2025

Cryptographic Inventory:

Deriving Value Today, Preparing for Tomorrow.

The strategic principle of establishing a cryptographic inventory is key to addressing today's vulnerabilities and preparing for a post-quantum world.

HSBC

Leon Molchanovsky

Alejandro Montblanch

Philip Intallura

Christian Albertelli
Previously at HSBC

INFOSEC GLOBAL
a Keyfactor company

Taher Elgamal

Nagy Moustafa

Vladimir Soukharev

Julien Probst

Peter Armstrong

Stefano Lindt

THALES

Blair Canavan

Jennifer Nuttall

Contents

1. Executive Summary

Cryptographic infrastructure serves as the cornerstone of the global digital ecosystem, underpinning the very essence of digital trust. As organisations increasingly rely on secure digital interactions, cryptography has emerged as a strategic asset. According to Gartner, "Cryptography is now Critical Infrastructure", underscoring its indispensable role in today's interconnected world.[1]

Establishing comprehensive visibility of cryptographic assets within an organisation through a cryptographic inventory is essential for managing complexity. Insights gained from a comprehensive cryptographic inventory provide critical input to broader Enterprise Risk Management (ERM) insofar as cryptographic risks are fundamental components of cyber risk. The latter, in turn, increases balance sheet exposure and can undermine critical service provision. Clarity of the status of the cryptographic estate provided by a cryptographic inventory enables the prioritisation of mitigation actions, addressing cryptographic vulnerabilities that pose significant business risks with direct impacts on operations and the balance sheet.

Current cryptographic infrastructure faces two foundational challenges:

1.1 Cryptographic infrastructure, designed more than thirty years ago, is struggling to remain fit for purpose in today's vastly evolved digital environment. As a result, significant vulnerabilities have emerged in the management of the cryptographic landscape, putting trust in digital business at risk.

1.2 Quantum computing poses a fundamental threat to digital trust. This emerging technology jeopardises the security of some of the most-used cryptographic methods, particularly asymmetric cryptography, in untrusted networks like the Internet. According to the 2024 Quantum Threat Timeline Report by the Global Risk Institute, quantum computers capable of breaking public key cryptography are expected to become available within 5 to 15 years.[2] This timeframe provides a critical window for preparation.

[1] Gartner, Infographic: Why You Need a Crypto Center of Excellence Now
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
[2] Global Risk Institute, 2024 Quantum Threat Timeline Report.

A comprehensive cryptographic inventory offers an important and immediate opportunity to address many of today's cryptographic shortcomings and to prioritise risk mitigation efforts. It has also been identified by the White House as the first and most critical step organisations must take in preparing for the transition to a quantum-safe environment.[3]

Preparing for the advent of quantum computing is a major undertaking. It presents technical challenges, impacts all partners within a value chain, requires substantial resources, and some existing digital systems may not be able to transition to quantum-safe status.

Cryptography has a direct impact upon business risk and in the ability to ensure compliance, such as with the General Data Protection Regulation (GDPR, European Union) or Payment Card Industry Data Security Standard (PCI-DSS). The value derived from a cryptographic inventory should be measured by its ability to reduce balance sheet risk, manage operational business risk, and provide actionable insights for risk mitigation. Moreover, it's important to recognise the dynamic nature of a cryptographic inventory as an asset that also leverages emerging concepts like a Cryptographic Bill of Materials (CBOM).

Establishing a risk management framework for cryptography to integrate with ERM will be critical to ensure that mitigation efforts are prioritised in alignment with critical enterprise risk scenarios. A cryptographic inventory provides the visibility needed to populate and support such a framework.

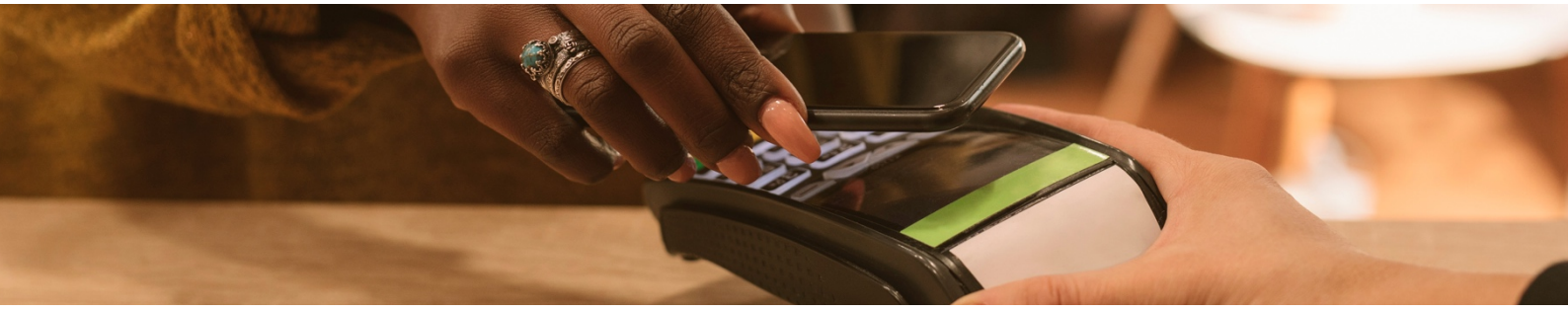
Cryptography is pervasive: it is complex, varied and often not readily visible. Consequently, creating a cryptographic inventory is challenging, and automation plays a critical role in this process. This white paper, authored by industry-leading practitioners, aims to provide insights that help technology and business leadership recognise and derive strategic value from establishing and maintaining a cryptographic inventory. The authors clarify the nature of such a cryptographic inventory, identify areas where value can be realised, highlight challenges, and set expectations for the required level of effort and approach.

[3] White House, "Report on Post-quantum Cryptography" As required by the Quantum Computing Preparedness Act, Public Law no:117-260

2. Intended Audience

"Cryptography is at the heart of digital trust and therefore at the heart of digital business. As such, organisations must recognise that cryptography is now critical infrastructure – infrastructure that must be measured and managed by multi-faceted physical and virtual teams."[4]

This paper is designed to help technology leaders such as Chief Information Officers (CIOs), Chief Technology Officers (CTOs), and Chief Information Security Officers (CISOs) derive strategic value from cryptographic discovery and cryptographic inventory. It aims to help them communicate to the broader leadership of an organisation the importance and value of establishing a cryptographic inventory today and the critical first step role it plays in preparing for a post-quantum world. It provides clarity on the nature of relevant cryptographic artifacts, identifies areas where value can be realised, outlines prioritisation considerations for mitigation and interventions, exposes significant hurdles, and sets expectations for the level of effort and approach. Additionally, it challenges the convenient assumption that cryptographic problems will only become relevant when Cryptographically Relevant Quantum Computers (CRQC) are deployed. The reality, however, is far more immediate and pressing; timelines are such that the building of a cryptographic inventory cannot be delayed.



[4] Gartner, Infographic: Why You Need a Crypto Center of Excellence Now

3. Introduction

3.1 Today's context

The world has gone digital, yet it continues to build Information Technology (IT) infrastructure using cryptographic constructs, designed over thirty years ago, which have not significantly evolved to meet the demands of today's complex digital environment.

The cryptographic infrastructure is "creaking" under the weight of all digital systems built on top of it. It has failed to adapt to the new reality and is no longer fit for purpose in many cases. This means the security of fundamental building blocks is no longer a given and, consequently, may be vulnerable.

Cryptography is everywhere and is the central pillar to digital business surety using untrusted networks like the Internet. Cryptography can be used for various purposes, including encryption, digital identities, authentication, integrity, and more. Therefore, cryptographic vulnerabilities erode the confidence and security of the digital world.

Cryptographic discovery and the creation of a dynamic cryptographic inventory are the first critical steps in understanding the vulnerabilities of the cryptographic assets upon which organisations depend. For example, an organisation needs to know the locations of its cryptographic keys, assess their quality, and evaluate the level of protection they receive to accurately determine the true state of its digital assets and estate's security.

Cryptographic vulnerabilities introduce additional exposure to an organisation's balance sheet, the assurance of continued availability of critical nation-state services, and the preservation of national security. Cryptographic discovery and inventory are essential tasks for today, helping to position the global economy and society at large to better protect our digital world tomorrow. It also describes an implicit expectation of a journey towards a post-quantum world – an important and complex transformation that demands a prioritised transition to quantum-resistant cryptography.

3.2 Tomorrow's challenges

Developed in 1994, Shor's algorithm[5] demonstrated that the mathematical problems of large number factorisation and discrete logarithms, which form the basis of modern asymmetric cryptographic algorithms, could be efficiently solved by a quantum computer.

The implementation of Shor's algorithm needs a viable Cryptographically Relevant Quantum Computer (CRQC) with more quantum computing power than is currently available. Even so, recent advancements in this field of computing show this capability is a "when" and not an "if" question, with the first CRQC availability (referred to as Q-Day) likely to occur within 5-15 years. Quantum computers will be able to break current asymmetric cryptography, meaning data and identities will no longer be secure under existing algorithmic schemes. This vulnerability undermines confidence in the identities of users and devices, as well as data in transit, in use, and at rest that relied on asymmetric cryptography at some point. The vulnerability also extends to symmetric schemes where keys are derived from public-key methods.

While symmetric cryptographic algorithms are, to a lesser extent, affected by Grover's quantum algorithm[6], they are safe against quantum computers for now, as no efficient quantum algorithm has been developed that can solve their underlying mathematical problems efficiently.

[5] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, quant-ph/9508027.
[6] A fast quantum mechanical algorithm for database search". Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery. pp. 212–219. arXiv:quant-ph/9605043.

Furthermore, other existing alternative cryptographic approaches, such as the use of one-time pads, can ensure the security of data and other assets.

The scale of this challenge impacts all business units within organisations. Achieving complete protection will be a multi-year undertaking, spanning up to a decade and maybe beyond. Government agencies around the world have expressed concern over the issue of quantum safety and have urged organisations to accelerate their preparedness for a subsequent migration. Some regulators have issued advisory notes encouraging organisations to begin addressing this issue. From a risk perspective, without proper protections in place, a successful future targeted CRQC attack could result in a loss of trillions of US dollars[7] and expose critically sensitive data. The challenge to become quantum-safe is further exacerbated by the presence of hardware and software from different vendors, complex architectures, and third-party dependencies. Cybersecurity agencies also warn about the store-now-decrypt-later (SNDL) attack, whereby malicious actors harvest data now, store it, and decrypt it when CRQCs become available. Therefore, data with long lifetime is at risk today.[8]

With the recent release of post-quantum cryptography (PQC) standards by the United States National Institute of Standards and Technology (NIST), which are quantum-resistant algorithms running on normal computers, and the availability of additional techniques that also mitigate the threat of quantum computers, it is time for organisations and institutions to begin the drafting of plans that will explore and implement the necessary measures to become quantum-safe.[9]

In highly complex and digitised multinational organisations, knowing which assets to migrate and when is challenging. This is why several cybersecurity agencies recommend cryptographic discovery as a crucial step in the migration to quantum safety, enabling the construction and establishment of a comprehensive cryptographic inventory. In the US, for example, the White House has mandated federal agencies to build a cryptographic inventory.[10] Some regulators are also encouraging specific sectors, such as financial services, to work toward establishing and maintaining a cryptographic inventory.

[7] A. Herman and A. Butler, Prosperity at Risk: The Quantum Computer Threat to the US Financial System, Hudson Institute, 2023.
[8] UK National Cyber Security Centre Whitepaper, Next Steps in preparing for post-quantum cryptography.
[9] National Institute of Standards and Technology, Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography.
[10] White House, Report on Post-quantum Cryptography as required by the Quantum Computing Preparedness Act, Public Law No 117-260.

4. Evolution of Cryptography

Since the inception of the digital society a few decades ago, cryptography has been employed to ensure confidentiality, integrity, and authentication. Today, cryptography is the backbone of every security programme in every organisation. Every organisation's security architecture assumes that cryptography functions as intended. Cryptography has been implemented in all layers of software and hardware systems and across most applications. We rely on its strength to protect data in transit, at rest, and in use, as well as to ensure identity, trust, non-repudiation and availability. Most modern devices include a variety of implementations of cryptography, with limited interoperability across an organisation's estate.

Over the last few decades, new technologies such as cloud, Internet of Things (IoT), 5G, robotics, Artificial Intelligence (AI), blockchain, Web3.0, and the metaverse have emerged. Cryptography has been used by a broad range of IT practitioners for decades without much consideration for the suitability of different configurations, under the assumption that cryptography inherently works as expected for any specific use case. However, we have now reached a tipping point where the assumption that all cryptographic implementations are robust is no longer valid. For example, the original application of Secure Sockets Layer/Transport Layer Security (SSL/TLS) was to enable e-commerce. Yet, over the past decades this same technology has been used for social networking, IoT device protection, cryptocurrency, video conferencing, and many other connected applications.

The cybersecurity community needs to shift its approach in defining cryptographic requirements, going from "you must use cryptography" to "you must use appropriate, robust cryptography." This evolution underpins the need to recognise that digital trust is the foundation of modern, digitally enabled business.

Modern systems use cryptography for various purposes beyond the traditional confidentiality, integrity, and authentication and place new requirements on it. Moving forward, the community should talk about cryptography embracing the following facets, as well as others in the future, that make up a hexagon framework (see Figure 1):

- Confidentiality
- Authentication
- Integrity
- Validation/Trust
- Availability
- Non-repudiation/Evidence

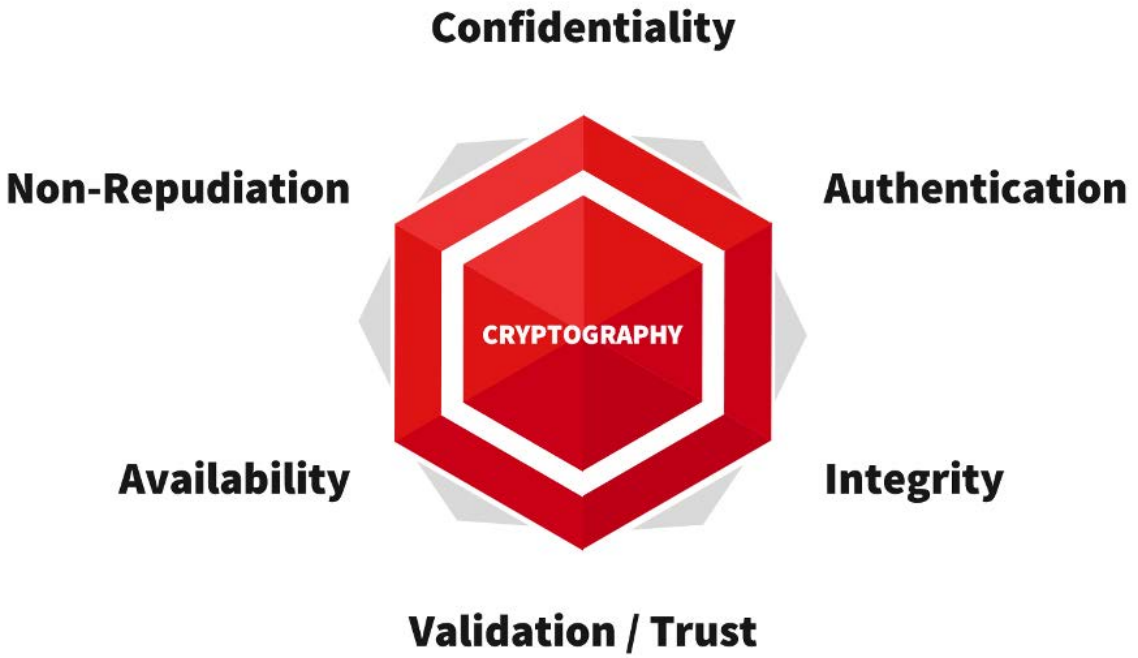


Figure 1. Cryptography Hexagon Framework

These facets should be incorporated into security control frameworks upon which we structure controls, compliance, and outcome expectations. This shift will directly influence performance indicators related to trust. As technology continues to evolve, this model may undergo further development.

Adding to the complexity of today's environments, applications and systems interact in numerous ways. Although protocols enable interoperability, in large organisations, these subsystems are often implemented separately and maintained by different groups. This generally results in weaker overall protection.

Organisations need to identify their cryptographic assets and evaluate whether they are cryptographically secure, compliant, adhere to best practices, and are appropriately used for their intended purposes, among other considerations.

5. Cryptographic Discovery & Inventory

Without a comprehensive review of cryptographic assets – including their location, effectiveness, relevance to required protection, and operational guarantees – the foundation of future trust cannot be guaranteed. Establishing such a review is a complex but critical first step in enabling digital operations to transition to cryptographic agility and a quantum-safe state.

But this is not just about the future. Organisations need a cryptographic inventory to ensure robust security and compliance within their digital infrastructure today. Cryptographic assets, such as keys, certificates, keystores, libraries, algorithms, and cipher suites, are critical for securing data and communications. Without a comprehensive cryptographic inventory, organisations risk unmanaged and potentially vulnerable cryptographic objects. A cryptographic inventory can help today with:

- Enhanced security
- Regulatory compliance
- Industry standards and best practices
- Risk reduction
- Future readiness
- Operational efficiency

5.1 What is a cryptographic inventory?

A cryptographic inventory is a dynamic, comprehensive, and systematic record of all current and evolving instances of cryptographic assets within an organisation's extended digital infrastructure.

A cryptographic inventory aims to provide a unified and detailed view of where and how cryptographic objects are deployed, ensuring they are effectively managed. Ultimately, a cryptographic inventory seeks to provide answers to some critical questions:

- **What have I got?** Providing a cryptographic inventory of all cryptographic objects deployed within the organisation, including those within purchased or acquired third-party applications.
- **Where are the assets?** Providing the exact location of the cryptographic objects within and across infrastructures.
- **How effective are the assets in relation to the protection needed?** Ensuring that the deployed cryptography delivers the expected outcomes and is fit for purpose.
- **What level of confidence do we have in the cryptographic processes?** Evaluating identities to zero-trust policies, quality of key generation, and cryptography strength relative to organisational needs.
- **What do I need to do first?** Providing prioritised, actionable insights – for example, remediation activities such as addressing security, compliance, quantum-safe transition, and align data models to protection levels in support of strategic initiatives like the adoption of zero-trust architectures.

5.2 Key elements for a cryptographic inventory

A cryptographic inventory encompasses a wide range of cryptographic assets deployed across an organisation's extended digital infrastructure. This includes, but is not limited to, cryptographic keys, certificates, algorithms, keystores, ciphers, protocols, and libraries. The scope of a cryptographic inventory extends to all environments where cryptographic objects are utilised, ensuring comprehensive coverage for effective management and security. When creating a cryptographic inventory, organisations should ensure it captures and aligns with organisation expectations in the form of a “Wish list and needs”

(section 5.3), driven by the opportunities that generate the "Organisational benefits derived from a cryptographic inventory" (section 5.4) and, in turn, address critical "Challenges" (section 5.5).

5.3 Wish list and needs

A cryptographic inventory should ideally contain (non-exhaustive):

- **Operational cryptography:** Cryptographic configuration and identity material deployed within core systems running on-premises or in the cloud.
  - Cryptographic configuration of systems that use specific keying material, ciphers, key exchange, message authentication codes, and other cryptographic elements.
  - Cryptographic keys, tokens or other cryptographic secrets deployed in systems, including keystores, private and public keys used for TLS, client authentication, and other purposes.
  - Certificates deployed in systems, including end-entity certificates, root certificate authorities and trust stores used for TLS, mutual TLS (mTLS), signing, and other purposes.
- **Software cryptography:** Cryptographic capabilities and identity material built into applications created by development teams. This includes:
  - Cryptographic operations performed by applications to protect sensitive assets, including digital signing or encryption.
  - Cryptographic algorithms embedded into software or hardware systems to perform different cryptographic operations.
  - Cryptographic libraries linked to software or hardware systems to perform cryptographic operations.
  - Root-of-Trust integrated within hardware security components, and that cannot be modified.
- **Network cryptography:** Cryptographic capabilities and identity material used by network communications between systems. This includes:
  - Cryptographic capabilities exposed in the network by different endpoints, including Secure Shell (SSH), TLS, Internet Protocol Security (IPsec), and others.
  - Cryptographic ciphers characteristics selected during negotiation between peers.
- **Managed cryptography:** Cryptographic material managed by internal security systems such as Hardware Security Modules (HSMs), Key Management Systems (KMSs), or Public Key Infrastructure (PKI). This includes:
  - Managed keys leveraging KMSs, key vaults, and other automation systems.
  - Managed certificates leveraging certificate lifecycle management solutions and other automation systems.
- **Hardware cryptography:** Cryptography used to secure cyber-physical systems such as IoT and edge devices, embedded trust modules, cryptographic chips, industrial controllers, and more. This includes:
  - Root of trust stored and protected within dedicated hardware.
  - Cryptographic keys stored and protected within dedicated hardware.
  - Hardware cryptographic capabilities supported by the hardware device.

5.4 Organisational benefits derived from a cryptographic inventory

A "good" cryptographic inventory has the following benefits:

- **Enhanced security:** Provides visibility into where and how cryptographic objects are deployed and managed. This helps identify and remediate weaknesses, such as compromised certificates or outdated algorithms.
- **Compliance:** Regulatory environments are demonstrating intent to ensure evolving standards are embraced. Compliance with such standards is likely to reduce the risk of legal fines and penalties in an environment where regulations evolve and perhaps become more prescriptive. Relevant standards and industry bodies have increased their focus on the development and adoption of comprehensive and up-to-date cryptographic inventories. These bodies include NIST, the National Cybersecurity Centre of Excellence (NCCoE, United States),

the Financial Services Information Sharing and Analysis Centre (FS-ISAC), the Payment Card Industry Security Standard Council (PCI-SSC), and the European Telecommunications Standards Institute (ETSI).

- **Risk reduction:** Identifies unmanaged cryptographic objects or leakage of sensitive keying or identity materials. This proactive approach mitigates the risk of security breaches and unauthorised access.
- **Future readiness:** Prepares for future challenges like quantum computing. A cryptographic inventory helps identify resources that are most exposed to quantum risk. These resources need to be assessed alongside the prevailing data criticality/risk model to ensure that the appropriate level of protection is applied. This enables a smooth transition to PQC and provides immediate mitigation for today's SNDL threat.
- **Operational efficiency:** Streamlines processes and reduces manual effort in cryptographic management by providing a clear map of how cryptographic operations are handled across the organisation. This leads to cost savings and improves operational efficiency. Deploying best practices for inventorying cryptographic assets also helps proactively verify that cryptographic objects are correctly managed in the context of evolving standards.

5.5 Challenges

The widespread nature of cryptography inevitably means that building a comprehensive cryptographic inventory is a complex and multi-faceted task. Moreover, the environment in which this happens is dynamic and multi-layered, with a mix of legacy systems, cloud services, and third-party applications involving a vast number of keys, certificates, algorithm instances and protocols. Many systems are often outside the control of a single organisation. Where third parties are involved, cryptography management and dependencies become important. Therefore, some level of automated cryptographic discovery and management will be required. However, there are very few candidate platforms that can fulfil this task across on-premises, cloud-native, and hybrid environments.

This means the main challenge organisations face when trying to build a comprehensive cryptographic inventory is the complexity and scale of the organisation environment itself. Solving this challenge in a structured programme requires deep expertise, specialised tools, and commitment.

An organisation's initiative involving a cryptographic inventory must additionally tackle the following challenges, which include not only the creation of the cryptographic inventory, but also the ability to maintain it in an ongoing manner that meets the cadence requirements of the organisation.

- **Heterogeneous sources can "hide" cryptographic assets:** Identifying all cryptography instances across diverse IT environments can be difficult. Cryptographic keys, certificates, and algorithms might be embedded in applications, filesystems, network interfaces, hardware devices, cloud services, and legacy systems, making them difficult to locate. Cryptography within compiled (possibly third-party) applications must be identified. Building a cryptographic inventory that covers such a heterogeneous ecosystem can be challenging from an integration perspective and requires multiple approaches to effectively discover and enumerate cryptographic objects.
- **Third-party dependencies:** Many systems are often outside the control of a single organisation. Wherever third parties are involved, cryptography management and dependencies become important. Third-party reliance can result in limited visibility over cryptographic assets.
- **Insufficient classical tools:** Traditional vulnerability and threat management tools are not designed to build a cryptographic inventory. They focus on providing information about a diverse range of vulnerabilities and potential threats, some of which are related to cryptography. Optimising such tools for cryptography is not trivial with additional costs and associated risks (e.g. false positives or false negatives). Building a cryptographic inventory requires specific technologies that focus on gathering, analysing, and centralising data about the cryptographic objects themselves.
- **Large-scale dynamic environments:** IT environments are constantly evolving with new deployments, updates, and configurations. It is crucial to keep the

cryptographic inventory up-to-date by identifying new cryptographic objects and their instances as they are introduced or removed from the infrastructure.

- **Sensitive data:** Cryptographic inventories contain highly sensitive information about the cryptographic assets and metadata deployed within an organisation. Protecting this data from unauthorised access and breaches is essential.
- **Need for automation:** Building a cryptographic inventory manually based on cryptographic specifications or systems deployed across an infrastructure is challenging at scale. Some level of automation will be needed to overcome inefficient manual processes, which would otherwise struggle to keep up with the continuous changes occurring within an infrastructure.
- **Blind spots of automation tools:** While automation helps to achieve scale, such tools often have limited coverage or compatibility. They also may ignore some artifacts they don't understand, thus creating blind spots in the overall cryptographic visibility. Identifying these blind spots and filtering out noise may require manual intervention.
- **Deep subject matter expertise:** A tool cannot find everything without being told where to look. The larger and more diverse the infrastructure, the more subject matter expertise and resource will be needed to understand where to look and to obtain the right access. There is also a need for experts to validate the output, determine what is active versus what are debris from previous configurations and testing, among others.
- **Diverse regulation:** There is no global legal framework that governs cryptography. Even though some standards are more widely used than others, nation-states often regulate cryptography independently, and therefore compliance should be localised.

5.6 What does "good" look like?

Ultimately, a cryptographic inventory is successful if it substantially enhances the robustness of the security of an organisation's digital infrastructure, and if it appreciably aids in ensuring compliance with the way the organisation conducts its digital activities. This means success criteria need to measure improvements in effectiveness of security outcomes, the reduction of risk, and the financial impact of each of these on the organisation.

Our thinking needs to evolve to ensure that we incorporate the additional facets described in Figure 1 (Hexagon) into our measurements of outcomes and into security control frameworks. These are the frameworks upon which we structure controls, compliance, and outcome expectations. These additional facets include Availability, Non-repudiation with Evidence Preservation, and Trust with Validation.

5.7 Pace

Pace has currency in this endeavour. Until a cryptographic inventory is compiled – particularly in the context of critical enterprise risk scenarios – It is difficult to prioritise the actions needed to mitigate cryptographic risk in both the short and the medium term. Additionally, prioritisation must consider the potential impact of such risks according to how exposed the balance sheet is. Organisations need to ensure that this activity is conducted in a business context where priority and investment – both in terms of effort and financial resources – are established with consideration for the risk to the organisation. For those operating in Critical National Infrastructure (CNI) and national security environments, there are additional responsibilities where pace is key, particularly in the context of secrets with long lifetime and the relevance of SNDL attacks. This creates an enhanced urgency to act.

6. Cryptographic Inventory Value

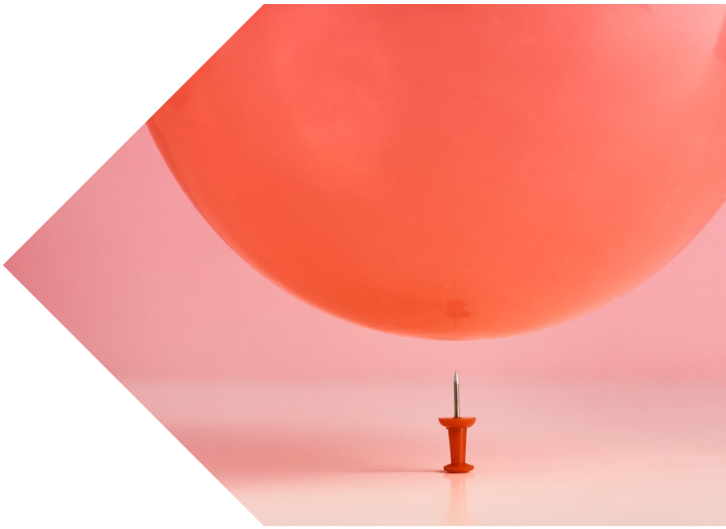
Relating cryptographic assets to business value is challenging. Ultimately, this connection must be tied to the means of value creation within the business and the risks that generate balance sheet exposure, measured within the organisation's risk appetite and tolerance. This implies that digital assets, including cryptographic assets, need to be visible to the organisation when working with critical risk scenarios. Relevant scenarios are those that lead to the erosion of value through balance sheet exposure for commercial organisations, and the resilience of the critical service being provided in a CNI context. Moreover, this visibility needs to be focused through the lenses of all facets of the Hexagon depicted in Figure 1, not just the traditional CIA triad.

It is not possible to have a comprehensive understanding of balance sheet risk without contextual visibility and an understanding of the effectiveness of the deployed cryptographic assets. Therefore, to establish contextual understanding of balance sheet exposure through risk scenarios, a comprehensive cryptographic inventory of cryptographic assets is essential. The cryptographic inventory serves as the fundamental building block for enabling a risk-based view of the organisation.

6.1 What business value does it have?

A cryptographic inventory provides insight into the potential organisation's exposure from compromised cryptographic assets. Effective cryptography is not optional. Cryptography has a direct relationship with business risk and manifests itself in several ways that can be measured in the context of incremental business exposure as outlined below. The business risks in this context represent segmentation of ERM themes frequently embraced in structured ERM regimes and frameworks. Such segmentation most often reflects a breakdown like that below.

- **Operational risk** which should be taken to reflect assessment of the probability of a material security breach occurring and where practicable, a quantification of impact associated with that breach. It should also specifically reflect any liability likely to accrue from any data breach.



- **Operational scenario risk** will always be specific to the core operations of the organisation. However, in the context of banking, asset management, and investment, there are some common system-related operational risk scenarios that have material potential to impact the organisation. These include:
  - Trading systems
    - Market impact
    - Algorithmic risk
  - Cross-border payments
    - SWIFT vulnerabilities
    - Settlement failures
  - Cryptocurrency and blockchain
    - Cryptocurrency wallets
    - Blockchain trust
- **Reputational risk** is a difficult construct to quantify particularly for organisations that are not publicly traded. It is generically difficult because of the inherently subjective nature of trust and confidence, the principal facets of reputational risk. However, there are financially driven quantification models available that focus upon the impact on trust and confidence as measured by impact upon share price. These models are normally derived from BetaPERT[11] distribution analysis of share price versus actual post-event performance. For such a model to be

[11] Beta distribution was consolidated with PERT to augment PERT and provide a model for the distribution of activity times. Clark, 1962.

deployed, an organisation needs to have a share price that is traded on an accredited exchange or market. For those organisations where this is not the case, more subjective approaches will be required.

- **Financial exposure** is usually a central component in risk management. This segment embraces direct costs, which in terms of cryptographically enabled cyber risk, could include fraud and financial losses. It will also include regulatory fines and penalties that are likely to be derived from compliance failures and litigation. They will also include balance sheet risk, manifesting itself in the form of capital impairment and valuation impact.
- **Hedging against emerging risk.** The emerging nature of risks associated with cryptographic evolution, in particular quantum computing, also suggests that hedging against emerging risk will be an important factor in the overall risk profile that a cryptographic inventory will help to manage. Hedging against emerging risks will involve costs associated with delay, for example, in the commencement of a quantum-safe transition where early insight enables early adoption and allows for a phased investment and risk mitigation. It is also likely that insurability of critical systems and processes will be a factor where evidence of robust cryptographic risk mitigation will be an important facet in both securing insurance and doing so at favourable rates. This is because quantum risks are likely to be excluded from cyber insurance policies without demonstrable safeguards and mitigation. This will not be possible without an effective and dynamic cryptographic inventory. It means that investment in cryptographic inventory and by extension in transitioning to quantum safety is not just important to evolving compliance requirements, but also an aid to risk transfer and ultimately being able to reduce uninsured exposure.
- **Evolving regulatory trends.** The final dynamic that needs to be embraced in managing the risk from cryptography relates to evolving regulatory trends. The transition to quantum safety can be characterised as likely to have a continually evolving regulatory environment, in particular for PQC. The publication for comment of NIST IR8547 in November 2024[12], that provides a breakdown of timeline expectations for the transition to quantum safety for specific algorithms and use cases, is a key milestone. Staying ahead of the regulatory wave allows for future compliance and reduces the risk from rushed upgrades that could lead to penalties being incurred.

Taking a broader view, the question of value relates to business priorities. Effective cryptography reduces risk to the business and delivers the prioritised outcomes determined by the Information Security Management System (ISMS) framework, shaped by the Hexagon (Figure 1).

6.2 How can we measure value?

An organisation should commit to leveraging the latest and best cryptography available. In this context, cost remains an essential metric for determining the relative success of an implementation. The budget for cryptographic discovery needs to be set in advance first, followed by budgets for remediation, which may be determined once the priorities and points of potential compromise are identified. Furthermore, a cryptographic inventory is a dynamic artefact requiring updates and maintenance, implying a clear need for ongoing funding from the operational budget.

These cost elements mentioned above are not popular topics and need to be articulated in the context of value to the business. This value manifests itself in terms of balance sheet risk reduction measured in currency units or in the strengthening of service provision resilience. Within an ERM framework, the organisation identifies critical risk scenarios, quantifies the exposure and, considering its risk appetite and tolerance, makes informed choices of how to manage the exposure.

For example, a biotech firm would include in its ERM a critical enterprise risk scenario where its research intellectual property (IP) is stolen and would make provision for the financial exposure that would result. Privileged Access Management (PAM), certificate management, and third-party zero-trust policy invocation would be significant components of the cryptographic support to

[12] NIST IR 8547: Transition to Post-quantum Cryptography Standards, NIST, 2024.

technical mitigation. This shifts the conversation from the Return on Investment (ROI) to reduction of balance sheet risk – like how credit risk, climate risk and other organisation risks are measured and managed. An organisation needs to ensure capabilities are in place to measure unmitigated exposures and, in turn, measure the different impacts that scenario-driven mitigations have.

Organisations can make risk capital provisions to mitigate the risk through technical or governance spending. Alternatively, they can retain the risk and fund it through methods such as pooling risk, using a captive insurance programme, or employing some other capital and balance sheet mechanism. Lastly, they can transfer the exposure to the insurance market.

These options are important because, when taken in the context of risk tolerance, they address the positive side of risk – the opportunity to derive capital benefit from knowledge of exposure. For example, risk can be taken to the market, or clarity of risk quality (such as the protection of IP) can be pooled among similar organisations to spread the risk and derive capital benefits across the pool. This can only be achieved when an organisation understands how cryptographic assets impact the quality of the risk being retained.

A cyber security programme needs to be tuned to these scenarios to quantify the additional exposure associated with cyber risk. Cryptographic risk is a subset of this and acts as both an enabler and a mitigator of risk, amplifying or mitigating financial exposure on the balance sheet or as measured, the resilience of the service being provided. A cryptographic inventory is perhaps the most foundational building block for a technology community's ability to relate cryptographic risk to the balance sheet exposure. Armed with this knowledge and financial data, the Chief Technology Officer (CTO), Chief Information Officer (CIO), or Chief Information Security Officer (CISO), can engage and debate at the board on the relative merit of cryptographic inventory investment for reducing balance sheet risk compared to other, more recognised balance sheet risks.

Recognising value in these ways also highlights the impact that cryptography and the effective management of cryptography has on overall risk. It underscores the need for organisations to address cryptographic risk mitigation as a higher priority than has been the norm until now. This paper identifies two lenses through which a cryptography-driven risk should be viewed. First, there is the incremental balance sheet exposure for the portfolio of operational risk being managed on a day-to-day basis. Second, there are longer-term, potentially existential implications for organisations failing to prepare for PQC, which needs to be addressed in a similar manner to preparing for and managing climate change risk.

- **Implications for immediate operational risk management:** Cryptographic risks have the potential to enable, accelerate, and amplify those risks already being managed within an ERM framework. Those risks may specifically involve balance sheet exposure for first-party risk or dilution of service resilience, leading to both first and third party-risk. Cryptographic discovery and inventory of cryptographic assets are indispensable central pillars in the evolving risk mitigation strategies aimed at minimising the impact of cryptographically driven cyber risks, which can exacerbate an already challenging situation.
- **Preparing for the post-quantum era:** For the 5–15-year period before quantum computing represents a direct threat, cryptographic discovery and inventory is the critical first step in preparing for the quantum-safe transition. The quantum-safe transition is a cost- and resource-intensive activity that will touch every part of an organisation and its value chain. Like climate change risk, a comprehensive understanding and preparation for a ubiquitous impact is a challenge that must be embraced today to be ready for the full effects of this risk when it materialises.

Together, these lenses suggest that it is crucial for organisations to elevate the importance of managing cryptographic risk within their operations. This means that both technical and business leadership require visibility into the risk and the exposure it creates to effectively mitigate its impacts.

Cryptographic discovery and inventory, though it might seem remote, is a critical opportunity to address today's ubiquitous vulnerabilities and the foundational challenge of quantum computing in the future.

7. Cryptographic Inventory versus Cryptographic Bill of Materials

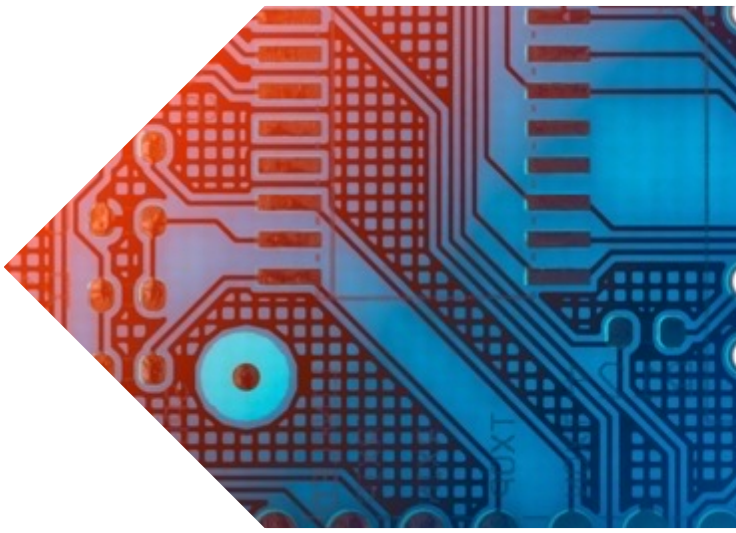
7.1 Introducing Cryptographic Bill of Materials

The concept of Cryptographic Bill of Materials (CBOM) builds on that of Software Bill of Materials (SBOM) by focusing specifically on cryptographic capabilities within software applications.[13] A CBOM lists and formalises cryptographic capabilities that are built into an application, such as algorithms (e.g., AES-256, RSA-2048), libraries (e.g., OpenSSL, Bouncy Castle), and supported keys (e.g. RSA-2048, ECC-384). It serves to establish an initial understanding of the cryptographic architecture of a software version, thereby aiding in the quick identification of potential vulnerabilities or weaknesses. Maintaining a CBOM is an important component in the understanding of the overall cryptographic capabilities of software applications. It ensures that organisations are aware of all cryptographic elements within their software, including from external vendors, facilitating better security audits and compliance with recommendations from NIST.

7.2 Cryptographic Bill of Materials limitations for cryptographic visibility

While a CBOM provides visibility into the built-in cryptographic capabilities of software, it does not include information about how the applications are configured within a specific organisation environment. For example, while the CBOM may indicate that an application supports a list of cryptographic algorithms like SHA-1 or SHA-256, it does not specify whether the company has configured the application to use SHA-1 or SHA-256. When a software application is deployed, it is provisioned with specific cryptographic material and configuration, none of which are listed in the CBOM. Additionally, applications are regularly updated nowadays, and this should be captured as well.

An organisation's cryptographic inventory should not limit itself to the built-in capabilities of software but must also encompass its overall



cryptographic operations. This includes how systems and technologies are specifically configured to utilise cryptography and cryptographic identities. For example, the cryptographic inventory should report the specific X.509 certificates, cryptographic keys, and cryptographic configurations that the company uses for an application.

7.3 Building an organisation-wide cryptographic inventory

An organisation-wide cryptographic inventory encompasses a wide range of cryptographic assets, including cryptographic keys, certificates, secrets, algorithms, keystores, ciphers, protocols, and libraries, deployed across a wide range of heterogeneous technologies. An organisation's cryptographic inventory will embrace cryptographic assets, dependencies, policies, weaknesses, and vulnerabilities in a continuously evolving environment, including:

- **Systems built-in cryptographic capabilities:** Cryptographic capabilities and identity material that are built into software and hardware systems.
- **System cryptographic configuration:** Company-specific cryptographic

[13] CycloneDX - Cryptography Bill of Materials (CBOM).

configuration and identity material deployed to software and hardware systems.

- **System cryptographic usage:** Specific cryptographic operations performed by a system to protect sensitive information using the built-in cryptographic capabilities and the cryptographic configuration defined by the company.

For example, an organisation's cryptographic inventory might detail that a particular server uses an HSM to store private keys for TLS certificates, which are rotated every 90 days according to a specific policy. Another example could be documenting the exact cipher suites enabled on a web server and ensuring they align with the organisation's security policies. By encompassing these detailed aspects, an organisation can ensure a comprehensive understanding of its cryptographic posture, facilitating better security management and risk mitigation.

7.4 Complementing a Cryptographic Bill of Materials

A CBOM and an operational cryptographic inventory can not only co-exist, but they can also complement each other effectively within a comprehensive cybersecurity framework. While a CBOM provides a detailed listing of cryptographic capabilities built into software applications, an operational cryptographic inventory takes a broader approach, also encompassing the cryptographic configuration and provisioning of systems. Essentially, the CBOM can be considered a foundational element of the larger operational cryptographic inventory, which also addresses the dynamic and operational aspects of cryptographic management. The key differences between a CBOM and an operational cryptographic inventory are the following (see Figure 2):

- **Scope**: A CBOM focuses on listing the built-in cryptographic capabilities of software, while a cryptographic inventory focuses on the broader view of how cryptography is configured and used across the extended organisation.
- **Purpose:** A CBOM offers visibility into the cryptographic elements of software for quick identification of potential misalignment with requirements, while an operational cryptographic inventory is for the holistic understanding of the organisations' cryptographic posture, facilitating better security management and risk mitigation.
- **Data collection:** A CBOM can be generated from source code, while an organisation's cryptographic inventory requires collecting and formatting data from multiple heterogeneous systems, technologies, and data sources.
- **Dynamic nature:** Both cryptographic inventory and CBOM need to be living assets. The dynamic nature of technology versions and releases and the evolving nature of threats and vulnerabilities requires continuous monitoring. This dynamic management of the cryptographic inventory is a key part of operationalising CBOM in a way that provides actionable insights for vulnerability management and, ultimately, cryptographic posture management. The key difference is that a CBOM is typically produced based on the release number of a software application, while an organisation's cryptographic inventory is continuously updated and capable of discovering multiple releases built on a constantly evolving digital infrastructure.
- **Correlation:** A CBOM provides the list of built-in cryptographic capabilities of software, while an organisation's cryptographic inventory also facilitates the understanding of dependencies between cryptographic objects generated and used by different systems and technologies.
- **Policies:** A CBOM can provide information about cryptographic weaknesses or vulnerabilities in software, while an organisation's cryptographic inventory also provides compliance and security insights about the global use of cryptography within a digital ecosystem.

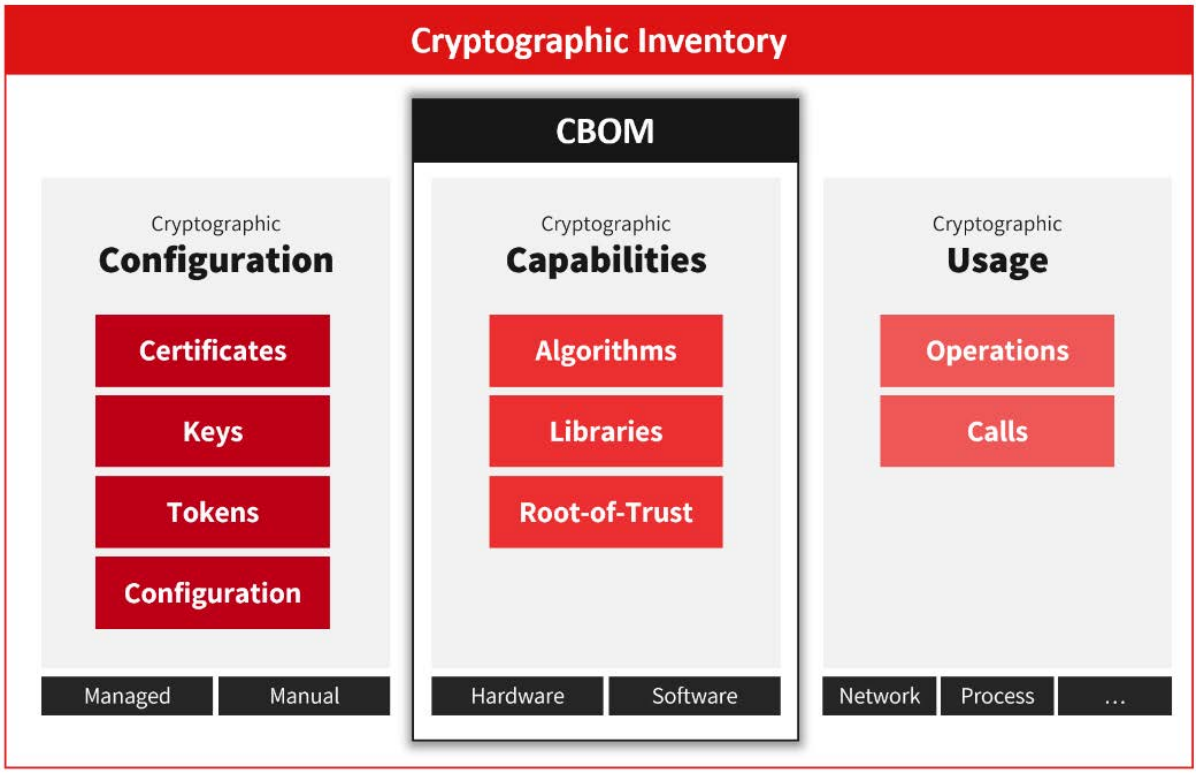


Figure 2. Positioning a CBOM Within a Broader Cryptographic Inventory

8. Ten Cryptographic Inventory Strategic Principles

The building of a cryptographic inventory should be guided by the following principles:

1. Seek executive sponsorship
2. Scale with automation
3. Optimise manual involvement
4. Prioritise efforts
5. Capture context to add value
6. Generate actionable insights
7. Leverage AI to extend the capabilities
8. Include supplier cryptography
9. Define a golden source to be trusted
10. Create a strategy to deal with false positives

Ideally, any organisation's goal should be to build a cryptographic inventory that covers the entirety of its cryptographic assets. This includes all assets directly created and managed by the organisation itself and all the assets controlled by vendors. However, achieving this comprehensive coverage is not always feasible, and difficult decisions may need to be made. These ten strategic principles should guide the decision-making process.

8.1 Executive sponsorship

Creating a cryptographic inventory is fraught with challenges and relies heavily on stakeholder collaboration. It is likely to be a multi-year process requiring substantial investment. Achieving the desired state and business objectives necessitates strong executive sponsorship.

8.2 Automation will help

Automation in the scanning and discovery of cryptographic assets enables the security team and other relevant stakeholders to leverage technological tools to create the baseline cryptographic inventory and keep it updated in accordance with corporate needs. The industry now benefits from various dedicated cryptographic discovery tools that can replace labour-intensive efforts. These tools are still relatively new and only now being adopted by some organisations. Each organisation will need to conduct proper analysis of these tools' benefits and shortcomings.

Automated solutions can play a key role in the discovery, monitoring, and management of cryptographic assets. Automation systems can track the lifecycle of cryptographic keys and certificates, assess cryptographic adequacy, and trigger changes if needed. Automation ensures that the cryptographic inventory is updated in almost real-time, enabling the security team to act on threats, prevent service disruptions, facilitate compliance reporting, and conduct forensic analysis.

8.3 Optimising manual cryptographic discovery

Automated cryptographic discovery tools often have limitations. For example, they may leave blind spots, such as offline keys or black boxes. Additionally, highly restricted regions or applications could be out of reach for some automated cryptographic discovery tools, despite these systems being critical to the business. In such cases, manual intervention is required. Industry data suggests that only a portion of cryptographic assets can be discovered using current automation tools. The remaining cryptographic assets will necessitate some manual intervention.

8.4 Prioritisation matters

If we assume that achieving cryptographic inventory coverage is difficult, how does one create the most relevant cryptographic inventory? Considering the Pareto principle, by which organisations shall focus on the fewer but more

materially significant cases, we are led to the fundamental questions: where do we start? What do we prioritise?

The answers will be highly dependent on the specific business. However, a common principle involves using a risk management framework, as outlined in Section 7. This approach involves mapping out the IT landscape to identify all instances of cryptographic usage, assessing the security posture of each asset and prioritising those that protect privileged data or are integral to key business operations in relation to critical enterprise risk scenarios. The totality of prioritisation criteria is a significant topic and will not be explored further in this paper. Nonetheless, a risk-based approach to cryptographic inventory management prioritises resources and efforts based on the potential impact and likelihood of cryptographic risk. The development of an effective risk model starts with understanding the data.

A phased approach to cryptographic inventory development ensures that the organisation can manage its resources efficiently while continuously improving its security posture. Due to the dynamic nature of cryptographic inventories and the threat landscape, a constant review of the organisation's prioritisation criteria will be needed.

8.5 Context matters

Capturing context using metadata for a cryptographic inventory object is critical to reach the right conclusions and enable remediation.

This context can include:

- **Asset criticality:** Understanding the value and sensitivity of the data or systems being protected.
- **Ownership and responsibility:** Assigning clear ownership of each cryptographic asset ensures accountability and faster remediation when issues arise.
- **Associated vulnerabilities:** Linking cryptographic assets to known vulnerabilities or internally established requirements.
- **Regulatory compliance:** Identifying any specific regulatory requirements or industry standards that apply to the asset or data.

Knowledge theory claims that information grows in value when it is contextualised and converted into actionable insights. This is depicted in Figure 3.

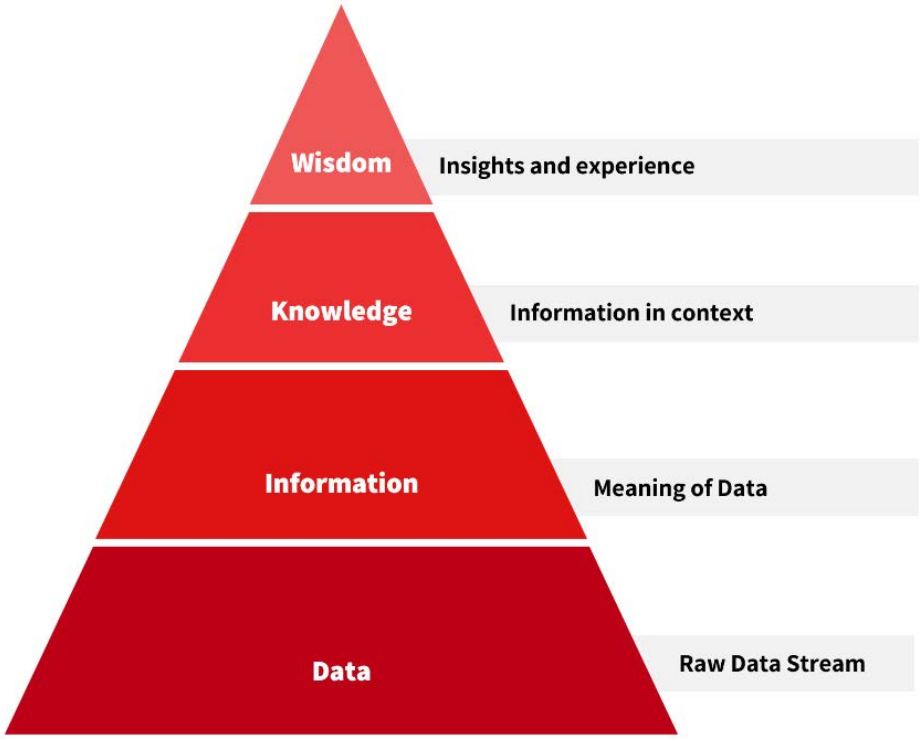


Figure 3. Knowledge Pyramid

8.6 Actionable insights

In the realm of prioritisation, it is critical to link cryptographic assets and respective findings to specific stakeholders and business functions. This ensures that identified vulnerabilities can be promptly addressed by the appropriate accountable teams.

A comprehensive and well-designed cryptographic inventory enables the organisation to act upon insights in a timely manner and serves as a foundational tool for effectively managing an organisation's security posture.

8.7 The case for Artificial Intelligence

Artificial Intelligence (AI) enables new capabilities and provides additional tools based on situational awareness and contextual analysis. AI has the potential to improve an organisation's cryptographic posture as it can contribute to automating asset classification and metadata enrichment, detect misconfigurations, and create recommendations such as vulnerability rating.

The following use-cases are possible:

- **Cryptographic data detection, manipulation, and formatting:** AI can be used to detect and standardise the format of cryptographic data found in structured or unstructured data sources. This can lead to the creation of an automated approach to ingest cryptographic assets from different systems into the golden source for cryptographic inventory.
- **Cryptographic assessment:** AI can be used to perform specific analysis on the cryptographic inventory to deliver better context and to proactively detect false positives.
- **Cryptographic advisory:** AI can be used to create contextual recommendations for remediation. This can help provide clear guidance to teams depending on the cryptographic issues and define a remediation plan. For example, it can be explaining to a team why using a specific cipher is no longer recommended, what the known compliance rules and weaknesses are, and then providing the best practices.
- **Threat hunting:** AI has the potential to enhance threat hunting through behavioural analysis. Machine Learning (ML) algorithms may be used to analyse a user or entity's behaviour over time, creating an algorithm's baseline dataset. An ML model could flag not only unauthorised configurations but unexpected ones as well, creating a dynamic alerting system. An ML algorithm can, for example, flag anomalies such as the creation of an authentication key with an unusually short lifespan accessing a critical service, or classified data that is secured by strong protocols but uses a weak algorithm. The change itself may not be forbidden but, in its context, it is unexpected. An ML algorithm can also take into consideration behaviours from across the network, correlating events from multiple assets to assess patterns and flag broader attacks. By combining these functionalities, ML models may help the organisation develop a more proactive approach to vulnerability management and cryptographic configuration monitoring.

8.8 Supplier management

While various capabilities can be outsourced, risk cannot be outsourced and will always be owned by the organisation. There will always be dependencies in the supply chain and digital ecosystem arising from the need for interoperability, cryptographic handshakes across organisations, and system boundaries.

There is particular concern in preparing for the quantum-safe transition about making visible those systems and components that are not likely to support PQC.

8.9 Golden Source for Cryptographic Inventory

One important principle is to identify sources of cryptography-related information and potentially create a single golden source for the cryptographic inventory.

A Golden Source for Cryptographic Inventory (GSCI) is a dynamic, trusted repository of cryptography-relevant data designed to enable users and systems to make decisions and take actions.

This task is more complex than it may appear. For instance, private keys must be protected and remain in secure memory or devices, never to be copied. However, various metadata about these keys should be accessible to other systems. It's possible that an HSM vendor might provide such functionality, yet this information may also be needed to demonstrate compliance and potentially exist in other systems. Under these

circumstances, which repository will become the GSCI that will drive decisions and actions? In the same context, identity management that crosses system or organisation boundaries, with potentially different zero-trust policy frameworks, can be challenging, considering that identity is not just users but also devices, system components, certificate authorities, and more.

The answer depends on the architectural choices made when designing a cryptographic inventory. The goal is to have one or more such sources that can be trusted by other systems (Figure 4).

It is also possible to have a combination of multiple inventories, if ultimately there is a single source of truth enabling better control and oversight, with improved risk assessment. This federated approach can also potentially reduce data storage and movement costs, although it may also mean a greater share of manual cryptographic discovery due to multiple dependencies. Sometimes this is unavoidable when local regulation requires the use of local cryptography or storage of cryptographic assets within national boundaries. This is often the case for regulated global organisations.

8.10 False positives

Large amounts of diverse data coming from multiple sources will lead to some false positives. These may create a lot of noise and lead to value erosion. It may take a considerable amount of time to tune the system to the acceptable level to minimise false positives. Having a clear strategy how to deal with them will help maintain momentum and generate value.

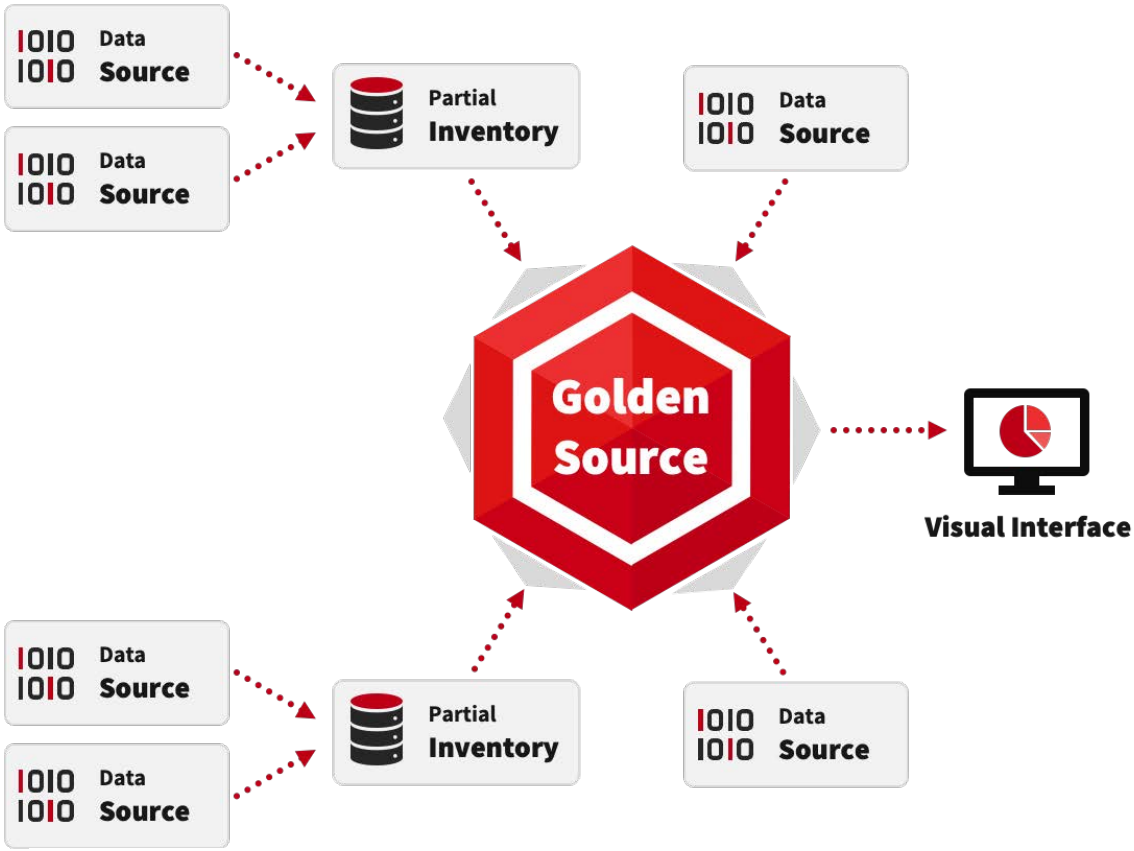
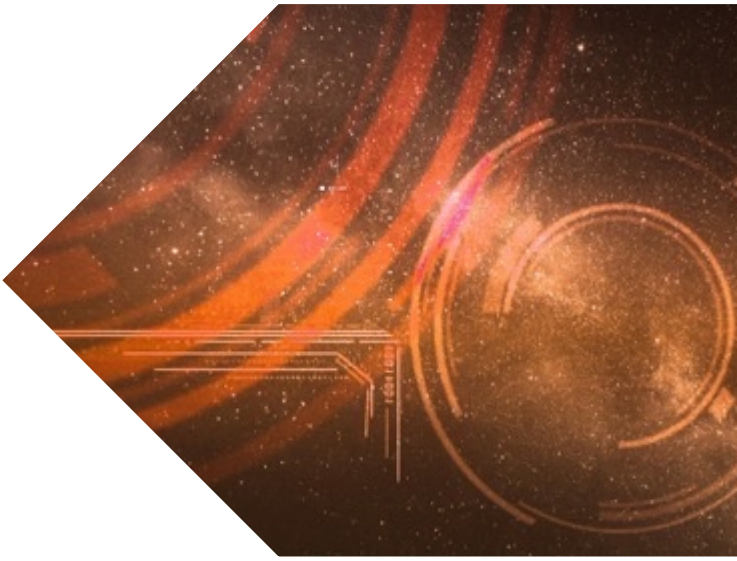


Figure 4. Representation of a GSCI environment

9. Practical Applications of a Cryptographic Inventory

Organisations have different motivation to create a cryptographic inventory. The following points are some possible applications of a cryptographic inventory. They should be placed within the context of the value that an inventory brings, as well as the strategic principles described previously.

- **Compliance:** The primary reason for implementing a cryptographic inventory is often compliance. Regulators are becoming more knowledgeable and sophisticated. While there are no explicit requirements yet, some regulators such as in the US and Singapore, have issued advisory notes recommending implementation of a cryptographic inventory.[14&15]
- **Vulnerability discovery:** Increasing numbers of cryptography-related vulnerabilities are being discovered. New Common Vulnerabilities and Exposures (CVEs) and Common Weakness Enumerations (CWEs) are added continually as part of the MITRE Corporation's maintenance role. The cryptographic discovery process facilitates discovery of vulnerabilities and informs vulnerability management platforms accordingly. Furthermore, automatic remediation can be triggered if configured.
- **Weakness identification:** A cryptographic inventory is crucial for identifying cryptography-related weaknesses in digital assets. When new vulnerabilities are discovered, assets can be updated quickly. Considering the fast pace of change, agile lifecycle management of cryptographic assets becomes an important aspect of cybersecurity operations and resilience. A cryptographic inventory is a critical facilitator.
- **Agility in cryptography operations:** Cryptographic operations must become agile. While significant progress has been made to bring agility to certificate and key management, other cryptographic assets are still managed traditionally. This approach assumes that good cryptography does not change often. As this assumption is no longer valid, cryptographic operations must extend their agility capabilities to other areas of cryptography.



- **Agility in software development:** The same agility principles apply to software development. Since cryptography is now an integral part of any modern software, cryptographic agility should be on par with agile software development best practices.
- **Supply chain dependencies:** Most industries use an extensive supply chain that brings dependencies and, therefore, risks. Organisations need to ensure third parties use best practices. One such way is by requesting a CBOM as part of a procurement process or including a joint incident response plan under the principle of shared responsibility. This includes checking suppliers for their PQC readiness as part of the procurement process and incorporating relevant clauses into legal and contract requirements.

[14] The Office of Management & Budget (OMB), Memorandum M-23-02 Migrating to Post-Quantum Cryptography.

[15] Monetary Authority of Singapore, Advisory on addressing the cybersecurity risks associated with quantum.

10. Who Is Accountable & Responsible

Given the shift from "you must use cryptography" to "you must use good, appropriate cryptography", frameworks for cryptographic responsibility are only now evolving. This is another example, this time in the governance context, of cryptography failing to evolve to meet the new technical realities. Consequently, it is difficult to determine which roles different stakeholders should assume. In a large organisation, this responsibility would fall under the CIO or CISO. There should be someone accountable for all cryptography and cryptographic inventory.

In practice, this responsibility could be distributed across various groups, such as DevSecOps, IT, a dedicated cryptographic team, security compliance, and others. Additionally, business teams also play critical roles, either by choosing what cryptography to use or specifying risk levels. Cryptography impacts a wide range of departments.

Each constituency will need to allocate roles (e.g., by using RACI Matrix: Responsible, Accountable, Consulted, and Informed) to ensure control and visibility of cryptography internally, or to have someone in the CISO's organisation who would be able to control it externally to each department. There are pros and cons to both approaches. Cryptography is a highly complex topic, and there are few experts in the field. If departments choose to individually control their cryptography, it will require significant resources, which might not be feasible. In the second approach, external control might bring additional difficulties for business unit operations.

It is important to understand that the requirement to manage cryptography efficiently will become unavoidable. The most effective approach is to start by assigning this responsibility to dedicated experts, CISOs, and IT organisations. The central team will then own the capability, the tools, and the golden source.

In a decentralised approach, CISOs can pass down relevant responsibilities to each business unit, and they would each be able to run cryptographic inventory tools that provide a GSCI of cryptographic artifacts. Simultaneously, each business unit would be able to run the tools to provide proof of proper security and compliance.

There is the possibility of other models, many of which entail hybrids of the two described. To make it viable for an organisation to perform these tasks, proper role assignment is needed. By using the RACI approach:

- **Responsible:** Responsibility can be centralised or decentralised, and determining the right approach is a key decision for the organisation.
- **Accountable:** A C-level executive should be made accountable for cryptography management.
- **Consulted:** This is where a cryptographic expert, either assigned to each business unit or designated as one individual or team for the entire organisation, is essential. Regardless of whether that person or team holds responsibility or authority over other business units, they must act as a consulting entity within the organisation for all matters related to cryptography due to their specialised knowledge.
- **Informed:** Regardless of the structure, it is vital that each business unit involved with cryptography is well-informed, and that the cryptography team is aware of and can monitor the cryptography being used. Achieving this requires tools that offer granular access and comprehensive cryptographic monitoring.

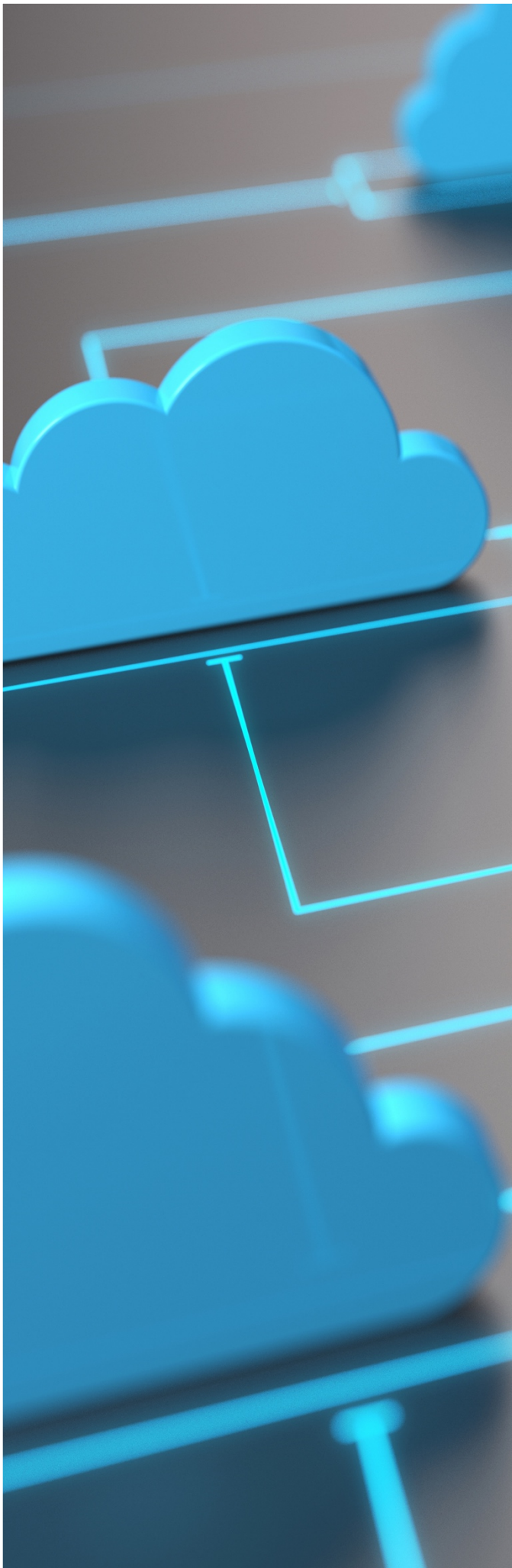
A significant challenge lies in understanding how the cryptographic inventory will be consumed, including remediation activities. Countless possibilities make listing every option impractical. The key is to understand RACI roles and ensure that cryptography-related decisions are not made without proper expertise.

11. A Note on Cryptographic Agility

Cryptographic agility refers to the ability of an organisation's cryptographic infrastructure to switch rapidly and efficiently between cryptographic algorithms, libraries, keys, tokens, certificates, and other cryptographic assets or protocols without major operational disruption. This flexibility is essential for maintaining security as cryptographic standards evolve, particularly in response to new vulnerabilities, technological advancements, or regulatory requirements. Cryptographic agility ensures that systems can adapt to future cryptographic needs, including transitioning to PQC as quantum computing advances.

Cryptographic agility is a significant step on the overall maturity journey of organisations seeking to operationalise cryptographic capabilities in a dynamic risk environment. Not all organisations will be ready to embrace this, but it is a natural evolution from a static response to the proactive configuration and management that an AI-enabled, post-quantum world will demand.

Cryptographic agility represents a new architectural approach and is outside the specific scope of this paper. However, what is definite is that cryptographic agility cannot be achieved without a solid cryptographic inventory in place.



12. Conclusion

Cryptographic infrastructure, designed more than 30 years ago, is struggling to remain fit for purpose in the much-evolved digital environment in which it is deployed today.

It has not kept pace, resulting in a mismatch with the technical burden it faces as the enabler of trust in the digital world. This mismatch has led to significant vulnerabilities in the management of the cryptographic environment, which degrade confidence and trust in digital interactions.

A cryptographic inventory represents an essential and immediate opportunity to provide actionable insights that will help address many shortcomings and prioritise mitigation of risk today. Moreover, the visibility and insight derived from a cryptographic inventory allows alignment with an imperative to update the long-held CIA triad pillars. This update has been described in this paper as a cryptographic framework with a Hexagon that adds Availability, Non-repudiation with Evidence Preservation, and Trust with Validation to the traditional cryptography domains to enable digital trust. These additions help the cryptographic inventory evolve into a dynamic asset that allows the operationalisation. Within that, the cryptographic inventory creates actionable insights to manage evolving risks and vulnerabilities.

Today's cryptographic risks are only one part of the story. The second part is the threat to asymmetric cryptography due to the anticipated advent of quantum computing within 5 to 15 years. This threat requires beginning transition planning to PQC now. The quantum-safe transition will likely be a significant, multi-year maturity journey for all organisations and agencies. Consequently, it is imperative to create inventories of cryptographic assets that will allow organisations to prioritise the practical response that constitutes quantum-safe transition.

Cryptography is ubiquitous: it is complex, varied, and not always visible. This means creating a cryptographic inventory is challenging, and automation plays a critical role in this process. However, some manual cryptographic discovery will still be necessary. Furthermore, a cryptographic inventory is not just about what cryptographic assets one has, but also where they are located, how effective they are, whether

they are compliant, and what they are used for. As crucial as this visibility is, it must also include interoperability within and beyond the organisation, and across system boundaries, necessitating the integration of multiple inventories.

Cryptography needs to be managed as a business risk. The value derived from a cryptographic inventory translates to a reduction in balance sheet risk and better management of business operational risk. Consequently, a report establishing a risk management framework will ensure the prioritised alignment of risk mitigation efforts to cryptographic assets that align with critical enterprise risk scenarios.

The mismatch of cryptography to specific use case requirements has reached a tipping point. It requires a shift in defining requirements from "you must use cryptography" to "you must use good, appropriate cryptography".

Cryptography must become a strategic asset of an organisation, as it constitutes critical infrastructure. The governance and risk management framework to clarify this responsibility matrix is not fixed. It is crucial for organisations starting this journey to do so within a robust responsibility matrix, potentially built around the RACI model.

13. Key Takeaways

1. **Cryptographic infrastructure vulnerabilities:** Cryptographic infrastructure is already showing signs of strain. To prioritise the mitigation of cryptographic vulnerabilities, the cryptographic discovery and inventory of cryptographic assets is a critical first step.
2. **Quantum computing threat:** Quantum computing represents a foundational threat to asymmetric cryptography that could manifest within a decade. Preparing for a quantum-safe transition is an immediate imperative and likely a maturity journey spanning several years. Establishing a cryptographic inventory is essential for a successful transition to post-quantum cryptography.
3. **Complexity and automation:** The complexity of the task will require extensive expertise and some level of automated cryptographic discovery. However, some manual cryptographic discovery will still be necessary. Understanding the complexity of the cryptographic interactions across system and organisation boundaries is a critical success factor due to multiple dependencies.
4. **Evolving digital landscape:** Cryptographic infrastructure has not kept pace with the evolution of the digital landscape and has led to an erosion of trust in digital interactions. This necessitates an update from the traditional Confidentiality, Integrity, and Authenticity triad of cryptography to an evolving Hexagon framework of cryptography pillars that includes Availability, Non-repudiation with Evidence Preservation, and Trust with Validation. The quantum-safe transition journey provides an opportunity to update the broad-based approach to cryptography and digital trust by operationalising a cryptographic inventory (incorporating Cryptographic Bill of Materials) to create actionable insights to manage evolving vulnerabilities.
5. **Organisation-wide risk management:** Cryptography is a key facet of business. Its management needs to be embedded in a robust, organisation-wide risk management framework that measures the significance of cryptographic risk in the context of overall risk reduction, whether that is risk to the balance sheet or risk to resilience of critical service provision and national security.

14. Authors & Contributors

Leon Molchanovsky
Cryptography SME
HSBC

Leon Molchanovsky leads the cryptographic agility and inventory efforts at HSBC. In this role he brings cryptography perspective to both internal and external activities. Leon also represents the bank in the Cybersecurity Centre of Excellence of NIST.
Before joining the bank, he worked in multiple projects across the globe in telecommunications, Blockchain, smart cities, Industry 4.0 delivering security by design and digital transformation. Leon holds a MSc in quantum electronics, an MBA degree and speaks multiple languages.

Alejandro Montblanch
Quantum Communications and Networking Lead
HSBC

Alejandro R.-P. Montblanch leads the quantum communication and quantum networking efforts at HSBC. In this role, he is leading the participation of HSBC in the London Quantum Key Distribution (QKD) network, where he successfully used QKD to quantum-secure an FX trading scenario for the first time in the world. Additionally, he directs HSBC's efforts to advance the assurance of QKD, and HSBC's involvement in QKD in Singapore. He also works toward building a cryptographic inventory and implementing Post-Quantum Cryptography in HSBC. Before joining HSBC, he was a postdoc in Delft, where he worked on developing a future Quantum Internet. He holds a PhD from the University of Cambridge on Quantum Physics, with a stay in Harvard, and master's degrees in Physics, and in Computational and Mathematical Engineering. He has received a Marie Curie scholarship and other prizes. He has published in renowned journals such as Nature Nanotechnology, Nature Communications, and Physical Review Letters.

Philip Intallura
Head of Quantum Technologies
HSBC

Philip Intallura is the Group Head of Quantum Technologies at HSBC. By spearheading quantum efforts at the bank, he has positioned HSBC as a global leader in quantum finance. Under his leadership, the team has delivered world-first quantum applications in quantum computing, quantum communications, and quantum security, along with groundbreaking research and patents. With a background that spans physics, finance, AI, and digital transformation, he has specialised in bridging complex science with commercial impact. He holds a PhD in Physics from the University of Cambridge.

Christian Albertelli
Data Engineer
Previously at HSBC

Christian Albertelli worked at HSBC as a Data Engineer in the Cryptographic team and specialised in structured data security in the Database Monitoring and Network Segmentation teams. He recently joined the team at Vocalink, Mastercard, as Senior Information Security Engineer. Christian holds a Master's degree in Mathematics from King's College London and a Bachelor's degree in Mathematics.

Blair Canavan
Director, Alliances - PKI & PQC Portfolio
Thales

Blair has 35+ years of cybersecurity sales, marketing and business development expertise. Blair started his cybersecurity and cryptographic career with Symantec, followed by Chrysalis-ITS (Thales), Titus (Fortra), Black Duck (Synopsys), InfoSec Global and Crypto4A. Blair was recruited back to Thales' Global Technology Alliances team in 2019, tasked with the growth & curation of the PKI and Post Quantum Cryptography (PQC) portfolio. He is an avid presenter, start-up consultant and PQC industry contributor, including the founding of Thales' PQC Palooza event held at the RSA Conference. Blair holds an Hons.BA Co-op from the University of Waterloo and Wilfrid Laurier University, Ontario, Canada.

Jennifer Nuttall
Product Marketing Manager
Thales

Jennifer has 20 years of marketing and communications experience, with a specialty in understanding how technology delivers value for its customers. She has spent the last 5 years expanding her knowledge in defense and cybersecurity technologies, particularly in post-quantum cryptography. Jennifer holds her Master's Degree in Communications from Carleton University, in Canada.

Taher Elgamal
Co-Founder
InfoSec Global

Dr. Taher Elgamal, co-founder of InfoSec Global and Partner at Evolution Equity Partners, is a cybersecurity pioneer known as the "father of SSL." With over four decades of expertise, he has driven innovation in online security, encryption, and data protection. A prolific inventor with numerous patents, he has also founded companies like NokNok Labs and Securify. Formerly

CTO of Security at Salesforce, he has earned prestigious honours, including the RSA Lifetime Achievement Award and the Marconi Prize, cementing his legacy in cybersecurity.

Nagy Moustafa
CEO & Co-Founder
InfoSec Global

Nagy Moustafa is the Co-founder and CEO of InfoSec Global, where he spearheads the company's cryptographic agility solutions, including the AgileSec Platform, and drives strategic initiatives to address quantum-resistant cybersecurity challenges for enterprise and government clients. A visionary entrepreneur with a proven track record of turning ideas into reality, Nagy has extensive international experience across North America, Europe, Asia, and the Middle East. Earlier in his career, he held senior roles at Rogers Communications and Canada's Ministry of Economic Development.

Vladimir Soukharev
Head of Cryptographic R&D
InfoSec Global

Dr. Vladimir Soukharev, Head of Cryptographic Research & Development at InfoSec Global, specialises in cryptography, security, and privacy. Earning his Ph.D. from the University of Waterloo, he has contributed and published works in world-renowned publications, such as Financial Cryptography and the Journal of Mathematical Cryptology. Since joining InfoSec Global in 2016, he has focused on advancing post-quantum cryptography, cryptographic agility, and cryptographic discovery. He is also contributing to government initiatives and standards related to PQC and cryptographic migration, which include NCCoE, NIST, and Quantum-Safe Canada.

Julien Probst
Chief Customer Officer
& Head of Product
InfoSec Global

Julien Probst leads product strategy and global customer engagements at InfoSec Global, the leader in cryptographic posture management. Julien works closely with financial institutions and large enterprises to help them understand, assess and modernise their cryptography. Julien holds an engineering degree from the University of Applied Sciences of Western Switzerland (HEIG-VD) and has over 17 years of experience in entrepreneurship, international business, product innovation, and cybersecurity.

Peter Armstrong
Head of Sales, UK & Ireland
InfoSec Global

Peter Armstrong is a cyber risk expert and seasoned executive in technology and risk, leading InfoSec Global's Strategic Engagement and UK business. Previously, he was Senior Cyber SME at Munich Re Group and led Willis Cyber risk consulting. With a background in Government and Defence, he led sensitive cybersecurity activities and managed businesses like Thales Cyber Security Business, the Finmeccanica Global Battlespace Business, and the UNISYS Commercial Industries Group. Peter holds an MSc in IT & Management and is a Fellow of The Institute of Directors.

Stefano Lindt
Head of Marketing
InfoSec Global

Stefano Lindt is Head of Marketing at InfoSec Global, where he leads strategic marketing initiatives to advance the company’s cryptographic posture management solutions, AgileSec Platform. With over 20 years of experience in marketing enterprise software, Stefano brings deep expertise in product marketing, go-to-market strategy, brand positioning, and demand generation. Prior to joining InfoSec Global, he held leadership roles at Hewlett Packard Enterprise’s AI Solutions team and C3 AI. He holds an MBA from the University of Michigan and a BS from Boston College.

15. About the Companies

HSBC Holdings PLC

HSBC Holdings plc, the parent company of HSBC, is headquartered in London. HSBC serves customers worldwide from offices in 58 countries and territories. With assets of US$3,017bn as of 31 December 2024, HSBC is one of the world's largest banking and financial services organisations.

InfoSec Global

As the pioneer and leader in Cryptographic Agility Management solutions, InfoSec Global secures the world's data by helping organisations discover, inventory, remediate and control their cryptographic assets with agile cryptography. From cryptographic asset discovery to ensuring a seamless transition to stronger cryptographic standards, our solutions restore digital trust to enterprises and governments.

Thales DIS CPL USA, Inc.

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognised brands and organisations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centre to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organisations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.