime, access rights, and formatting guidelines
 - b. **Define publisher roles within the DCM Tool:**
 - Use role-based permissions to control who can publish content
 - Ensure publishers are trained on content formatting, review steps, and tagging procedures
 - c. **Document escalation paths for publishing issues:**
 - Identify who to contact for urgent publishing needs or technical issues
 - Include publishing support contacts in training material and onboarding guides

A

5.7.B
(1/2)

A

Configure Publishing Workflow, Formatting, and Distribution Rules: The IT Team, in collaboration with the Metadata Specialist and Communications Team, configures a lightweight, approval-based publishing process within the document and content management tool or connected publishing platforms.

- i. **Configure publishing workflows in the tool:** Ensure that content cannot be published without following a defined approval path.
 - a. **Set up publishing-specific workflows:**
 - Include steps such as “Submit for Review,” “Approve for Publishing,” and “Send to Publishing Channel”
 - Allow parallel reviews if multiple stakeholders (e.g., Legal + Comms) must approve content
 - Auto-assign reviewers based on content type or department
 - b. **Restrict publishing rights to authorized roles:**
 - Only Publisher or Content Owner roles can trigger final publishing
 - Reviewers and approvers can suggest edits but cannot bypass the workflow
 - Log all workflow actions in the audit trail for accountability
 - c. **Require key metadata fields before publishing:**
 - Ensure fields like Document Type, Sensitivity Classification, Department, and Keywords are populated
 - Block publishing if mandatory metadata is missing or fails validation rules
 - Use tooltips or prompts to guide metadata completion
- ii. **Apply formatting and accessibility standards:** Ensure published content follows consistent styling, branding, and accessibility practices.
 - a. **Standardize document templates and export formats:**
 - Use approved templates for common content types (e.g., reports, policies)
 - Set output formats (e.g., PDF/A for policies, HTML for articles) based on channel requirements
 - Remove tracked changes, hidden comments, or personal metadata before publishing
 - b. **Implement accessibility and readability checks:**
 - Ensure published content meets WCAG standards (e.g., alt text, headings, color contrast)
 - Use automated tools or publishing checklists for final formatting validation
 - c. **Maintain a style guide or publishing checklist:**
 - Provide departments with a publishing checklist to validate content before submission
 - Include do's and don'ts for formatting, images, tables, and links

5.7.B
Cont.
(2/2)

iii. **Define and manage content distribution rules:** Ensure published content reaches the correct platform or audience segment reliably.

a. **Route published content to the appropriate publishing channel:**

- Use workflows or rules to automatically push content to the designated site, folder, or library
- Configure APIs or integrations if pushing content to external portals or WCMS platforms
- Tag content with destination metadata (e.g., “Channel = Intranet”) for automated routing
- Ensure keyword tagging is applied to all published content to support internal and external searchability. Keywords should include synonyms, citizen-friendly terms, and relevant language variations where applicable

b. **Schedule or delay publishing when needed:**

- Allow scheduling of future publishing dates for time-sensitive content
- Enable embargo settings if content must not be visible before a set date/time
- Allow auto-expiry or unpublishing for short-lived content (e.g., announcements, event notices)

c. **Notify stakeholders post-publishing:**

- Trigger confirmation messages or dashboard notifications once content goes live
- Send alerts to content owners, reviewers, or publishing team based on distribution rules
- Optionally include content links in newsletters or internal announcements

RACI Matrix – Content Publishing & Delivery

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Information Security and Risk Management Team	Data Governance Specialist	Metadata Specialist	Data Stewards	Communications Team	IT Team
5.7.A	Define Official Publishing Channels and Access Points	I	A		R			R	R
5.7.B	Configure Publishing Workflow, Formatting, and Distribution Rules	I	A			R		R	R

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

Based on this Activity, the Entity can



Define Publishing Channels



Configure Publishing Workflow

6. Performance Management



6. Performance Management

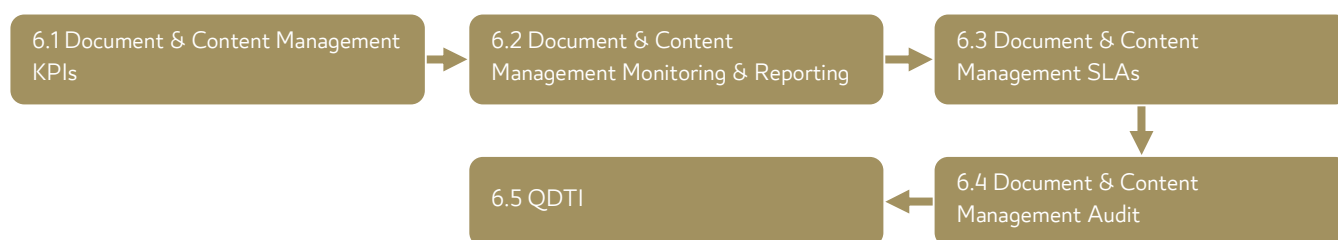
What is Performance Management and why does the Entity need it?

The Document & Content Management Performance Management process ensures that the Entity can monitor, measure, and continuously improve the effectiveness of its document governance environment. It translates operational activities into measurable performance insights and establishes the structures needed to track SLA compliance, audit readiness, and strategic improvement opportunities.

Through the definition of KPIs, structured monitoring routines, SLA tracking, and audit preparation, the Entity can ensure that content governance is not only implemented — but sustained and optimized. This process also helps surface risks, inefficiencies, or adoption challenges that may not be visible through system logs alone.

Performance management activities include defining and updating DCM Tool KPIs, creating reports, monitoring SLA compliance, escalating operational issues, preparing audit evidence, as well as calculating the Qatar Data Trust Index (QDTI) data compliance score for document and content management. These efforts reinforce accountability, support transparency, and ensure alignment with the national data standards over time.

The remaining sections of this chapter will detail the activities that guide the Entity through executing the Document & Content Management Performance Management process.



Guiding Principles for Performance Management

1. **Measure What Matters:** Focus on KPIs and SLAs that reflect operational value, governance goals, and actual system usage — not vanity metrics.
2. **Track, Act, Improve:** Use performance monitoring not just for reporting, but to surface problems, assign ownership, and drive action.
3. **Automate Where Possible:** Use system-integrated alerts to minimize manual checks and ensure issues are identified in real time.
4. **Be Audit Ready by Default:** Maintain governance artifacts and evidence in a structured way so that audit response is fast, consistent, and stress-free.

6.1 Document & Content Management KPIs

To monitor the effectiveness, usage, and governance of the Document and Content Management Tool, the Entity must define and track a set of key performance indicators (KPIs). These KPIs allow the Entity to measure content volume, system adoption, and digitization progress — and provide a foundation for improving content lifecycle governance and operational efficiency.

The National Data Standards require all Entities to define a baseline set of document management KPIs. These include the total number of documents stored, number of active users, and the percentage of paper-based documents converted to digital format. More advanced Entities may also track user engagement and document retrieval efficiency as part of a more sophisticated content performance strategy.

In addition to supporting compliance, these KPIs offer practical value. They help content managers assess user adoption, identify bottlenecks in content access or publishing, and prioritize future improvements in metadata quality, automation, or digitization. This activity outlines how the Entity can define, document, track, and refine its Document & Content Management KPIs using the standardized Data Management KPIs Register Template.

Process – Document & Content Management KPIs

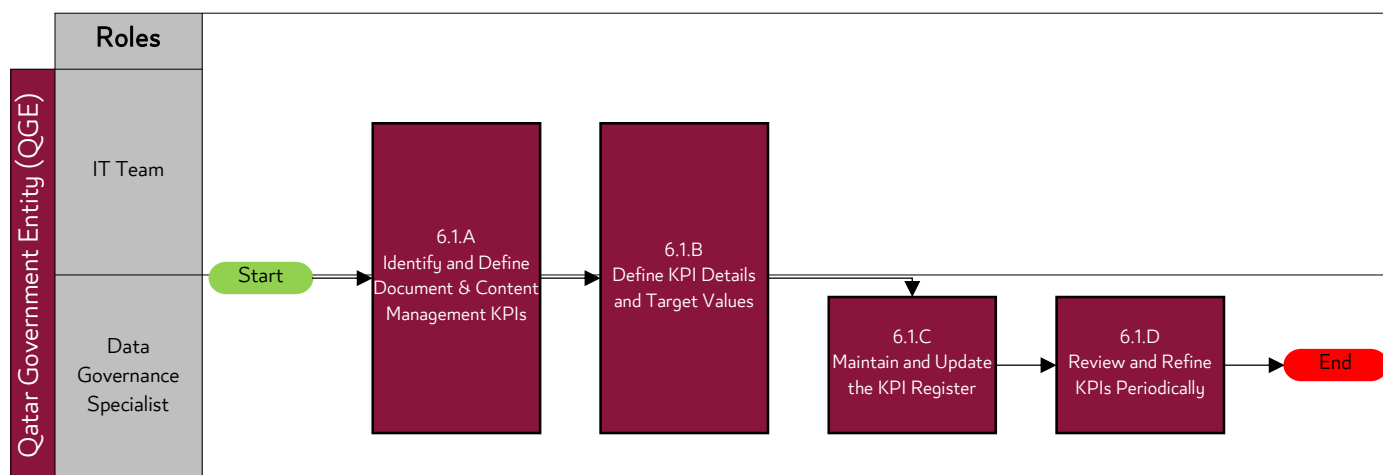


Figure 15: Document & Content Management KPIs Process Map

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

6.1.A
(1/2)

Identify and Define Document & Content Management KPIs: To evaluate the effectiveness and usage of the document and content management tool, the Entity must identify and define KPIs aligned with the national data standards. These KPIs should reflect both baseline adoption and usage, as well as more advanced engagement and lifecycle efficiency metrics.

- i. **Review National KPI Requirements:** Start by aligning the Entity's KPIs with the National Data Standards.
 - a. At a minimum, the following KPIs must be included:
 - Total quantity of documents stored and managed within the document and content management tool
 - Total number of users accessing the document and content management tool
 - Percentage of paper-based documents converted to electronic format
 - Advanced analytical KPIs that measure not only basic metrics but also user engagement and efficiency of document retrieval and processing

6.1.A
Cont.
(2/2)

- b. Confirm that these KPIs can be tracked using document and content management tool logging or analytics dashboards.
 - ii. **Identify Additional KPIs (If Needed):** Extend beyond the minimum to reflect Entity-specific objectives.
 - a. Examples may include:
 - Average document retrieval time
 - Percentage of documents found via search vs. browsing
 - Number of documents reused across departments
 - b. Only include additional KPIs if they are measurable, actionable, and relevant to catalog performance or governance outcomes.
 - iii. **Assign Preliminary Ownership and KPI ID:** Start preparing each KPI for inclusion in the register.
 - a. Assign a unique KPI ID and draft the KPI Name for each selected metric.
 - b. Assign preliminary ownership based on who will be responsible for tracking or updating the KPI.
 - c. These entries will be further detailed in 6.1.B and formally populated into the KPI Register Template in 6.1.C.



Tip

- Ensure KPIs are practical. Only define what can be tracked in the document and content management tool.
- Consider starting with just the national minimum and adding others later based on usage.
- Consult IT or the tool administrator to confirm which metrics are system-generated.

6.1.B
(1/2)

Define KPI Details and Target Values: After identifying the tool KPIs in 6.1.A, the Entity must complete the initial setup of each KPI in the KPI Register Template. This includes defining how each KPI is calculated, how frequently it will be measured, and what the performance target will be. This step ensures KPIs are ready for ongoing tracking and governance use.

- i. **Complete KPI Definitions in the Register:** Using the Data Management KPIs Register Template, define the technical and business context of each KPI.
 - a. Populate the following fields for each KPI:
 - KPI Name
 - KPI Type (Operational or Strategic)
 - Calculation Methodology (formula or logic used)
 - Measurement Frequency (e.g., monthly, quarterly)
 - Target Value (numeric or percentage-based benchmark)
 - Owner (who is responsible for tracking and updating)
 - b. Confirm that all required KPIs from the National Data Standards are included.

A

6.1.B
Cont.
(2/2) **Asset Guidance**

The **Data Management KPIs Register Template** can be used to track the DCM tool usage metrics through a structured set of fields. Entities may use this template to define and monitor relevant KPIs along with their calculation methods, target values, current status, and ownership.

Illustrative

 Data Management KPIs Register Template				
The following table is a template containing what is needed to provide a brief overview of the performance of data management initiatives				
Field	Description			
KPI ID	A unique identifier assigned to each Key Performance Indicator (KPI)			
KPI Name	A short, descriptive name that summarizes what the KPI measures			
KPI Type	Operational or Strategic KPI (if applicable)			
Calculation Methodology	The formula / approach (if any) used to calculate the KPI value			
Target Value	The predefined value or benchmark to achieve for the KPI			
Measurement Frequency	Outlines how frequently the KPI needs to be measured			
Last Updated Date	The date when the KPI's current value was last recorded or updated			
Status	On Track/Off Track			
Comments	Additional notes or explanations regarding the KPI's performance			
Owner	Outlines whether the business or IT is the owner of the KPI			

KPI ID	KPI Name	KPI Type (if applicable)	Calculation Methodology	Target Value

Measurement Frequency	Last Updated Date	Status	Comments	Owner

ii. **Validate Definitions and Targets with Stakeholders:** Before finalizing, review the register entries with relevant roles.

- a. Share draft KPI definitions with the Data Governance Specialist, IT Team, and Data Stewards
- b. Confirm that:
 - Calculation methods are technically feasible
 - Targets are realistic and measurable
 - Ownership is clear and accepted

6.1.C
(1/2)

Maintain and Update the KPI Register: Once the KPI Register has been initialized, the Entity must maintain it as a live governance tool. This step involves regularly updating KPI statuses, tracking progress toward targets, and logging any contextual notes or explanations. It ensures transparency and supports continuous improvement of catalog adoption and performance.

i. **Update KPI Status and Measurement Data:** Maintain current information in the register as KPIs are tracked.

- a. For each KPI, update the following fields on a defined schedule:
 - Last Updated Date
 - Status (e.g., On Track, Off Track)
 - Comments (explanations, changes in interpretation, or improvement actions)

A

6.1.C
Cont.
(2/2)

- b. Ensure updates are aligned with the Measurement Frequency defined in 6.1.B.
- ii. **Assign Roles for Ongoing Maintenance:** Ensure KPI updates are timely and consistent.
 - a. Confirm the data governance specialist or delegated owner is responsible for each update cycle.
 - b. Store the register in a centralized location (e.g., governance SharePoint or shared folder).
- iii. **Use the Register for Oversight and Reporting:** Leverage the KPI Register as a governance tool.
 - a. Share updated KPIs with governance leads during review cycles.
 - b. Reference the register in internal reports or communications with the DGO, if required.

**Key Message / Information**

The KPI Register must remain up to date to serve as a useful tool for governance and accountability. It supports transparency in how the document and content management tool is used and improved.

6.1.D
(1/2)

A

Review and Refine KPIs Periodically: To ensure continued relevance and effectiveness, the Entity must regularly review and refine its document and content management KPIs. This includes reassessing calculation methods, adjusting targets, incorporating feedback, and aligning KPIs with evolving organizational needs, document and content management tool features, and governance priorities.

- i. **Establish a KPI Review Schedule:** Set a consistent cadence for KPI evaluation and refinement.
 - a. Define a review cycle (e.g., annually or semi-annually).
 - b. Schedule review checkpoints in advance and include them in the Entity's data governance calendar.
- ii. **Evaluate KPI Performance and Usage Trends:** Assess how well each KPI reflects tool usage and supports decision-making.
 - a. Review KPI trends based on actual performance vs. targets.
 - b. Identify KPIs that are consistently off track, no longer relevant, or lacking in actionability.
 - c. Consider tool feature updates or governance process changes that may require KPI adjustments.
- iii. **Refine KPI Definitions, Targets, or Ownership (If Needed):** Update KPIs to reflect new realities while maintaining traceability.
 - a. Modify fields such as:
 - Calculation Methodology
 - Target Value
 - Measurement Frequency
 - Assigned Owner
 - b. Record updates in the Comments and Last Updated Date fields of the KPI Register.
 - c. Notify stakeholders of any changes that impact performance evaluation or reporting.

6.1.D
Cont.
(2/2)

Tip

- Use visual summaries (e.g., KPI dashboards or charts) to support review meetings.
- Remove or replace KPIs only after careful evaluation and stakeholder agreement.
- Reassess KPIs annually to confirm continued alignment with the National Data Standards.



Key Message / Information

Reviewing and refining KPIs ensures they remain relevant, measurable, and aligned with the Entity's evolving needs and catalog usage maturity.

RACI Matrix – Document & Content Management KPIs

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	IT Team	Data Steward
6.1.A	Identify and Define Document & Content Management KPIs	I	A	R	R	C
6.1.B	Define KPI Details and Target Values	I	A	R	R	C
6.1.C	Maintain and Update the KPI Register	I	A	R	C	C
6.1.D	Review and Refine KPIs Periodically	I	A	R		C

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

Based on this Activity, the Entity can



Define KPIs Aligned With the National Data Standards



Track and Update DCM Tool Performance



Continuously refine KPIs to Stay Relevant and Effective

6.2 Document & Content Management Monitoring & Reporting

To ensure ongoing governance and performance improvement, the Entity must monitor its Document and Content Management tool regularly using the KPIs established in Section 6.1. Monitoring enables the Entity to track system usage, surface operational or compliance issues, and evaluate adoption trends across departments.

The National Data Standards require the generation of reports that compare actual performance against targets, log issues, and document how they are resolved. Entities are further expected to implement automated reporting tools that provide real-time dashboards, highlight bottlenecks, and offer data-driven insights into document usage, workflow performance, and user engagement.

This section outlines how the Entity can establish a practical monitoring process, document findings, and leverage dashboards and analytics tools to support transparent, real-time oversight of its document and content management environment.

Process – Document & Content Management Monitoring & Reporting

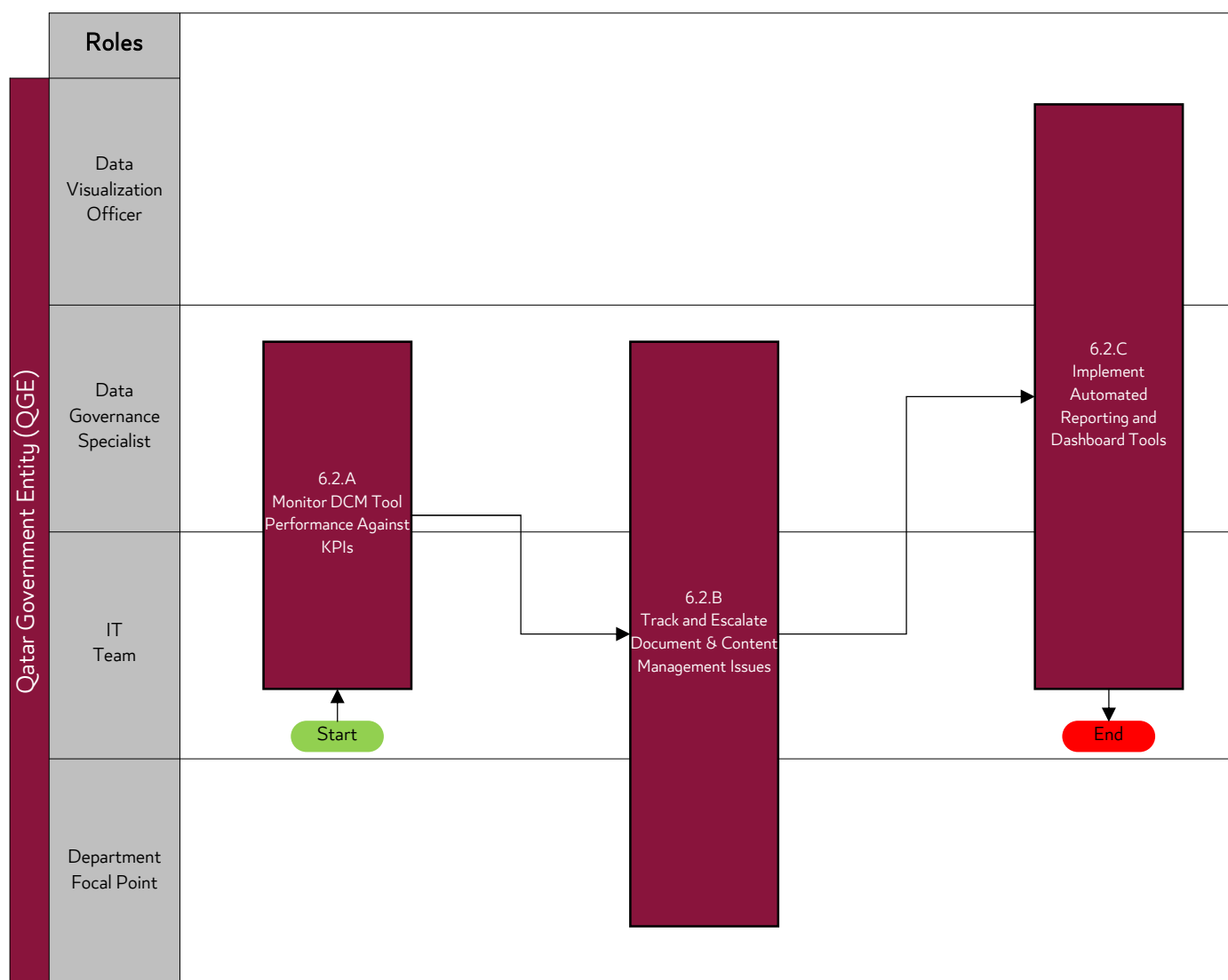


Figure 16: Document & Content Management Monitoring & Reporting Process Map

6.2.A

A

Monitor DCM Tool Performance Against KPIs: The Data Governance Specialist, in coordination with the IT Team, monitors system performance by tracking progress against the KPIs defined in Section 6.1. This supports compliance, visibility, and continuous improvement.

- i. **Generate regular performance reports:** Track usage and governance metrics on a quarterly basis.
 - a. **Pull data directly from the tool or reporting dashboard:**
 - Number of documents created
 - Number of active users
 - Paper-to-digital conversion rate
 - Workflow completion stats (if available)
 - b. **Compare performance against KPI targets:**
 - Use the KPI Register to compare actual results to defined targets
 - Mark each KPI as On Track, Off Track, or At Risk
 - c. **Highlight areas needing follow-up:**
 - Flag KPIs consistently below target (e.g., low adoption, overdue retention reviews)
 - Record notes or trends in the Comments section of the KPI Register
- ii. **Share monitoring outputs with governance leads:** Ensure visibility and actionability of reported insights.
 - a. **Summarize results in a one-page report or dashboard snapshot:**
 - Include trends, outliers, and highlights
 - Keep visuals simple: line charts, tables, stoplight status
 - b. **Submit to the Data Governance Office:**
 - Include the report in quarterly governance reviews
 - Use results to inform tool related improvement plans
 - c. **Store reports in a central location:**
 - Save performance reports in the governance SharePoint or documentation library
 - Maintain version control and access logs for audit trail

6.2.B

A

Track and Escalate Document & Content Management Issues: The Data Governance Specialist, in collaboration with the IT Team and relevant department focal points, tracks issues affecting the performance, usage, or governance of the document and content management tool. Escalation paths are used to ensure timely resolution and accountability.

- i. **Log issues related to document and content management:** Capture operational, user, and governance-related issues as they occur.
 - a. **Maintain a centralized issue log or tracker:**
 - Record issues such as broken workflows, misconfigured permissions, metadata errors, or untagged content
 - Include fields for issue description, affected department, reported date, and status
 - b. **Link issues to relevant KPIs when applicable:**
 - For example: if “Percentage of Tagged Documents” is falling, link the issue to incomplete metadata tagging
 - Use KPI deviations to identify and flag hidden issues
- ii. **Route issues to responsible units for resolution:** Ensure that each issue is owned, tracked, and resolved by the appropriate function.
 - a. **Assign each issue to a clear resolution owner:**
 - Example: Metadata errors → Metadata Specialist
 - Access issues → IT or Tool Administrator
 - b. **Track resolution progress and close-out actions:**
 - Mark issue status as Open, In Progress, Resolved, or Closed
 - Log resolution notes and any corrective actions taken

6.2.C
(1/2)

VA

Implement Automated Reporting and Dashboard Tools: The IT Team, with input from the Data Governance Specialist, and Data Visualization Officer, sets up automated reporting tools and dashboards to provide real-time insights into tool usage, performance, and governance compliance.

- i. **Enable automated data extraction from the DCM Tool:** Configure the tool or connected analytics tools to extract key metrics without manual intervention.
 - a. **Identify key metrics to be auto-reported:**
 - Document count by department or type
 - Workflow completion rates
 - Tagging completeness (e.g., % of documents with required metadata)
 - User activity logs (logins, edits, approvals)
 - b. **Schedule data pulls on a defined frequency:**
 - Weekly or monthly refresh depending on system performance
 - Sync data to a central repository, dashboard tool, or BI platform

6.2.C
Cont.
(2/2)

- ii. **Build and share interactive dashboards for key stakeholders:** Develop role-based views to help users and governance leads monitor performance.

a. **Create high-level dashboards for leadership:**

- Include adoption trends, top-performing departments, and off-track KPIs
- Use visual summaries (e.g., heat maps, trend lines, status indicators)

b. **Develop operational views for tool administrators:**

- Show metadata gaps, failed workflows, or expired retention tags
- Filter by content type, business unit, or time period

RACI Matrix – Document & Content Management Monitoring & Reporting

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	IT Team	Department Focal Points	Data Visualization Officer
6.2.A	Monitor DCM Tool Performance Against KPIs	I	A	R	R		
6.2.B	Track and Escalate Document & Content Management Issues			R	R	R	
6.2.C	Implement Automated Reporting and Dashboard Tools	I	A	R	R		R

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

Based on this Activity, the Entity can



Monitor Tool Performance



Track and Escalate DCM Issues

6.3 Document and Content Management SLAs

To ensure consistency, accountability, and reliability in the management of business-critical documents and content, the Entity must define and implement Service-Level Agreements (SLAs). These SLAs specify the expected performance levels for content accessibility, as well as escalation and remediation protocols when those expectations are not met.

The National Data Standards require SLAs to define which content is covered, what risks arise from non-compliance, and how performance will be measured and monitored. Entities are expected to further implement automated SLA monitoring tools that proactively track compliance and trigger alerts when issues occur.

This section outlines how the Entity can develop and enforce SLAs that are practical, measurable, and aligned with its document governance policies and system capabilities.

6.3.A
(1/2)

A

Establish SLAs with the DCM Tool Vendor: The IT Department, in coordination with the Procurement Team, Data Governance Specialist, and Legal Team, establishes formal Service-Level Agreements (SLAs) with the document and content management tool vendor. These SLAs define expectations for platform availability, support, performance, and security — and form part of the contractual obligations governing the service.

- i. **Define the scope of vendor SLA coverage:** Ensure the SLA focuses only on areas under the vendor's direct control.
 - a. **Limit SLA scope to system-level responsibilities:**
 - System uptime and availability
 - Data integrity, backups, and recovery
 - Performance (e.g., page load time, search latency)
 - Technical support response and resolution times
 - Security (e.g., access controls, encryption standards)
 - b. **Document the systems and services covered:**
 - Tool application
 - Integrated components (e.g., workflow engine, WCMS module)
 - Hosting, storage, or managed services (if applicable)
- ii. **Define measurable performance standards and thresholds:** Translate service expectations into specific, trackable metrics.
 - a. **Establish availability and performance metrics (illustrative):**
 - Example: "System uptime $\geq$ 99.9% per calendar month"
 - Example: "Document retrieval time $\leq$ 2 seconds for 95% of requests"
 - b. **Define backup and recovery SLAs (illustrative):**
 - Daily full backups with 7-day retention
 - Recovery Point Objective (RPO) $\leq$ 24 hours
 - Recovery Time Objective (RTO) $\leq$ 8 hours in disaster scenario

6.3.A
Cont.
(2/2)

c. Define support and incident response SLAs (illustrative):

- Critical issues: response within 1–2 hours
- Major issues: resolution within 1 business day
- Minor issues: resolution within 3–5 business days

iii. Establish escalation, reporting, and governance terms: Ensure issues are tracked, escalated, and addressed transparently.

a. Define notification protocols for SLA breaches:

- Require vendor to notify the Entity when a threshold is missed
- Document how issues will be logged, reported, and followed up

b. Include escalation and remediation procedures:

- Outline what happens if SLAs are consistently breached
- Escalate to vendor senior management and contract owner within the Entity

c. Define penalties or service credits (if applicable):

- Apply service credits or contract penalties for repeated non-compliance
- Allow for review and renegotiation after sustained underperformance

6.3.B

Implement Automated SLA Monitoring and Alerts: The IT Department, in collaboration with the tool Vendor, configures automated monitoring tools to track SLA compliance in real time. This reduces reliance on manual checks, speeds up incident detection, and ensures prompt response to service issues.

i. Configure automated SLA tracking tools: Use system-integrated tools or external monitoring platforms to track key SLA metrics.

a. Monitor uptime, latency, and availability in real time:

- Use built-in dashboards or third-party monitoring tools
- Track server response times, login success rates, and system uptime

b. Log and analyze platform events tied to SLA metrics:

- Record system outages, slow response times, and failed workflow executions
- Use metadata or tags to categorize incidents by SLA category

c. Enable system-level alerts for threshold breaches:

- Configure alerts when uptime, performance, or support timelines fall below the SLA standard
- Send alerts to designated IT owners and escalate automatically based on severity

VA

RACI Matrix – Document & Content Management SLAs

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	Legal Team	IT Team	Procurement Team
6.3.A	Establish SLAs with the DCM Tool Vendor	I	A	R	C	R	R
6.3.B	Implement Automated SLA Monitoring and Alerts	I	A			R	

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

Based on this Activity, the Entity can



Establish SLAs



Implement Automated SLA Monitoring

6.4 Document & Content Management Audit

To support transparency, accountability, and compliance, the Entity must be prepared to support both internal and external audits related to document and content management. This includes providing access to relevant records, documenting adherence to policies and standards, and offering clear evidence of governance activities. This section outlines how the Entity can develop compile relevant documentation.

6.4.A

Prepare Audit Evidence: The Data Governance Specialist, with support from the IT Team, prepares and provides structured documentation and system evidence to support internal or external audits related to document and content management.

- i. **Compile standard audit artifacts and documentation:** Ensure a consistent package of evidence is readily available for audits.
 - a. **Maintain a current Document & Content Management Plan:**
 - Confirm that the document & content management plan aligns with the national data standards and the internal document and content management policy
 - b. **Provide evidence of Inventory Assessment activities:**
 - Share the most recent inventory file from Section 4.1
 - Include metadata about systems, document types, volume, and ROT flags
 - c. **Include proof of DCM Tool configuration and implementation:**
 - Provide system screenshots or export logs
 - Record of digitized documents
 - d. **Provide DCM Tool performance and KPI reports:**
 - Share quarterly or monthly performance reports (as per 6.1 and 6.2)
 - Include KPI register and measurement logs
 - Attach governance meeting notes or improvement actions (if available)

RACI Matrix – Document & Content Management Audit

Indicative

Sr No.	Activity	Data Management and Security Director	Data Management and Governance Section Head	Data Governance Specialist	IT Team	Metadata Specialist	Data Steward
6.4.A	Prepare Audit Evidence	I	A	R	R	C	C

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

Based on this Activity, the Entity can



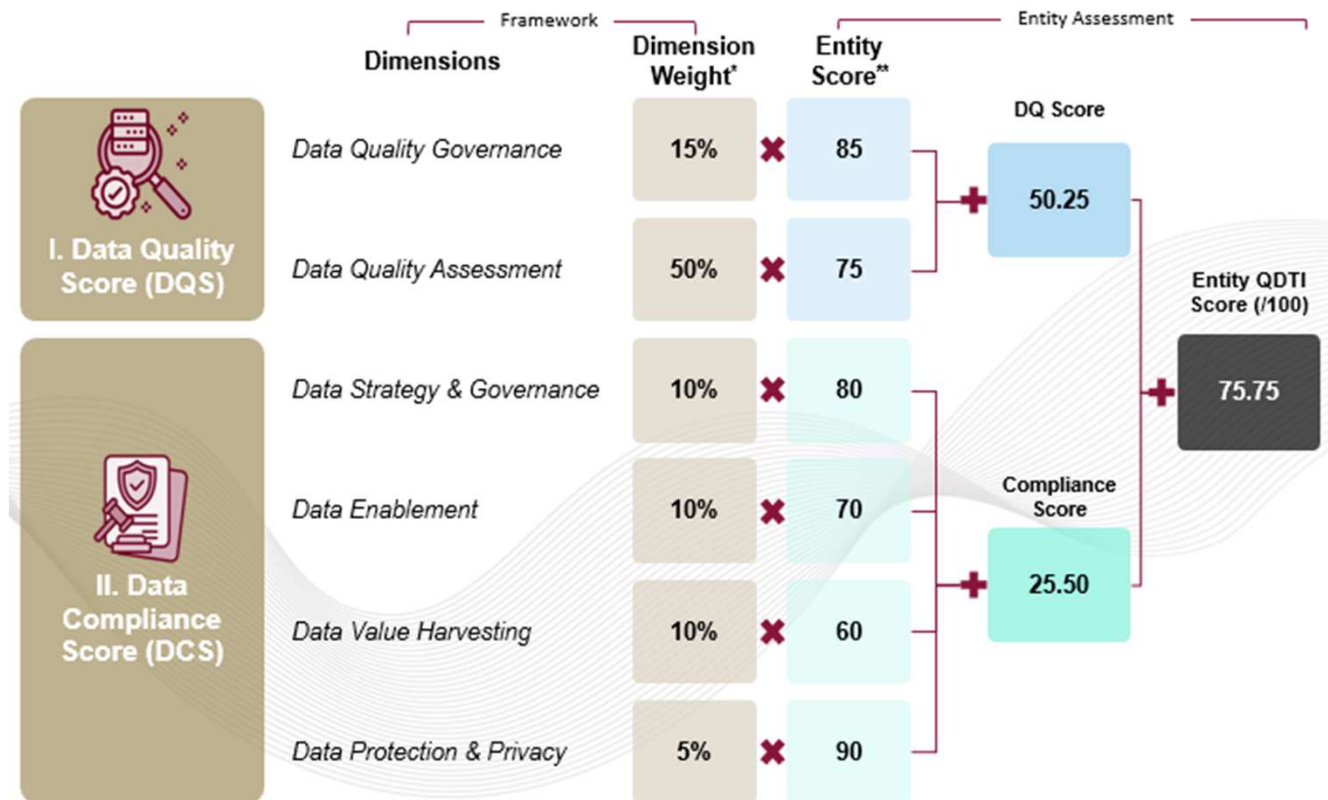
Prepare Audit Evidence

Legend: Capability Level **A** Advanced

6.5 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 17: Illustrative QDTI Scoring Methodology for an Entity

6.5.A

Initiate Document and Content Management 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 National Document and Content Management Standards.



Key Message / Information

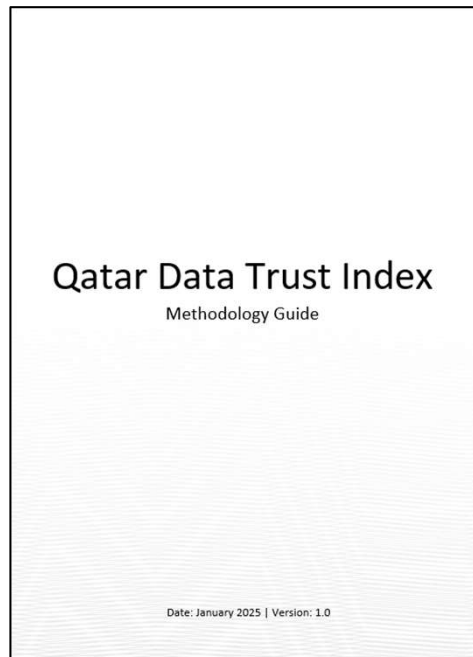
The Document and Content Management Domain falls under the Data Enablement Dimension in the National Data Management Framework and, consequently, within the QDTI Dimension.

6.5.B

Conduct Document and Content Management Assessment: Initiate the self-assessment to evaluate adherence to the National Document and Content Management 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	Specification
DQM	DQM.1.1: Data Quality Policy	As part of the Data Quality Policy control, the Entity shall establish and publish a Data Quality Management Policy.	DQM.1.1.1: Data Quality Policy Creation
DQM	DQM.1.1: Data Quality Policy	As part of the Data Quality Policy control, the Entity shall establish and publish a Data Quality Management Policy.	DQM.1.1.2: Data Quality Policy Publication
DQM	DQM.1.2: Data Quality Planning	As part of the Data Quality Planning control, the Entity shall profile its data and develop a data quality plan.	DQM.1.2.1: Data Profiling
DQM	DQM.1.2: Data Quality Planning	As part of the Data Quality Planning control, the Entity shall profile its data and develop a data quality plan.	DQM.1.2.2: Data Quality Plan

Control Specification	CapabilityLevel	Compliance
The Entity shall create a data quality policy in alignment with (NQAF) published by the NPC.	Foundational	Compliant
The Entity shall publish its data quality policy	Foundational	Compliant
The Entity shall identify CDEs and perform initial data profiling for the identified CDEs.	Foundational	Compliant
Based on the initial data profiling results, the Entity shall develop a data quality plan, in alignment with the Entity's data strategy.	Foundational	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.

6.5.C

Submit Document and Content Management Score to the DGO: Submit the Document and Content 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.

RACI Matrix - QDTI

Indicative

Sr No.	Activity	DGO	Data Management & Security Director	Data Management and Governance Section Head	Data Compliance Specialist	Data Governance Specialist
6.5.A	Initiate Document and Content Management Compliance Assessment		I	A	R	
6.5.B	Conduct Document and Content Management Assessment		I	A	R	C
6.5.C	Submit Document and Content Management 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 DCM Compliance Score

7. Appendix



7.1 Templates and Frameworks

Asset No.	Asset Name	Description	File Name
1	Document and Content Management Policy Template	Template containing a sample table of contents the Entity can refer to when drafting its policy.	NPC_DGO_QDKC_DCM_Document & Content Management Policy Template
2	Data Management Policy Communication Email Template	Template containing a sample email the Entity can use to announce the publishing of the new policy.	NPC_DGO_QDKC_General_Data Management Policy Communication Email Template
3	Initiative Card Template	Template used to outline and track the details of a specific initiative.	NPC_DGO_QDKC_General_Initiative Card Template
4	Data Management Domain Plan Template	Template that helps the Entity capture an overview of identified initiatives, detail their sub-activities, owners, stakeholders, and activity timeframe.	NPC_DGO_QDKC_General_Data Management Domain Plan Template
5	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
6	Inventory Assessment Template	Template can be leverage by entities to evaluate the current state of their document and content management systems	NPC_DGO_QDKC_DCM_Inventory Assessment Template
7	Document & Content Prioritization Template	Template helps entities identify and prioritize key documents and content assets for management, digitization, or migration to a document management system.	NPC_DGO_QDKC_DCM_Document & Content Prioritization Template
8	Workflow Prioritization Template	Template enables entities to identify and rank workflows that are candidates for automation within a Document and Content Management System.	NPC_DGO_QDKC_DCM_Workflow Prioritization Template
9	DCM Tool Selection Criteria Template	Template that helps the Entity document mandatory and additional document & content tool features, list various tool options, and specify feature and cost weightings	NPC_DGO_QDKC_DCM_Tool Selection Criteria Template

Asset No.	Asset Name	Description	File Name
10	Data Management KPIs Register Template	Template containing a table that helps the Entity define KPIs.	NPC_DGO_QDKC_General_Data Management KPIs Register Template
11	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
12	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



المجلس الوطني للتخطيط
National Planning Council

دولة قطر • State of Qatar