An Enterprise Cryptography Policy

Securing Digital Trust Infrastructure for the Quantum Age.

Version 1.1

Prepared by Louise Davey (LDIQ)

March 5, 2026

Introduction — Read Me First

Why I wrote this policy

This document began as an adaptation of the **Dutch Cryptographic Framework for Government**, shared by Pieter Schneider. The original framework provides a strong foundation covering traditional elements of enterprise cryptography governance but treated cryptography primarily as a **security control managed by the information security function**.

In modern digital environments, however, **cryptography behaves less like a control and more like foundational digital infrastructure** embedded across systems, applications, networks, devices, and third-party ecosystems.

As organizations approach the **largest cryptographic migration in history**, driven by emerging quantum computing risks, treating cryptography purely as a technical security control is no longer sufficient.

This policy was therefore written to **extend that foundation into a governance model capable of managing cryptography as enterprise trust infrastructure.**

Design principles behind this policy

The policy reflects a **systems-based approach to organizational design**, informed by many years operationalizing digital transformation and risk frameworks in highly regulated environments.

- Cryptography as Systemic Risk Control Principle
- Structural Dependency Principle
- Long-Term Cryptographic Resilience Principle

Governance structure

The policy uses the **Three Lines of Defence model** to clearly define accountability across the organization. First Line of Defence responsibilities are explicitly assigned (e.g., 1A / 1B distinctions) to accelerate operationalization and reduce governance ambiguity - a common weakness in many policy frameworks.

Why this policy avoids process detail

This document intentionally **does not prescribe detailed operational processes**.

Policies require **board-level approval** and therefore evolve slowly. Their role is to define **accountability, expectations, and governance structure**, not operational procedures.

Detailed implementation guidance should instead reside in **directives, standards, and operational rules**, which can evolve more rapidly as technologies and risks change.

Outcome

The resulting policy retains the foundations of traditional cryptographic governance while extending them to address:

- Systemic cryptographic risk
- Enterprise-scale cryptography lifecycle management
- Long-term digital resilience
- Readiness for **Post-Quantum Cryptography (PQC)** migration

Acknowledgement

This work builds on the **Dutch Cryptographic Framework for Government** shared by Pieter Schneider. His openness in sharing the framework made this adaptation possible and helped advance an important discussion on modern cryptographic governance.

For discussion or feedback on this policy, connect with **Louise Davey on LinkedIn**.

Contents

1. Purpose of this policy

Cryptography underpins the organization's **digital trust infrastructure**. It protects the confidentiality, integrity, authenticity, and long-term security of data, transactions, identities, and communications across the enterprise.

Because cryptography is deeply embedded in systems, infrastructure, products, and third-party ecosystems, it must be governed as a **strategic enterprise capability**, not merely as a technical security control.

This policy establishes governance, accountability, and operational requirements to ensure cryptography across the enterprise:

- is implemented securely and consistently
- remains visible and lifecycle-managed
- can evolve as threats and standards change
- can transition to **post-quantum cryptography (PQC)** without destabilizing enterprise operations

2. Principles of this policy

Cryptography as Systemic Risk Control Principle

Cryptography constitutes **core digital trust infrastructure** for the organization.

It secures the confidentiality, integrity, and authenticity of the data, transactions, identities, and communications that underpin the organization's operations, products, and relationships with clients, partners, and regulators.

Because cryptography is embedded across enterprise systems, infrastructure, and third-party technologies, weaknesses or obsolescence in cryptographic mechanisms can create **systemic operational, financial, and reputational risk**.

Cryptographic capability must therefore be governed as a **strategic enterprise control**, with visibility and accountability comparable to other forms of critical infrastructure such as financial controls, payment systems, and identity management.

The organization therefore maintains:

- enterprise visibility of cryptographic dependencies
- controlled cryptographic lifecycle management
- the ability to replace cryptographic mechanisms at scale (**crypto-agility**)
- readiness to transition to post-quantum cryptographic standards

Structural Dependency Principle

Modern digital systems accumulate layers of software, infrastructure, protocols, and third-party technologies over decades. Cryptographic mechanisms are embedded deeply within these layers and often become **invisible structural dependencies**.

Because these dependencies propagate across applications, networks, devices, and vendor platforms, weaknesses in cryptographic algorithms or key management practices can create **system-wide vulnerabilities that are difficult to detect and slow to remediate**.

Effective governance of cryptography therefore requires enterprise-wide visibility, coordinated lifecycle management, and the ability to replace cryptographic mechanisms across large technology estates.

Long-Term Cryptographic Resilience Principle

Certain classes of digital information — including financial records, contractual obligations, identity data, intellectual property, and regulated information — must remain secure over **long time horizons**.

Emerging computational capabilities, including **quantum computing**, are expected to undermine widely used cryptographic algorithms that currently protect digital systems and data. Data encrypted today may therefore become vulnerable to future decryption.

The organization has a responsibility to protect the **long-term confidentiality and integrity of digital assets entrusted to it**, including protection against threats that may materialize years or decades after data is created or transmitted.

Accordingly, the organization will maintain the capability to:

- identify cryptographic mechanisms vulnerable to emerging computational threats
- prioritize protection of long-lived and high-value data
- transition cryptographic mechanisms in a controlled and timely manner
- adopt post-quantum cryptographic standards as they mature

Failure to anticipate cryptographic obsolescence can expose organizations to **long-tail systemic risk**, where data compromised in the future undermines trust in past transactions, records, and commitments.

3. Scope

This policy applies to all organizational environments including:

- applications, platforms, and infrastructure
- networks and communications systems
- data at rest and in transit
- identities, certificates, and cryptographic keys
- digital products and services
- embedded and operational technologies
- third-party systems integrated with the enterprise

The policy applies to **employees, contractors, vendors, and partners** responsible for systems or services using cryptography.

4. Governance

Cryptography is governed as a **cross-enterprise digital trust capability** requiring coordination across technology, security, procurement, and risk functions.

Board Oversight

The **Board Risk Committee** oversees enterprise cryptographic risk as part of technology resilience, cybersecurity, and digital trust governance.

The committee receives periodic reporting on:

- enterprise cryptographic risk exposure
- cryptographic dependency visibility and coverage
- crypto-agility capability
- PQC transition readiness
- third-party cryptographic dependency risk

Enterprise Governance Bodies

Technology Risk Committee

Oversees:

- enterprise cryptographic risk posture
- PQC readiness and migration planning
- cryptographic modernization initiatives

Security Architecture Review Board

Approves and governs:

- enterprise cryptographic standards
- approved algorithms and protocols
- architectural requirements supporting crypto-agility

Third-Party Risk Committee

Oversees cryptographic security expectations across the vendor ecosystem and monitors systemic cryptographic dependencies within the technology supply chain.

5. Three Lines of Defence

First Line — Operational use of Cryptography (1A)

Lines of Business & Support Functions (1A)

provide the context needed to determine where cryptographic protections are essential and where future cryptographic disruption would create material enterprise risk.

Responsibilities include:

- Identify and classify long-life confidential assets within their domains.
- Classify business processes that depend on cryptography based on value, criticality, and risk tolerance.
- Identify processes where cryptographic failure or obsolescence creates enterprise risk.
- Provide business impact context for cryptographic prioritization and migration planning.
- Collaborate with security, architecture, and technology teams to support long-term resilience.

Technology Ownership (1A)

The **Technology function (CIO organization)** owns the technology estate and is responsible for secure cryptographic implementation across enterprise systems and infrastructure.

Responsibilities include:

- integrating cryptography into system architecture and design
- implementing approved cryptographic algorithms and protocols
- maintaining visibility of cryptographic dependencies within applications and infrastructure
- ensuring systems support cryptographic lifecycle management and upgrade capability

Technology teams must ensure cryptographic components are **discoverable, replaceable, and upgradeable**.

First Line — Security and Procurement Controls (1B)

Security Control Ownership (1B)

The **Information Security function (CISO organization)** operates enterprise cryptographic security controls and infrastructure.

Responsibilities include:

- defining enterprise cryptographic standards
- operating key and certificate management infrastructure
- maintaining approved algorithm and protocol lists
- monitoring exposure to vulnerable or deprecated cryptography
- establishing enterprise strategy for cryptographic modernization and PQC transition

Procurement and Supply Chain Control Ownership (1B)

The **Procurement function** ensures cryptographic requirements are enforced across the organization's technology supply chain.

Responsibilities include:

- embedding cryptographic requirements into vendor contracts and procurement processes

- requiring vendors to disclose cryptographic dependencies within their products and services
- ensuring vendor solutions support cryptographic lifecycle management and algorithm upgrades
- requiring vendor readiness for cryptographic modernization, including PQC where relevant

Procurement ensures that third-party technologies do not introduce **structural cryptographic risk** into the enterprise.

Second Line — Risk Oversight

The **Risk Management function (CRO organization)** provides independent oversight of enterprise cryptographic risk.

Responsibilities include:

- defining cryptographic risk tolerance and policy expectations
- monitoring enterprise cryptographic exposure
- overseeing PQC transition planning and progress
- challenging first-line practices where risk thresholds are exceeded

Third Line — Internal Audit

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

Audit activities include:

- evaluation of policy compliance
- review of cryptographic dependency management practices
- assessment of key and certificate management controls
- evaluation of crypto-agility capability
- review of PQC readiness programs

6. Requirements

Author note: The elements listed are requirements should normally be developed in subsequent Directives declining from and respecting the framework of this policy.

6.1 Cryptographic Standards

All cryptographic implementations must comply with enterprise standards approved by the **Security Architecture Review Board**.

Standards define:

- approved algorithms and protocols
- minimum key lengths and cryptographic parameters
- approved cryptographic libraries and services

- key and certificate lifecycle management practices

Algorithms identified as vulnerable or deprecated must be replaced within defined timelines.

6.2 Cryptographic Dependency Management

The organization must maintain **enterprise visibility and governance over cryptographic dependencies** embedded across systems, infrastructure, products, and third-party technologies.

The organization will maintain a continuously updated inventory including:

- algorithms and protocols
- cryptographic libraries and modules
- keys and certificates
- hardware security modules
- embedded cryptography within applications, infrastructure, and products

6.3 Key and Certificate Management

All cryptographic keys and certificates must be generated, stored, distributed, rotated, and retired according to enterprise standards.

Key management practices must ensure:

- secure key generation and storage
- controlled access to cryptographic material
- defined lifecycle management
- secure certificate issuance and renewal

6.4 Crypto-Agility

Enterprise systems must support **crypto-agility**, defined as the ability to replace cryptographic algorithms and parameters across systems, infrastructure, and vendor technologies without major system redesign.

Crypto-agility must extend beyond internally developed systems to include **third-party software, platforms, and technology providers** whose products rely on cryptographic mechanisms.

6.5 Post-Quantum Cryptography Readiness

The organization must maintain readiness to transition to **post-quantum cryptographic standards**.

Key requirements include:

- identifying cryptographic assets vulnerable to quantum attack
- prioritizing protection of long-lived data and critical systems
- aligning migration planning with emerging cryptographic standards
- integrating PQC transition planning into enterprise technology roadmaps

Progress toward PQC readiness must be reported to the **Technology Risk Committee and the Board Risk Committee**.

6.6 Monitoring and Reporting

The organization must maintain continuous visibility over enterprise cryptographic posture.

Monitoring and reporting must include:

- coverage of the cryptographic dependency inventory
- exposure to deprecated or vulnerable algorithms
- key and certificate lifecycle compliance
- PQC readiness progress
- third-party cryptographic dependency risk

Reporting must be provided regularly to enterprise risk governance bodies and the Board Risk Committee.

7. Exceptions

Exceptions to this policy require approval by the **Information Security function** and review by the **Technology Risk Committee**.

Exceptions must include documented risk acceptance and defined remediation timelines.

8. Policy Review

This policy must be reviewed at least **annually** or when significant changes occur in:

- cryptographic standards
- regulatory expectations
- threat landscape
- enterprise technology architecture

Policy updates require approval by the **Technology Risk Committee** with oversight from the **Board Risk Committee**.

****

Author note: I chose to limit the policy to the above critical content, normally you would include a lexicon of term and a relationship matrix to show how this Policy first within the overall enterprise policy framework.