An Enterprise Cryptography Policy

Securing Digital Trust Infrastructure

Version 3.0

Prepared by **Louise Davey | LDIQ**

August 19, 2026

Preface

This document is a broadly shareable board-level policy template for governing cryptography as critical digital trust infrastructure. It is intended to accelerate the development of cryptographic policy within organizations that do not yet have one, and to provide a benchmark for organizations seeking to strengthen an existing policy.

The policy is designed for medium and large organizations in financial services, government, healthcare and other regulated or critical sectors. It governs cryptography across enterprise information technology (IT), operational and embedded technology (OT), and third-party or externally operated technology on which these types organizations depend.

This policy establishes enterprise level accountability and requirements. It defines what must be true. The implementation details belong in downstream Directives, Standards, Operational Procedures, and transformation programs managed by accountable functions.

The policy is durable. It is designed to govern the organization's cryptographic capability through steady-state operations and through periods of major change. Post-quantum cryptography (PQC) migration is therefore treated as a major current transformation within an enduring cryptographic-governance mandate, not as the reason the policy exists.

How to Use This Document

This document represents a "worked example" baseline template. Before adoption, the organization should adapt it to its structure, operating model, technology estate, risk profile, and regulatory obligations. The adaptation process should include:

1. Confirm the assignment of 1A and 1B responsibilities, particularly the CIO/CISO operating split, and the ownership of cryptography in OT and embedded technology.
2. Map the governance bodies referenced in this policy to the organization's existing committee structure.
3. Map the requirements in Section 7 to an appropriate Directive and Standard architecture.
4. Identify and integrate organization-specific legal, regulatory, records-retention, privacy, resilience, and sector obligations that affect cryptographic practice.
5. Confirm the interfaces between this policy and existing policies such as security, architecture, data, operational resilience, procurement, privacy, legal, clinical/biomedical, facilities, and third-party risk.

Copyright and Contact Information

For questions, feedback, or assistance adapting or implementing this policy, contact Louise Davey at louise@ldiq.ca.

History and Acknowledgements

Version 1 of this policy was inspired in part by the Dutch *Framework Cryptography Policy for the Central Government*, originally shared with me by **Pieter Schneider**. That framework provided a valuable reference point for structuring enterprise cryptography governance requirements and was the catalyst for developing the first version of this policy.

Version 1 was intentionally an early iteration and was published on **March 3, 2026**.

➔ Framework Cryptography Policy for the Central Government | Netherlands

---

Version 2 introduced more professional formatting and sharpened several concepts and requirements as the work continued to evolve. Discussion, knowledge sharing and emerging practices across the broader professional community, including through LinkedIn, were an important source of challenge and learning during this period. The catalyst for this version came from **Moona Ederveen-Schneider**, who told me she was incorporating links to the policy into her training materials. That was the moment I realized the document had moved beyond a prototype and was beginning to be used as a reference.

Version 2 was published on **July 5, 2026**.

Version 3 (this document) was significantly strengthened through knowledge sharing and collaboration with **Shayne de la Force** following the publication of Version 2.

Shayne and **LFI's** work on an industry-specific cryptography policy for advanced manufacturing helped sharpen my thinking around operational technology, embedded systems, long-lived assets, cryptographic stranding and supply-chain dependencies. The two documents are being released together on **August 19, 2026**. Our two policies are intended to be complementary. This policy is written primarily for information-driven and regulated sectors such as **financial services, government and healthcare**, while the LFI policy addresses cryptography across the **industrial enterprise, the plant and the product**. They share the same governance foundation while extending it into different operating environments.

➔ An Industrial Cryptography Policy — Advancing Industrial Economics with Quantum | LFI

Next Version? Never say never, but I do not expect another major version for some time. Version 3 represents a mature and substantially complete expression of the governance model. From here, I expect the more important work will be applying it, challenging it in practice, and allowing new standards, technologies and operating experience to reveal where it eventually needs to evolve.

Table of Contents

Assumptions

This policy is built on the structural assumptions below. Organizations should review them carefully and adjust the policy where their organizational context differs.

Assumption 1: Three Lines Model

This policy strictly adheres to the Three Lines of Defense Risk Management Framework that separates operational ownership, risk oversight, and independent assurance. An overview of the Three Line of Defense model is provided in the Annex. The Three Line of Defense model is widely used in risk sensitive industries. For practical operating clarity, this policy further distinguishes between First Line of Defense 1A and 1B accountabilities

Governance consideration	Like data, cryptography is a complex asset to manage. A lack of clarity in how First-Line responsibilities are divided around it is a frequent source of friction. The most important questions are who operates the cryptographic estate, who sets and monitors the standards, and who owns remediation when requirements are not met

Assumption 2: CIO and CISO Roles

This policy assumes the CISO occupies a 1B role, and the CIO occupies a 1A role in relation to cryptography. Under this assumption, the CIO function operates the enterprise cryptographic estate, while the CISO function sets standards, monitors compliance, and challenges execution without operating the estate it oversees.

Adaptation requirements	The positioning and responsibilities of the CISO function varies across organizations. In some, the CISO function takes on certain 1A responsibilities for cryptography, operating certificate or key-management infrastructure. In others the CISO function sits in the second line of defense. You will need to adapt this policy accordingly if your CISO does not occupy the clean 1B role laid out for them in this version of the policy.

Assumption 3: Ownership of OT and Embedded Technology

This policy is designed primarily for information-driven sectors, including financial services, government and healthcare. Its principal focus is therefore cryptography within Information Technology environments. However, its governance requirements also apply to Operational Technology and embedded technology where cryptography is used to support the organization's operations, services or mission.

Adaptation requirements	The relative presence of OT and embedded technology varies across sectors and organizations. It may reside within Technology, Facilities, Operations, Clinical or Biomedical Engineering, Physical Security, Laboratory Operations, or another function. Organizations with a significant OT or embedded technology estate may require more extensive cryptographic governance, standards, controls, and lifecycle requirements for those environments.

Assumption 4: Board Governance Bodies

This policy assumes that the Board Risk Committee is responsible for technology and cyber-risk oversight.

Adaptation requirements	Some organizations may have a specific IT or Technology Committee at the Borad level. In this case, this policy will need to be adopted to reflect the different risk oversight responsibilities of the different committees.

Assumption 5: Policy Hierarchy

This policy assumes governance document hierarchy where policies sit at the top of the hierarchy. It does not go into the technical or operational specific of the cryptographic estate (algorithms, parameters, protocols, migration sequences, and technical timelines). These details are left to downstream Directives, Standards and Procedure documents that are used to operationalize this policy.

1. Context: Why We Need this Policy

Digital trust is a critical asset without which an organization cannot effectively operate in the digital age. Cryptography is foundational infrastructure for that trust, protecting the confidentiality, integrity, authenticity, and reliability of information, identities, communications, transactions, software, devices, and records.

Given its critical role and pervasive nature across the organization, cryptography must instead be governed at the enterprise level, with the same discipline applied to other critical assets and capabilities such as data, technology, human capital, and financial resources.

This need is becoming more urgent as organizations undertake post-quantum cryptography (PQC) migrations. These programs are necessary, complex, and multi-year, but they are also transitional. The need to govern cryptography does not end when vulnerable algorithms have been replaced. Algorithms, standards, technologies, suppliers, threats, and regulatory expectations will continue to evolve.

This policy establishes the permanent governance model that is necessary to support the transformation and institutionalize sound cryptographic practices for the long term.

Establishing enterprise policy is therefore foundational. It defines ownership, accountability, risk expectations, minimum requirements, and decision rights across the organization. Only once these expectations are formally established can the second and third lines effectively perform their respective oversight, challenge, assurance, and audit responsibilities that ensure that cryptographic governance and management become a permanent capability.

2. Purpose

The purpose of this policy is to govern cryptography as critical digital trust infrastructure and an enduring enterprise capability. It establishes the requirements necessary to protect the confidentiality, integrity, authenticity, non-repudiation, and long-term trustworthiness of the organization's data, identities, transactions, communications, operations, and records, while ensuring that cryptography can evolve as threats, technologies, and standards change without destabilizing critical operations.

To that end, this policy:

- establishes board-level oversight and executive accountability for cryptography as an enterprise capability;
- defines enterprise expectations for governing cryptography across technology environments and third-party dependencies;
- establishes requirements for cryptographic discovery, inventory, dependency mapping, lifecycle management, and crypto-agility, including the prevention of cryptographically stranded critical assets;
- governs PQC transition and other cryptographic transformation as executive-led, risk-prioritized, and assured activity; and
- requires cryptographic decisions to remain consistent with legal, regulatory, privacy, resilience, sovereignty, and operational constraints.

3. Principles

These principles establish the enduring foundations for how cryptography is governed across the organization. They guide interpretation of this policy, support consistent decision-making where detailed requirements may not address every circumstance, and ensure that cryptographic governance remains aligned with our digital trust objectives as technologies, threats, and standards evolve.

3.1 Cryptography as Foundational Infrastructure

Cryptography is not merely a security control. It is foundational digital trust infrastructure: the mechanism by which the organization protects and verifies data, identities, transactions, communications, software, devices, and records. Digital trust is a critical business asset. Weakness, compromise, or obsolescence in cryptographic mechanisms can undermine that trust and create operational, financial, legal, regulatory, safety, and reputational consequences.

3.2 Enterprise Accountability and Risk-Based Governance

Cryptography must be governed as an enterprise capability, with decisions informed by business context and risk. Cryptographic priorities and decisions must consider factors such as asset and service criticality, expected service life, data retention periods, exposure, legal and regulatory obligations, dependency constraints, risk tolerance, and acceptable disruption. Accountability must extend beyond technology and cybersecurity functions to the appropriate business, risk, operational, and executive stakeholders.

3.3 Crypto-Agility and Lifecycle Management

Cryptographic mechanisms must be discoverable, manageable, and capable of being replaced or upgraded as threats, technologies, and standards evolve. Cryptography must be governed throughout its lifecycle, from selection and implementation through operation, maintenance, migration, and retirement. Critical assets must not become cryptographically stranded because their cryptographic mechanisms cannot be identified, upgraded, replaced, or otherwise remediated within their required service life.

3.4 Resilience Across the Extended Enterprise

Cryptographic change must be managed in a manner that preserves the resilience and continuity of critical operations. The organization must consider cryptographic dependencies across enterprise technology, operational and embedded environments, third parties, suppliers, platforms, software, hardware, and other external dependencies. Reliance on third parties does not transfer accountability for cryptographic risk.

3.5 Permanent Governance and Assurance

PQC migration and other major cryptographic transformations are transitional initiatives within a permanent enterprise cryptographic governance capability. The organization must maintain ongoing governance, oversight, evidence, challenge, and assurance so that cryptographic risks and future changes in algorithms, standards, threats, technologies, and regulatory expectations can be managed in a controlled, accountable, and repeatable manner.

4. Scope and Governance Interfaces

4.1 In Scope

4.1.1. Cryptography is in scope where it supports, protects, or enables the technologies, is embedded in systems, products, services, or operational tools used to execute the organization's mission, deliver its services, support its operations, or meet its legal and regulatory obligations.

Accordingly, the policy applies to cryptography used across the organization's technology estate, including:

- enterprise information technology and applications;
- cloud, platform, infrastructure, and managed services;
- operational technology and embedded technology;
- products, devices, equipment, and other long-lived technology assets;
- data, identity, authentication, communications, transactions, software, and digital records;
- cryptographic keys, certificates, trust anchors, algorithms, protocols, libraries, and cryptographic services;

- development, integration, deployment, and technology management practices that introduce or depend upon cryptography; and
- third-party products, services, platforms, suppliers, and other external dependencies where the organization relies on cryptography to protect or sustain its operations, information, or digital trust.

4.1.2. Scope is determined by the organization's reliance on cryptography, not by organizational ownership or technology classification. Where cryptography supports a critical business capability, service, asset, obligation, or dependency, the associated cryptographic mechanisms and dependencies are subject to this policy.

4.1.3. The policy applies regardless of whether cryptographic capabilities are developed internally, acquired commercially, delivered as a service, embedded within technology, or managed by a third party.

4.1.4. The requirements of this policy apply proportionately based on factors such as business criticality, information sensitivity, expected service life, retention requirements, exposure, dependency risk, legal and regulatory obligations, and the potential consequences of cryptographic failure or obsolescence.

4.2 Out of Scope

The presence of cryptographic material within a broader control domain does not, by itself, bring that domain into scope. Questions regarding the inclusion or exclusion of cryptographic elements must be evaluated through the exception process detailed later in the document.

4.3 Governance Interfaces

This policy operates within the organization's broader governance framework. Where cryptography intersects another governance domain, this policy governs the cryptographic requirements and associated risks, while established authorities remain accountable for their respective domains. Applicable functions must coordinate to ensure requirements are integrated without duplication, conflict, or gaps in accountability across the governance framework.

5. Governance

Cryptography is governed as a cross-enterprise digital trust capability requiring coordinated accountability across business, technology, operational, security, procurement, risk, legal, and assurance functions.

5.1 Board Oversight

The Board of Directors holds ultimate oversight accountability for the integrity and resilience of the organization's cryptographic estate. The Board Risk Committee must satisfy itself that:

- enterprise-wide visibility exists over cryptographic assets and dependencies, including material OT and third-party dependencies;

- critical systems and services have viable cryptographic lifecycle and crypto-agility paths;
- management has a credible, funded plan to address cryptographic obsolescence and transition within regulatory and risk-acceptable timelines;
- cryptographically stranded and potentially stranded critical assets are identified, risk-assessed, and subject to remediation or accepted risk;
- third-party and supply-chain cryptographic dependencies are effectively governed;
- cryptographic sovereignty and jurisdictional exposures are understood where material; and
- applicable legal, regulatory, privacy, resilience, and records obligations are being met.

The Board Risk Committee reviews this policy at least annually or on material change in the cryptographic threat landscape, regulatory environment, standards environment, or enterprise architecture, and recommends approval to the Board where required by the organization's governance model.

5.2 Executive Management

Executive management is accountable for translating board oversight into organizational action. It allocates resources, sets direction, resolves cross-functional priorities, and makes material investment and risk-acceptance decisions required to maintain cryptographic resilience.

Executive management must ensure that cryptographic transformation is treated as an enterprise change agenda rather than a narrowly scoped security project when the scale, dependencies, or business impact warrant that treatment.

5.3 Operational Governance Bodies

5.3.1 Technology Risk Committee

- oversees enterprise cryptographic risk posture;
- oversees PQC readiness and other cryptographic transformation;
- reviews stranded-asset exposure and remediation;
- reviews regulatory and third-party cryptographic risk;
- escalates material risk and investment decisions to executive management or the Board as appropriate.

5.3.2 Security Architecture Review Board

- approves enterprise cryptographic standards;
- approves cryptographic inventory frameworks and taxonomy;
- approves crypto-agility and lifecycle requirements;
- reviews architecture exceptions and significant cryptographic design decisions;

- ensures standards apply coherently across enterprise IT, OT/embedded technology, and third-party technology.

5.3.3 Third-Party Risk Committee

- oversees cryptographic expectations across the vendor ecosystem;
- monitors material supplier dependencies and cryptographic lock-in;
- reviews suppliers lacking credible cryptographic modernization paths;
- escalates systemic supplier risk into the enterprise risk framework.

6. Roles & Responsibilities: Three Lines Model

Adaptation requirements	The roles below preserve the 1A/1B operating distinction used in this policy. Organizations should map these roles to their actual functions without weakening separation between operation, control, independent oversight, and assurance.

6.1 First Line: Operational Ownership (1A)

6.1.1 Lines of Business and Support Functions (1A)

Lines of business and support functions provide the context needed to determine where cryptographic protection is essential and where cryptographic failure, obsolescence, or loss of trust would create material enterprise risk.

- Identify and classify long-lived confidential information and records within their domains.
- Identify processes and services where cryptographic failure or loss of trust creates material business, legal, safety, service-delivery, or reputational impact.
- Provide retention, criticality, service-level, and impact context for prioritization.
- Participate in remediation, migration, testing, and risk-acceptance decisions affecting their processes.
- Identify critical business services and dependencies that could become operationally unviable as a result of cryptographic obsolescence or inability to remediate dependent assets.

6.1.2 Technology Ownership - Enterprise IT (1A)

The Technology function owns and operates cryptography across the enterprise IT estate this includes all data and electronic records.

- Implement approved cryptographic standards across systems and infrastructure.
- Operate enterprise key and certificate lifecycle infrastructure.
- Maintain the enterprise IT portion of the cryptographic inventory and dependency map.

- Ensure systems support cryptographic lifecycle management and practical crypto-agility.
- Identify assets that are cryptographically stranded or at risk of becoming stranded.
- Execute remediation, modernization, algorithm replacement, and PQC migration.
- Produce operational evidence and reporting on posture, coverage, exceptions, and remediation.

6.1.3 Operational and Embedded Technology Ownership (1A)

Additional Information	The function designated by the organization owns and operates cryptography across OT and embedded technology within its domain. This may include operational systems such as ATM and POS, medical or laboratory devices, facilities systems, physical-security systems, specialized appliances, IoT/edge devices, and other long-lived or vendor-controlled technology.

The line of business or support functions are responsible for OT and embedded technology supporting operational activities under their domain.

- Maintain the OT/embedded portion of the cryptographic inventory, including device identity, firmware/code signing, remote-access dependencies, certificates, protocols, and vendor dependencies where applicable.
- Apply approved standards where technically and operationally feasible, and document constraints where they are not.
- Ensure cryptographic change enters the appropriate operational, clinical, safety, maintenance, and change-control processes before implementation.
- Identify unsupported, unpatchable, vendor-locked, or otherwise cryptographically stranded assets and escalate their risk.
- Plan cryptographic lifecycle requirements jointly with asset replacement and capital planning.
- Ensure operational resilience is preserved during cryptographic remediation or migration.

6.2 First Line: Security and Procurement Controls (1B)

6.2.1 Information Security Control Ownership (1B)

The Information Security function defines, maintains, and monitors enterprise cryptographic standards across the cryptographic estate, including IT, OT, embedded and third parties.

- Define enterprise cryptographic standards and submit them for approval.
- Maintain approved algorithm, protocol, library, service, and parameter requirements.
- Monitor compliance and exposure to weak, deprecated, or non-standard cryptography.
- Define crypto-agility, lifecycle, discovery, inventory, and dependency-mapping requirements.

- Establish enterprise strategy for cryptographic modernization, including PQC transition.
- Assess cryptographic risk in vendor solutions and modernization roadmaps.
- Independently assess cryptographic posture and escalate material gaps.
- Define standards for identifying and classifying cryptographically stranded assets.
- Support all other functions in determining the technical adequacy of the cryptographic systems within their respective domains.

6.2.2 Procurement and Supply Chain Control Ownership (1B)

Procurement ensures that cryptographic requirements are embedded in contracts and supplier lifecycle processes.

- Embed cryptographic requirements into procurement criteria, contracts, renewals, and supplier onboarding.
- Require supported cryptographic upgrade paths, lifecycle commitments and supplier migration roadmaps where readiness cannot yet be demonstrated.
- Require notification of material cryptographic vulnerabilities, deprecations, library changes, and end-of-support conditions.
- Preserve contractual rights to require cryptographic upgrades within defined timelines.
- Identify and escalate supplier dependencies that create unacceptable cryptographic lock-in or stranded-asset risk.

6.3 Second Line: Risk Oversight

The Risk Management function (2LoD) provides independent oversight of enterprise cryptographic risk.

- Ensure cryptographic risk appetite and tolerance are established within the enterprise risk framework.
- Monitor enterprise cryptographic exposure, including stranded-asset, third-party, HNDL, TNFL, and PQC transition risk.
- Challenge First-Line execution where risk thresholds are exceeded or remediation is inadequate.
- Provide oversight of cryptographic transformation initiatives
- Identify and monitor applicable laws, regulations, and regulatory guidance relating to cryptography.
- Ensure material regulatory changes are translated into standards, priorities, and governance decisions.
- Report cryptographic related risk to the Board in accordance with the organizational governance model.

6.4 Third Line: Internal Audit

Internal Audit provides independent assurance that cryptographic governance, controls, and operational practices are effective.

- Verify compliance with this policy and downstream directives and standards.
- Review discovery, inventory, and dependency-management practices.
- Assess key and certificate management controls.
- Evaluate crypto-agility and cryptographic lifecycle capability.
- Review cryptographically stranded asset identification and remediation governance.
- Review PQC and other cryptographic transformation programs.
- Assess third-party and regulatory compliance evidence.
- Report independently to the Board or its Audit Committee in accordance with the organization's governance model.

6.5 Delivery Partners

Any externally developed methodology or tooling must operate within the requirements, decision rights, and evidence expectations established by this policy and its downstream governance.

Specialist delivery partners may support internal functions in the design, discovery, implementation, migration, tooling, assurance preparation, or operational execution. However, they may never substitute for the organization's policy accountability.

7. Requirements

The requirements below establish governed outcomes. Each requirement must be operationalized through downstream Directives and Standards owned by the accountable functions. A single Directive may address more than one requirement.

7.1 Cryptographic Standards

All cryptographic implementations must comply with enterprise standards approved by the Security Architecture Review Board or equivalent authority. Standards must cover, as applicable: approved algorithms and protocols; minimum key sizes and parameters; randomness; approved libraries and services; key and certificate lifecycle practices; trust anchors; code and firmware signing; cryptographic requirements for device and service identity; and migration/deprecation rules.

Standards must be reviewed regularly and updated when algorithms are deprecated, vulnerabilities are discovered, authoritative guidance changes, or new regulatory requirements arise. The Information Security function 1B maintains the standards; the relevant 1A owner implements them.

7.2 Cryptographic Discovery, Inventory, and Dependency Mapping

The organization must maintain the capability to discover cryptographic use, maintain an authoritative enterprise cryptographic inventory, and map material cryptographic dependencies to the systems, services, business processes, data, and third parties that rely on them.

The enterprise cryptographic inventory must be sufficient to identify exposure rapidly when an algorithm, protocol, library, certificate class, trust anchor, or supplier implementation becomes vulnerable or deprecated.

For material assets, the inventory must record or link to:

- algorithms and protocols in use;
- cryptographic libraries, modules, and services;
- keys, certificates, and trust anchors where relevant;
- hardware security modules and other cryptographic hardware;
- embedded cryptography in applications, infrastructure, devices, OT, and third-party products;
- asset owner and accountable cryptographic owner;
- critical business process or service dependencies;
- data sensitivity and retention requirements where relevant;
- expected service life or planned retirement date for long-lived assets;
- vendor support and cryptographic upgrade path; and
- known constraints that may create cryptographically stranded-asset risk.

7.3 Key and Certificate Lifecycle Management

All cryptographic keys and certificates must be generated, stored, distributed, used, rotated, renewed, revoked, archived, and retired according to enterprise standards. The organization must maintain authoritative lifecycle visibility sufficient to prevent expiry, orphaned material, unmanaged trust anchors, and uncontrolled cryptographic dependencies.

Signing keys and certificates used for long-lived document, code, firmware, transaction, device, or record integrity must be assessed for TNFL exposure and for the duration over which trust must remain verifiable.

7.4 Crypto-Agility and Cryptographic Lifecycle Resilience

The organization must maintain the technical and organizational capability to change cryptography without disproportionate redesign or disruption. Crypto-agility requirements apply to algorithms, protocols, parameters, keys, certificates, cryptographic libraries/modules, trust services, and material supplier dependencies.

For critical systems and services, the organization must be able to demonstrate a supported, authorized, and operationally viable change path during the expected service life of the asset. Technical replaceability alone is insufficient if the organization lacks the supplier rights, maintenance path, decision process, funding, or operational window needed to execute the change.

7.5 Cryptographically Stranded Assets

The organization must identify, govern, and reduce exposure to cryptographically stranded and potentially stranded assets. A critical asset must be classified as potentially stranded when its expected service life extends beyond the period in which its cryptography is expected to remain supportable, or when no credible upgrade, replacement, or compensating-control path exists.

For each material stranded or potentially stranded asset, the accountable 1A owner must establish one of the following:

- a funded remediation or upgrade plan;
- a replacement or retirement plan aligned with the asset lifecycle;
- a supplier-supported modernization path with defined dates and obligations; or
- a formally approved risk-acceptance decision with compensating controls and a time-bound review.
- New procurement and architecture decisions must seek to prevent the creation of additional cryptographically stranded critical assets.

7.6 Post-Quantum Cryptography Readiness

The organization faces a defined transition requirement to replace quantum-vulnerable public-key cryptography in accordance with applicable standards, regulatory guidance, and risk-based timelines. HNDL and TNFL exposure begin before a cryptographically relevant quantum computer exists and must therefore be considered in current prioritization.

- Quantum-vulnerable assets and dependencies must be identifiable through the enterprise cryptographic inventory.
- PQC transition must be integrated into enterprise technology, OT/embedded technology, procurement, and third-party roadmaps.
- Long-lived confidential information and long-lived signed material must be prioritized according to exposure period and business impact.
- Critical systems that cannot support required cryptographic change must be treated as stranded-asset risks.
- The Technology Risk Committee oversees transition prioritization and progress.
- Material progress and risk must be reported to the Board Risk Committee.

7.7 Operational and Embedded Technology Cryptography

Cryptography in OT and embedded technology must be governed with the same enterprise standards and risk principles as enterprise IT, while recognizing that change may be constrained by operational continuity, safety, clinical use, certification, maintenance windows, vendor control, and long asset lifecycles.

The organization must, where applicable:

- maintain visibility of cryptography used for device identity, authentication, remote access, secure communications, firmware/code signing, update integrity, and certificates;
- identify legacy or proprietary protocols that cannot meet current standards;
- ensure cryptographic changes enter established operational, clinical, safety, and change-control processes;
- plan cryptographic modernization jointly with asset-management and capital-replacement planning;
- avoid treating OT cryptographic remediation as routine enterprise IT patching when the operational risk profile differs;
- require vendor-supported upgrade paths for newly procured long-lived technology; and
- escalate unsupported or unchangeable cryptography as stranded-asset risk.

7.8 Third-Party and Supply-Chain Cryptographic Dependency

The organization must maintain governance over material cryptographic dependencies inherited through third parties, including cloud services, SaaS, managed services, platforms, appliances, devices, software components, and outsourced infrastructure.

Where suppliers cannot fully disclose embedded cryptography, the organization must apply a risk-based disclosure and remediation approach rather than assume absence of risk. Material suppliers must provide sufficient information and contractual commitments to support vulnerability response, algorithm deprecation, PQC migration, lifecycle management, and exit or replacement decisions.

7.9 Cryptographic Sovereignty and Jurisdictional Exposure

The organization must assess material cryptographic dependencies for sovereignty and jurisdictional exposure where these could affect its ability to preserve control, continuity, confidentiality, or freedom of action.

Assessments should address, where relevant:

- jurisdiction over key-management and trust infrastructure;
- control over root trust, certificate authorities, identity trust services, and cryptographic administration;

- ability to replace suppliers, trust services, or cryptographic components without unacceptable disruption;
- hardware, software, and service origin where law, regulation, national-security, sector, or procurement rules make origin material;
- legal or contractual rights that could affect access to, control of, or continuity of cryptographic services; and
- supplier concentration or lock-in that could impair cryptographic modernization.

Sovereignty requirements must be proportionate to the organization's sector, jurisdiction, criticality, and legal obligations. They are not intended to mandate domestic sourcing where no such requirement exists.

7.10 Regulatory, Legal, Privacy, and Records Compliance

Cryptographic governance must comply with applicable laws, regulations, regulatory guidance, privacy requirements, records-retention obligations, and evidentiary requirements across all jurisdictions in which the organization operates. Where an applicable requirement is stricter than this policy, the stricter requirement prevails.

The Risk Management function 2LoD is responsible for identifying and monitoring applicable requirements and ensuring they are escalated into governance. Legal, Privacy, Compliance, and Records functions provide authoritative interpretation within their domains. Information Security 1B translates requirements into standards; the accountable 1A function implements them and produces evidence of operational compliance.

7.11 Operational Resilience, Continuity, and Recoverability

Cryptographic failure must be treated as a distinct operational resilience scenario. Continuity and recovery planning must consider compromise, loss, expiry, deprecation, unavailability, or forced replacement of cryptographic keys, certificates, algorithms, trust services, and critical supplier cryptography.

- Critical key material and cryptographic configurations must be included appropriately in backup and recovery.
- Encrypted and signed archived information must remain accessible and verifiable for its required retention period.
- Critical trust services must have recovery procedures proportionate to business impact.
- Business continuity plans must account for cryptographic incidents that disrupt authentication, communications, transactions, software trust, device trust, or data access.
- Recovery and migration paths for high-impact cryptographic failure scenarios must be tested on a risk-based basis.

7.12 Personnel and Capability

The organization must ensure that personnel with cryptographic design, implementation, operation, procurement, risk, or oversight responsibilities are appropriately qualified and current. Training and capability requirements must be reviewed at least annually and updated as standards, threats, regulation, and technology change.

External expertise may be used where needed, but accountability remains with the organization and the designated internal owner.

7.13 Monitoring and Reporting

The organization must maintain continuous visibility over its cryptographic posture. Monitoring is an operational responsibility of the relevant 1A owner. Reporting to governance bodies is shared between 1A operational owners and Information Security 1B, with 1B providing independent assessment rather than relying solely on operational self-reporting.

Monitoring must cover, at a minimum:

- discovery and inventory coverage and completeness;
- key and certificate lifecycle compliance;
- exposure to deprecated, vulnerable, or non-standard cryptography;
- HNDL and TNFL exposure for long-lived information and signed material;
- PQC transition progress;
- crypto-agility and lifecycle capability;
- cryptographically stranded and potentially stranded critical assets;
- OT/embedded technology cryptographic constraints and remediation;
- third-party cryptographic dependencies and supplier modernization readiness;
- cryptographic sovereignty exposures where material; and
- regulatory and policy compliance posture.

Reporting must be provided to the Technology Risk Committee on a defined cadence and to the Board Risk Committee at least annually or on material change in cryptographic risk posture.

7.14 Cryptographic Incident Response

The organization must maintain a defined and tested capability to respond to cryptographic incidents. A cryptographic incident includes, but is not limited to: compromise of a key, certificate, trust anchor, or cryptographic service; disclosure of a critical algorithm, protocol, or library vulnerability; unexpected deprecation; cryptographic supplier failure; confirmed or suspected exfiltration of material subject to HNDL or TNFL risk; or discovery of a critical asset that can no longer maintain required cryptographic protection.

Information Security 1B defines incident classification and response standards and triggers the response process. The relevant 1A function executes operational remediation. Risk Management 2LoD manages enterprise escalation and regulatory-notification governance where applicable. Material incidents must be escalated to the Technology Risk Committee and, where impact warrants, to the Board Risk Committee.

8. Governing Cryptographic Transformation

Cryptographic transformation is a recurring enterprise capability. PQC migration is the largest current example, but future algorithm failures, standards changes, supplier events, and technology shifts will require additional transformation. This policy governs such transformation as an activity within the organization's enduring cryptographic mandate.

Any material cryptographic transformation must be governed against the following expectations:

- **Executive mandate and prioritization.** Transformation proceeds under an explicit mandate with funding and prioritization grounded in risk, criticality, service life, exposure period, regulatory timeline, and operational constraints.
- **Executive decision-making.** Material decisions about scope, sequencing, investment, and residual risk are made by accountable executives and governance bodies rather than being deferred into technical delivery.
- **Assurance.** The program produces evidence of what has been changed, what remains exposed, what exceptions exist, and what the resulting posture is.
- **Managed transition risk.** Mixed cryptographic states during migration are explicitly governed, inventoried, risk-assessed, and time-bounded.
- **Integration with asset lifecycle.** Where remediation depends on replacing or upgrading long-lived technology, cryptographic transformation is integrated with architecture, capital planning, procurement, vendor management, and asset-retirement roadmaps.
- **Continual improvement.** The cryptographic operating model is reviewed and improved as threats, standards, regulation, and organizational capability evolve.

Key Consideration	A transformation program is finite; this policy is durable. When a program ends, the policy remains and governs the cryptographic capability the program delivered.

9. Exceptions

Exceptions to this policy require formal approval proportionate to the risk they create.

9.1 Exception Request

Any proposed exception to this policy or an associated cryptographic standard must be formally documented, assessed, approved by the appropriate authority, and time-bound. Exceptions must not be used as a substitute for remediation where compliance is reasonably achievable.

An exception request must document:

- the policy or standard requirement affected;
- the business justification;
- the risk created by the exception (rated by risk level);
- proposed compensating controls;
- a remediation or retirement plan; and
- a defined expiry and review date.

9.2 Approval Authority

- **Low-risk** exceptions may be approved by Information Security 1B in accordance with a defined Directive.
- **Elevated-risk** exceptions require approval by the Technology Risk Committee.
- **High-risk** exceptions, including those affecting critical systems, long-lived sensitive information, material stranded assets, or PQC transition timelines, require escalation to the Board Risk Committee or the body designated by the organization.

The CISO Function is responsible for establishing and maintaining the Standards used to determine the risk rating of exception requests.

The CISO Function must not approve exceptions to requirements for which it is the requesting party. CISO-initiated exception requests must be escalated to the Technology Risk Committee.

9.3 Duration and Review

Exceptions are time-limited and may not exceed twelve months without formal renewal. Renewal requires reassessment of risk, confirmation that compensating controls remain effective, and validation that remediation or retirement remains credible. Exceptions that cannot be resolved within a reasonable timeframe must be escalated for explicit risk acceptance and included in governance reporting.

10. Policy Review

This policy must be reviewed at least annually and whenever significant change occurs in cryptographic standards, regulatory expectations, the threat landscape, enterprise or OT architecture, material supplier dependencies, or the organization's operating model. Policy updates require approval in accordance with the organization's board governance model.

Annex

Annexe 1: Policy Hierarchy

This policy establishes outcomes, principles, accountability, boundaries, and requirements at the policy tier. Downstream governance are designed to achieve the defined outcomes and detail the defined requirements in accordance with the principles, accountabilities and boundaries defined herein.

Typical Organizational Policy Hierarchy

- **Policy.** Board-approved and durable. Establishes what must be true and who is accountable.
- **Directives and Standards.** Management-approved and adaptable. Define specific requirements, control expectations, technical standards, metrics, timelines, and evidence.
- **Operational Procedures and Programs.** Define and execute implementation, discovery, migration sequencing, testing, remediation, and operational processes.

Annex 2: The Three Lines Model Explained

This policy uses the Three Lines Model to separate operational ownership, independent risk oversight, and independent assurance. Within the First Line, this template additionally uses 1A and 1B designations to distinguish operating ownership from security/control ownership. This is a practical policy convention and should be mapped to the adopting organization's operating model.

First Line - Operational Ownership and Control

The First Line owns and operates the activities that create and manage cryptographic risk. In this policy:

- Lines of Business and Support Functions (1A) provide the business, legal, operational, and information context that determines criticality and impact.
- Enterprise Technology (1A) operates cryptography across enterprise IT.
- Operational/Embedded Technology Owners (1A) operate cryptography in OT and specialized technology domains.
- Information Security (1B) defines standards, monitors compliance, and challenges execution without operating the estate under the operating assumption used here.
- Procurement and Supply Chain (1B) embeds cryptographic requirements into supplier relationships and monitors contractual compliance.

Second Line - Risk Oversight

Risk Management (2LoD) provides independent oversight and challenge. It sets or facilitates risk appetite, monitors exposure, oversees major transition risk, and ensures cryptographic risk is integrated into the enterprise risk framework. It does not operate cryptographic controls.

Third Line - Independent Assurance

Internal Audit independently assesses whether cryptographic governance, controls, evidence, and reporting are effective. It reports through the organization's audit governance structure and preserves independence from management.

Executive Management and the Board

Executive management allocates resources, sets direction, and makes material prioritization, investment, and risk decisions. The Board holds ultimate oversight accountability and challenges management through its committee structure. Together they sit above the Three Lines and ensure that cryptographic governance is treated as an enterprise accountability rather than a specialist technical activity.

Annex 3: References

This policy draws on established governance and cryptographic frameworks, including:

- National Cyber Security Centre Netherlands (NCSC-NL), Cryptographic Framework for Government (2025).
- National Institute of Standards and Technology (NIST), FIPS 203, FIPS 204, and FIPS 205 post-quantum cryptography standards (2024).
- The Institute of Internal Auditors (IIA), The IIA's Three Lines Model (2020).
- Companion industrial-sector policy work developed in coordination with this enterprise policy, addressing cryptography across enterprise, plant, product, and manufacturing supply chains.

Organizations adopting this template should supplement these references with the laws, regulations, regulatory guidance, sector standards, and jurisdiction-s