Guidelines for Quantum Risk Management for Telco

Version 1.0

22 September 2023

*This is a **whitepaper** of the GSMA*

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

1 Executive Summary

Cryptographically Relevant Quantum Computers (CRQC) pose new threats to telecommunication systems and significant new cybersecurity challenges, because they disrupt widely used encryption algorithms and protocols.

The overall objective is to ensure that key stakeholders and business owners have the information required to make proportionate decisions in Quantum Risk Management (QRM) in the right timeframes. We believe that a Quantum Cryptanalytic Risk Assessment (QCRA) for Telco is a critical methodology that supports Telecommunication Service Providers and the extended Telecommunication supply chain building a multi-year plan to address quantum risk.

Given the complexity and breadth of the impacts on current cryptography related to both legacy and future cybersecurity capabilities used in Telecommunication environments, an important element of proactive threat management is the ability to identify, evaluate and prioritise risks on an ongoing basis.

Improving education and awareness about Quantum Computing, building skills and knowledge, are important aspects for all organisations in creating an effective Quantum Risk Management (QRM) capability.

This document provides an analysis of how some common risk assessment frameworks can be adapted specifically for a Cryptanalytic Risk Assessment for Telco, using telco relevant use cases as examples.

The recommendation is to consider relevant risk assessment methodologies as part of the overall risk framework.

“A Methodology for Quantum Risk Assessment” and “Crypto Agility Risk Assessment Framework (CARAF)” are two examples of Quantum Cryptanalytic Risk Assessment (QCRA), while the NIST Risk Management Framework [2] and ISO/IEC 27000 [1] can be adapted to address quantum risk.

Common considerations across risk assessment frameworks and a QCRA include: definition of roles and responsibilities, threat identification, asset and cryptographic inventory, impact calculation, and control selection.

Two attacks should be considered for threat identification:

- immediate threat from “Store now decrypt later” where a Quantum Capable Threat Actors (QCTA) gains access to sensitive data with a long shelf life that can be accessed once a CRQC is available; and
- future threats that originate from Quantum Capable Threat Actors (QCTA) that will have access to CRQC.

The result of the impact assessment aids the analysis and prioritisation for identified threats.

The QCRA informs a holistic, balanced and full lifecycle risk management program that drives significant change to the cryptographic mechanisms used by Telecommunication Service Providers. It guides the Telecommunication supply chain management to address the Quantum threat.

While the focus of the document is specifically on Quantum related security aspects in Telco, we fully recognise that CRQC is one of the many threats that Telco organisations face going forward. The document also highlights the rapidly and continuously evolving compliance and regulation landscape for Quantum security.

1.1 Recommendations

- Governance
    - Build board-level awareness of the quantum risk.
    - Establish an organisation-wide governance process to manage quantum risk.
    - Identify an executive owner, and update roles and responsibilities to include quantum risk.

- Capability
    - Develop organisational capability to manage quantum risk.
    - Update education and training programs to increase understanding of the quantum risk.
    - Monitoring the development of tools to facilitate the transition.
- Risk Management
    - Adapt a Risk Framework to manage quantum risk for your organisation.
    - Integrate Quantum risk into Enterprise Risk Management (ERM).
    - Perform a Quantum Cryptanalytic Risk Assessment (QCRA) to prioritise critical systems and data for mitigation.
    - Identify and manage residual risk.

- Planning for transition
    - Determine the organisation’s current cryptographic estate.
    - Determine the organisation’s data assets, data protection requirements, and data longevity.
    - Prioritise the assessment of critical applications and services.
    - Create a transition plan, based on the Quantum Cryptanalytic Risk Assessment (QCRA) and informed by the organisation’s risk appetite.

2 Introduction

The first step in addressing the vulnerabilities presented by a CRQC is to determine the cryptographic estate, by gathering an inventory of assets (including files, storage units and communication channels), and their current cryptographic protection. It is also important to identify and record the storage lifetime required for each inventory asset. These elements must then be prioritised for mitigation. The best way to conduct this process is through a risk

assessment. A QCRA focuses only on the issues that emerge from CRQC - the data and assets at risk and the cryptographic protocols that need to be upgraded in order to mitigate risks to the data. However, a typical Risk Assessment (RA) has much of the information needed to conduct a QCRA, including standard data/asset inventory & classification, and a detailed mapping of the cryptographic protocols used to protect these assets. Depending on the resources available to the enterprise, either a standalone QCRA can be conducted or QCRA elements can be integrated into an existing risk assessment (RA) framework. This document provides a starting point for conducting a QCRA. It also describes how to integrate QCRA practices into common risk frameworks e.g., NIST Risk Management Framework [2] and ISO/IEC 27001 [1].

2.1 Scope

The scope of this document is the evaluation of risk frameworks that are either quantum specific or that could be adapted to incorporate the unique threat aspects that quantum computing introduces. It also supports the understanding of the threat landscape and timeline related to the emergence of CRQC in the context of the telecommunication industry. This approach is Quantum Risk Management (QRM) which is a subset of Cybersecurity Risk Management (CSRM). CSRM is one aspect of broader Enterprise Risk Management (ERM) [30].

This document describes the risk exposure for the telecommunications ecosystem in a post-quantum-computing environment. It provides an overview of QCRA applicability. It includes Risk Assessment guidelines for organisations using either ISO27001/NIST [1],[2] or a combination of use cases in this document. Individual enterprises determine their own risk appetite and risk mitigation for each use case.

2.2 Definitions

Term	Description
ISO/IEC 27001	International Standard covering guidance for information security management systems (ISMS) covering establishing, implementing, maintaining and continually improving an information security management system.
NIST RMF	NIST SP 800-37 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [2]
Crypto agility	The ability of an entity to replace existing cryptographic primitives, algorithms, or protocols with a new alternative quickly, inexpensively, with no or acceptable risk
Quantum Risk Management	The management of risks related to quantum computing.
NIST CSF	Tiered framework detailing qualitative measures on organisational cybersecurity Risk management practices

2.3 Abbreviations

Term	Description
CARAF	Crypto Agility Risk Assessment Framework

Term	Description
CRQC	Cryptographically Relevant Quantum Computer
CSRM	Cybersecurity Risk Management
CSF	Cyber Security Framework (NIST)
DSS	Data Security Standard
ERM	Enterprise Risk Management
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HSM	Hardware Security Module
ISMS	Information Security Management Systems
ISO	International Organisation for Standardisation
NIST	National Institute of Standards and Technology, US Department of Commerce
OAM	Operations, administration and management
OSS	Operational Support System
PCI	Payment Card Industry Security Standards Council
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PPK	Post-Quantum Pre-shared Keys
PQC	Post-Quantum Cryptography
QCRA	Quantum Cryptanalytic Risk Assessment
QCTA	Quantum Capable Threat Actor
QKD	Quantum Key Distribution
QRA	Quantum Risk Assessment
QRCA	Quantum-Resistant Cryptographic Algorithms
QRM	Quantum Risk Management
RA	Risk Assessment
RMF	Risk Management Framework
TLS	Transport Layer Security

2.4 References

Ref	Doc Number	Title
[1]	ISO/IEC 27001	ISO/IEC 27001. (2022. Information security management systems – Requirements. International Organization for Standardization – ISO, Geneva
[2]	NIST RMF	NIST Special Publication 800-37 Revision 2 (2022) Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy
[3]	CARAF	CARAF: Crypto Agility Risk Assessment Framework

Ref	Doc Number	Title
		Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, Vaibhav Garg Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab013, https://doi.org/10.1093/cybsec/tyab013
[4]	NIST CSF	Framework for Improving Critical Infrastructure Cybersecurity V1.1 (April 2018)
[5]	GSMA PQ.01	Post-Quantum Telco Network Impact Assessment Whitepaper, February 2023
[6]	NIST	Post-Quantum Cryptography Standardization
[7]		A Methodology for Quantum Risk Assessment, June 2023 https://www.evolutionq.com/publications/quantum-risk-assessment
[8]	ISO/IEC 27001	ISO/IEC 27001 Standard – Information Security Management Systems
[9]	ISO/IEC 27002	ISO/IEC 27002: Code of Practice for Information Security Controls
[10]	ISO/IEC 27005	ISO/IEC 27005 (2022): Information security, cybersecurity and privacy protection – Guidance on managing information security risks
[11]	NCSC	Cloud security guidance: How to choose, configure and use cloud services securely. Version 2.1 (07 June 2023) National Cyber Security Centre https://www.ncsc.gov.uk/collection/cloud
[12]	ETSI White Paper No. 8	Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges, June 2015, ETSI. ISBN No. 979-10-92620-03-0 etsi.org/images/files/etsiwhitepapers/quantumsafewhitepaper.pdf
[13]	ISO/IEC 31000: 2018	ISO/IEC 3100:2018 – Risk management: Guidelines.
[14]	ISO/IEC 31000: 2019	ISO/IEC 3100:2019 – Risk management: Risk assessment techniques.
[15]	Missing	Guest Post: Harvest Now, Decrypt Later? The Truth Behind This Common Quantum Theory (thequantuminsider.com)
[16]	IACR 2022/1713	Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste https://eprint.iacr.org/2022/1713
[17]	RFC 8784	Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security https://datatracker.ietf.org/doc/html/rfc8784
[18]	draft-ietf-tls-hybrid-design-08	Hybrid key exchange in TLS 1.3 https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
[19]	ETSI ETI 001	Encrypted Traffic Integration (ETI); Problem Statement.

Ref	Doc Number	Title
		ETSI GR ETI 001
[20]	GDPR.EU	What are the GDPR Fines? https://gdpr.eu/fines/
[21]	EU COM (2022) 454	Proposal for EU Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[22]	EU NIS 2	The NIS 2 Directive. Measures for a high common level of cybersecurity across the Union. Directive (EU) 2022/2555 14 Dec 2022 https://www.nis-2-directive.com/
[23]	SEC	SEC Fact Sheet. Public Company Cybersecurity; Proposed Rules https://www.sec.gov/files/33-11038-fact-sheet.pdf
[24]	Quantum Readiness Toolkit	World Economic Forum Quantum Readiness Toolkit: Building a Quantum-Secure Economy (June 2023) https://www.weforum.org/whitepapers/quantum-readiness-toolkit-building-a-quantum-secure-economy/
[25]	NIST	Quantum Information Science https://www.nist.gov/quantum-information-science
[26]	NIST	NIST Announces First Four Quantum-Resistant Cryptographic Algorithms https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms)
[27]	NIST	Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography (nist.gov)
	NSM.10	National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, The White House, May 04, 2022 https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[28]	H.R.7573	Quantum Computing Cybersecurity Preparedness Act. Public Law No: 117-260 (12/21/2022) https://www.congress.gov/bill/117th-congress/house-bill/7535
[29]	TSA	Telecommunications (Security) Act 2021

Ref	Doc Number	Title
		17 November 2021 https://www.legislation.gov.uk/ukpga/2021/31/enacted
[30]	NISTIR 8286	Integrating Cybersecurity and Enterprise Risk Management (ERM)
[31]	GOV.UK	Cyber security longitudinal survey: wave 1 - GOV.UK (www.gov.uk)
[32]		Variational quantum attacks threaten advanced encryption standard based symmetric cryptography, Zeguo Wang, Shiji Wei, Gui-Lu Long, Lajos Hanzo. *Sci. China Inf. Sci.* **65**, 200503 (2022). https://doi.org/10.1007/s11432-022-3511-5

3 Common Considerations across Risk Assessment Frameworks

In cybersecurity risk assessment, CRQCs represent not only a new threat vector in the form of a significant increase in computational power, but also a new attack vector in the form of store now, decrypt later. This does not drive a radical change in how risk assessments are performed, it does present the need to understand how CRQCs change the risk landscape. The common considerations across risk assessment frameworks, such as asset and cryptographic inventories, threat identification, qualitative or quantitative impact calculations, security control selection and monitoring, and compliance with relevant industry regulations, all need to be adjusted based on the capabilities of CRQCs.

A QCRA is a risk assessment that focuses solely on identifying and prioritising the threats and vulnerabilities that are presented by a CRQC. Any QCRA should include the current threat landscape of CRQCs, an inventory of assets and their current cryptographic protection, a methodology for prioritisation, a strategy to implement quantum-resistant controls, a capability to repeat the assessment as the threat and quantum-resistant cryptography standards evolve, and a plan to monitor the threat landscape and implementation. The prioritisation method should be based on data sensitivity, length of confidentiality, cost, and operational feasibility.

Table 3.1 shows the various steps across a few of the common risk frameworks.

Mosca's Methodology	CARAF	NIST RMF	NIST CSF	ISO 31010	ISO 27005
Identify Assets	Identify Threats	Prepare	Identify	Elicit insight from stakeholders	Communication and Consultation
Estimate CRQC Timeline	Inventory of Assets	Categorise	Protect	Identify Risks	Context Establishment
Identify threat	Risk Estimation	Select	Detect	Determine Sources of Risk	Risk Identification

Identify Lifetime and Transformation Timeline	Secure Assets through Risk Mitigation	Assess	Respond	Analyse Controls	Risk Analysis
Determine Risk	Organisational Roadmap	Authorise	Recover	Understand Consequences	Risk Evaluation
Prioritise Activities		Monitor		Analyse Dependencies	Risk Treatment
				Provide Measure of Risk	Monitoring and Review
				Evaluate Significance of Risk	
				Select Between Options	
				Recording and Reporting	

Table 3.1.1 Commonalities between various frameworks

Table 3.1 illustrates the commonalities between various frameworks focusing on execution of the risk assessment flow. Many organisations have already implemented their own framework and it may not be feasible for them to switch to a completely new framework. Understanding where process overlaps occur may help determine how adding a quantum approach to a risk framework could be feasible for your organisation.

Note that applying the risk assessment framework is an ongoing process. The identification of threats is dynamic. The discovery of new vulnerabilities, changes in government and industry regulations, the issuance of updated best practice are all on-going. The cryptographic and asset inventory changes as systems are updated.

3.1 Roles and Responsibilities

One key question when considering QRM is how to address the roles and responsibilities for existing risk and technical teams across the organisation.

This document recommends establishing governance to deal with QRM.

Quantum computing is a complex technical area. One option is to enhance the existing risk team with quantum skills. A second option is to recruit a quantum team and train them to manage risk.

In some industry verticals, the best practice seems to be the creation of a Cryptography Center of Excellence (CCoE) that becomes responsible for both the QRM and all security

and compliance topics related to cryptography, including data governance and encryption, policy setting, key and certificate management.

3.2 Threat Identification

Understanding who can deploy CRQCs for attack – Quantum Capable Threat Actors (QCTAs) – is important to determine the level of effort to protect against such risks. Until quantum computing becomes pervasive, the assumption here is that a threat actor is quantum-capable and can bring CRQCs to bear against its intended target. Whether the QCTA is a nation state, a well-funded hacking organisation, or some other type of entity becomes more relevant as CRQCs get closer to reality, but we note that today there is a low barrier to access quantum computers, which are made available via cloud platforms, with free trials and access at costs which are not insurmountable to smaller groups.

Another critical point is to understand the nature and timing of the threat, depending on the type of asset & cryptographic protocol involved. There are two broad attacks that could be used by adversaries, with different threat timing & risk profiles.

3.2.1 Store Now, Decrypt Later Threat

The Store Now Decrypt Later threat. Today it represents a significant risk to organisations with long-term sensitive data. The data is harvested now and stored, with the goal of decrypting it later when CRQCs become available. This attack is primarily against data confidentiality and is outlined in Use Case 4.1.2.

3.2.2 Trust Establishment Threat

Attacks on trust establishment, via attacks on the digital certificates. This type of attack is a real-time attack. In theory, it is only relevant when a CRQC is already available and capable of running this attack against the organisation's PKI. Mitigation of this type of an attack, without disrupting the business, must be considered. Mitigation time is the time required to build the internal capability to migrate from one cryptographic standard to another. This time is estimated to be between 5 and 20 years as experienced across the industry, depending on the size and complexity of the organisation. The attack described here is outlined in Use Case 4.2.2.

3.2.3 Hybrid Threats

Hybrid attacks are also important. In this case, an attacker uses a CRQC for one or more of the exploits in the attack chain, but the attack chain also involves classical vulnerabilities. For example, if the attacker used a CQRC to forge a digital signature on a piece of software that appears legitimate, and this leads to a system administrator being tricked into installing a classical malware on the machine. Techniques such as threat trees can be used to study these hybrid attacks, and determine both the level of risk and the best strategies to mitigate the threat.

3.2.4 How Threats Affect Assets

Assets that maintain data-at-rest are targets for "Store Now, Decrypt Later" attacks. Sets of assets that process or manage data-in-transit are additionally targets for PKI- and TLS-based attacks where a QCTA could leverage quantum computing to attack digital

certificates. Although each organisation has the assets it identifies as most critical, the categories these assets may fall into are numerous. Some examples include:

- Software based cryptographic implementations for data-at-rest for structured and unstructured data
- Software based cryptographic implementations for data-in-transit such as PKI and TLS
- Hardware based cryptographic implementations, such as Hardware Security Modules (HSM)

It is critical that any chosen risk assessment framework has an accurate and up to date inventory of assets impacted by CRQCs. It is also critical that the cryptographic protocols and other mechanisms protecting these assets are well inventoried and understood. Ideally, the asset and cryptographic inventory is monitored in an ongoing manner.

3.3 Asset and Cryptographic inventories

Since the focus here is on cryptography, asset inventories must include all areas where cryptography is used and could be impacted by a threat actor with a Cryptographically Relevant Quantum Computer, along with the business impact value of the assets involved. The inventories should cover both physical and logical locations of data and associated cryptographic implementations, particularly when an organisation leverages both on-premises and cloud-based services, whether wholly owned by the organisation or held via contractual relationships with third parties. Tying inventory to impact, data asset inventories typically play a larger role in the financial impact calculations related to data loss and business continuity, while cryptographic inventories play a larger role in the decisions around control selection and tangible changes to information security infrastructure. The inventory process itself is two-fold covering assets and cryptography.

3.3.1 Asset Inventory

The organisation must conduct an inventory of assets. This inventory is typically part of a data classification procedure, undertaken during classical risk assessments for any organisation with sensitive assets. It is equally relevant for Quantum Risk Assessment (QRAs). The sensitivity of the data assets must be assessed, their longevity, their value (time to replicate or value if lost or duplicated), as well as their classification under the current relevant regulation (i.e. regulatory repercussions if the data confidentiality or integrity is infringed).

3.3.2 Cryptographic Inventory

At the same time, the organisation must conduct an inventory of the actual cryptographic artifacts and protocols used to protect access to the data assets. This could be in the form of encryption of the assets (protecting data confidentiality and integrity), and/or the authentication and authorisation mechanisms used to access the assets. The cryptographic protocols, required to be used, are largely defined by governments and regulatory authorities for a given industry and level of asset sensitivity. While most conscious organisations monitor cryptographic artifacts in line with risk and audit recommendations, the importance of cryptographic inventories is boosted significantly by the emergence of CRQCs.

3.4 Impact Calculations

The goal of this section is to calculate potential loss to the business should the QCTA, using CRQCs, successfully exploit a vulnerability. At the time of this writing, the estimated future financial loss is greater than zero because of the capabilities that CRQCs represent relative to the strength of present-day cryptographic algorithms.

Any calculation of impact is dependent upon the asset inventory and associated asset values within that inventory. It is also dependent on compliance with the mandated or recommended cybersecurity standards and best practices, where non-compliance can lead to significant fines and penalties, loss or reputation, loss of customer-base, and revenue overall.

The actual monetary value of potential loss can be hypothetically calculated under certain assumptions, such as assuming that an entire dataset can be decrypted using a CRQC. Here the potential loss is manifold: firstly, if the asset relates to intellectual property of the organisation, then the financial loss can be estimated based on the asset value determined during the asset inventory phase referenced in section 3.3. One needs to build a kill chain to determine if the assets have been duplicated. Next, it is necessary to determine if the assets are corrupted or deleted. Those steps determine the value of the asset, including their replication value (how many resources it takes to re-create that asset). The threat of exposure of sensitive data may also make the organisation vulnerable to extortion and blackmail by hackers, a rising trend in ransomware attacks. This is essentially a question of business continuity and its livelihood for the business.

If the decryption of the asset exposes sensitive regulated data then the impact is increased by penalties for non-compliance (includes: personally identifiable data (PII) protected under financial regulation (e.g. Payment Card Industry – Data Security Standard (PCI-DSS)) or healthcare regulation (e.g. Health Insurance Portability and Accountability Act (HIPAA)). Regulations around cybersecurity and data protection, such as the General Data Protection Regulation [20] (GDPR) in Europe, mandate stringent penalties for the leakage of sensitive personal data, up to 4% of the organisation’s global annual turnover or EUR 20 million (whichever is higher). These penalties can be reduced or offset if the organisation can demonstrate ongoing compliance with industry cybersecurity best practices (e.g., NIST/ISO recommendations). New regulations around cybersecurity are on the rise – from the EU Cyberesilience Act [21] to NIS2 [22], to proposals by the US Securities and Exchange Commission (SEC) for new regulations [23] for market entities (financial institutions), which mandate C-Suite and board responsibility for cyber resilience, as part of the board’s critical risk and audit function. The US government [28, 29] has also mandated federal agencies to improve security in the face of quantum threats and prepare for migration to post-quantum cryptographic standards.

Outside of loss of assets, other impacts like fines and judgments, compliance penalties, or even cyber insurance premium increases play an ever-increasing role in the overall risk calculation. Reputational loss, impacting the organisation’s competitiveness, which may affect the role of the CEO and other executives within the impacted organisation, must also be accounted for. For-profit companies must consider brand damage and reputation from a “customer perspective”, leading to revenue losses.

3.5 Control Selection

The existing regulations around cybersecurity and data privacy, as well as the mature cybersecurity risk frameworks, provide a wealth of existing best practices which may be used as the foundation for an extended Quantum Risk Assessment.

QRAs typically involve deeper analysis and controls in the following areas to account for the risk of CRQCs:

- continuous asset classification, notably around the longevity of sensitive data,
- ongoing inventory of cryptographic protocols, notably on the analysis of deprecated or non-quantum-resistant protocols,
- ongoing inventory of cryptographic protocols and quantum awareness of third-party vendors and suppliers,
- ongoing identification and analysis of emerging and changing threats in the timeline of a CRQC,
- ongoing analysis of compliance with dynamic government and industry regulations, standards and best practices relevant to quantum safety.

While several quantum-resistant solutions have been proposed and are being researched, this document only addresses risk and prioritisation of the cryptographic methods using Post-Quantum Cryptography. Hybrid solutions [5], which incorporate both classic and quantum-resistant cryptography, can also be implemented to reduce risk in the interim or for backwards compatibility. The chosen solutions are dependent on the individual use case and any relevant standards or regulations as well as the individual risk appetite of the enterprise. Multiple governments and international organisations are already establishing control recommendations for addressing quantum risk [24]. These recommended approaches and mitigation measures apply to government, as well as regulated industries such as critical infrastructures, telecoms networks, financial institutions and utilities…etc…

Additional information on the current state of the NIST post-quantum cryptography standardisation project can be found here: Post-Quantum Cryptography | CSRC (nist.gov) [6].

3.6 Residual Risk

As is the case with all risk assessment processes, once the risks are identified and measured and a plan of action is devised, there is still the chance for residual risk to be present after the mitigation measures have been implemented. This is typically the case when either risk acceptance (see section 5.1.3A) or risk reduction (see section 5.1.3B) are selected as the risk response. If the risks are accepted, meaning the organisation does nothing other than monitor the risk, then residual risk is equivalent to inherent risk since no new controls or other behaviour changes are performed. With risk reduction where the organisation implements one or more controls to reduce the risk, the residual risk is some remaining subset of inherent risk based on the efficacy of those implemented controls. In the case of risk transfer as a mitigation strategy, an organisation contracts with a third party that accepts the burden of data security either operationally or through a vehicle like cyber insurance. Unless there is a guarantee that 100% of the risk is transferred, there is some residual risk remaining that must be accounted for, which is similar to risk reduction.

Regardless of the qualitative or quantitative rating of residual risk, the organisation must understand that there is some form of risk left over that should, at a minimum, be monitored.

4 Quantum Cryptanalytic Risk Assessments

There are currently two published QCRAs: A Methodology for Quantum Risk Assessment and Crypto Agility Risk Assessment Framework (CARAF). Either can be used to conduct a standalone QCRA.

4.1 A Methodology for Quantum Risk Assessment

A Methodology for Quantum Risk Assessment [7] provides insight on conducting a QCRA. This was written by Dr. Michele Mosca and John Mulholland. Mosca's "x, y, z" quantum risk model is frequently referenced in quantum risk works, including this one. This six phase QCRA aligns with the NIST Risk Management Framework [2] and can be used to expand any Risk Assessment (RA) to include QCRA elements.

4.1.1 Framework

The Framework consists of six (6) Phases, as follows:

- **Phase 1:** *Identify and document information assets, and their current cryptographic protection.*

  Create an inventory of important assets, with an emphasis on sensitive or valuable information assets. Inventory all of the cryptographic mechanisms used to protect these assets, including all embedded cryptography and how any encryption mechanisms are generated, stored, and applied. Asset value, access control, back up recovery, and end of life should be documented. Any legal or regulatory requirements that influence these assets or cryptographic mechanisms should also be documented.

- **Phase 2:** *Research the state of emerging quantum computers and quantum-safe cryptography. Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography.*

  Continuous quantum research should be conducted to understand the quantum threat landscape. The methodology states, "Having either a dedicated team of quantum experts or a relationship with an organisation specialising in quantum technology is critically important to completing a QRA." Third party experts, such as consultants or consortia could also be consulted in this phase.

- **Phase 3:** *Identify threat actors, and estimate their time to access quantum technology "z".*

  Determine the estimated time when CRQC technology is either scalable or available to threat actors. This time frame offers the "z" in Mosca's model.

- **Phase 4:** *Identify the lifetime of your asset's "x", and the time required to transform the organisation's technical infrastructure to a quantum-safe "y".*

Assess the time it takes to migrate your assets. Each asset has a shelf life of "x" and the length of time to implement quantum resistance is "y". Security shelf life includes any regulations that govern how long the data is to remain secured.

- **Phase 5:** *Determine quantum risk by calculating whether business assets will become vulnerable before the organisation can move to protect them. (x + y > z?)*

  If the shelf life of asset "x" plus the time to implement quantum resistance "y" is greater than the determined "z", then the asset is at risk and should be prioritised. This is illustrated in the Figure 4.1.1.1.

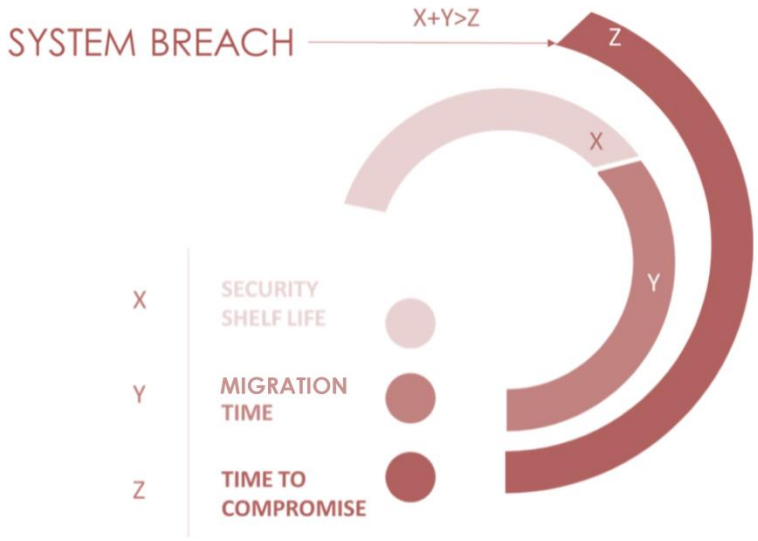

Figure 4.1.1.1 QRA Variables

- **Phase 6:** *Identify and prioritise the activities required to maintain awareness, and to migrate the organisation's technology to a quantum-safe state.*

  The quantum threat landscape and mitigation methods should continuously be monitored, and "z" should be modified accordingly. Standards and regulations on quantum safety and mitigation methods are also changing and should be tested to accurately determine "y".

4.1.2 Framework Drawbacks

Determining the risk using Mosca's method almost always creates a low-risk label when "z" is 15 – 20 years. This also prioritises items with a longer security shelf-life instead of high impact areas, with little to no required security shelf-life. This is designed to highlight sensitive or critical data that could potentially be exposed in the future, such as through a store now and decrypt later attack. Assets are either at risk or not at risk without consideration of risk level to aid in the prioritisation. For example, items with high impact, such as the telecommunication control plane, may have a lower "x" or "y" value, but should not be labeled as no risk (see 4.2.3 Use Case).

An extension to Mosca's theorem is offered that considers potential overlap of "x" and "y". Mosca's theorem does not consider use cases in which "x" and "y" are happening concurrently. Even if the migration process has started "y", the "x" timeline continues. This is important as the migration process can take a significant amount of time in some use cases.

4.1.3 Use Case Example

The following use case examines an enterprise that focuses on gNodeB (gNb) base stations used in 5G networks. In a gNb, there is both user plane and control plane data. This use case focuses on the user plane data as an asset and therefore sensitive customer data.

- **Phase 1:** *Identify and document information assets, and their current cryptographic protection.*

  These data instances present data in rest and data in transit. There are also symmetric and asymmetric methods of cryptographic protection. Some of the asymmetric protocols used are TLS, IKE, and PKI. All of these are quantum vulnerable.

Asset	Data State	Data Sensitivity	Methods of Protection
User Plane Data	Transit	High	IPSec, DTLS

Table 4.1.3.1: Identify and document information assets – Example

- **Phase 2:** *Research the state of emerging quantum computers and quantum-safe cryptography. Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography.*

  The enterprise uses its QRM team to gather information on the emergence of a quantum computing. Quantum-resistant algorithms are not yet (September 2023) standardised or incorporated into protocols.

- **Phase 3:** *Identify threat actors, and estimate their time to access quantum technology "z".*

  The enterprise's QRM team believe that CRQC development is between 5 – 10 years away. They also believe that the attackers targeting this sensitive user data has immediate access to a CRQC. The enterprise assigns a z value of 5 years.

z = 5

- **Phase 4:** *Identify the lifetime of your assets "x", and the time required to transform the organisation's technical infrastructure to a quantum-safe "y".*

  There are no standards that give a specific timeframe for data to remain secured while traveling over the user plane. However, the enterprise gives the data a security shelf life of 10 years.

The enterprise determines it would take 3 years for the new PQC algorithms to be integrated into protocols and industry standards and another 2 years to upgrade equipment to meet these standards, creating a migration timeline of 5 years.

x = 10 y = 5

- **Phase 5:** *Determine quantum risk by calculating whether business assets will become vulnerable before the organisation can move to protect them. (x + y > z?)*

x + y = 15 z = 5 15 > 5

The asset is at risk and should be prioritised to migrate to a quantum-resistant solution.

- **Phase 6**: *Identify and prioritise the activities required to maintain awareness, and to migrate the organisation's technology to a quantum-safe state.*

The enterprise identifies this asset as high risk. It follows the PQC standardisation process closely and prepares by creating a migration strategy.

4.2 Crypto Agility Risk Assessment Framework (CARAF)

CARAF: Crypto Agility Risk Assessment Framework was published by Comcast Cybersecurity [3] in April 2021. This was the first instance of a risk assessment framework directly aimed at the quantum threat with crypto agility as the solution. CARAF refers to **crypto agility** as the ability to replace existing cryptographic primitives, algorithms, or protocols with an alternative. CARAF is a five-phase process.

4.2.1 Framework

- **Phase 1:** Identify Threats

Start by identifying the threats and the timeline for future risks. For the quantum threat, use recently published quantum threat reports and research to determine the arrival of a CRQC. This should continuously be evaluated as the threat landscape and timing is constantly changing.

Different threat categorises, such a regulatory requirement, new vulnerabilities, or CRQC realisation, impact assets differently and should be noted. Not all assets are affected by the threat and should be considered out

of scope. For example, older systems may be phased out prior to a mitigation implementation and should not be include in the next phase.

- **Phase 2:** Inventory of Assets

  Only inventory assets that are impacted by the threat identified in phase 1. This differs from other risk assessments. Assets must be prioritised based on sensitivity. Inventory must include information related to the management of secrets such as keys, passwords, API tokens, and certificates. Assets and how their cryptographic protections are implemented, their location, who owns them, and their lifecycle, such as back up or recovery, must also be annotated in the inventory.

- **Phase 3:** Risk Estimation

  This builds on Mosca's x + y > z model by adding a scoring component. The scoring methods labels risks between a 1 and 4 or low risk to critical, respectively.

  Cost to implement specific risk mitigation methods is also consider in the risk estimation phase. A more crypto agile asset is less expensive to migrate.

  The risk mitigation strategy depends on the organisational risk tolerance and the expected value of risk determined by the Timeline and Cost.

  Risk = Timeline x Cost.

- **Phase 4:** Secure assets through risk mitigation

  Risk mitigation is offered through three options:

  1. Secure the asset by spending resources
  2. Accept the risk and maintain the status quo
  3. Phase out impacted assets

- **Phase 5:** Organisational Roadmap

  Organisation must build a roadmap, processes, and policies for implementing crypto agility. This must tie in some common practices such as the incident response plan, third party risk assessment, security architecture reviews, product development, and change management. The updated practices should include removing deprecated algorithms, addition of new cryptographic requirements, and reviews of existing tools to determine if additional technical solutions are necessary.

4.2.2 Framework Drawbacs

"Phase 4: Secure assets through risk mitigation" leaves out risk transference, which might be an option in the future using various third party services or insurance. CARAF could also be expanded to include another phase after Phase 4 and before Phase 5. This new phase would be an analysis after the risk mitigation, to analyse its effectiveness and identify any residual risk.

4.2.3 Use Case Example

The following use case examines an enterprise that focuses on gNodeB (gNb) base stations used in 5G networks. Securing the telecommunications control plane requires that gNb authentication and integrity are protected. Protecting confidentiality is also important, to prevent attackers creating a map of the telecommunication system, discovering the types of systems and protocols used (which would make it easier to exploit known vulnerabilities). The greatest threat to the control plane is loss of availability.

Telecommunication providers run reference models (testbeds) to test the resilience and implementation security of new products, and updates to the control plane software or hardware implementation. The design, test and acceptance process for new telecommunication products and services can take months or even years to complete, and therefore it is already necessary to begin this process (if it has not already been begun).

- **Phase 1:** Identify Threats

  One of the most critical pieces of 5G infrastructure is the OAM/OSS. If an adversary gains control of the OAM/OSS, they have control of the network, could bring it down, and have access to all data being transferred. This use case focuses on a specific PKI instance.

  The threat identified is the use of a CRQC against the current PKI instances.

- **Phase 2:** Inventory of Assets

  A PKI instance is used to establish authentication in the connections between the gNb and OSS/OAM over the control plane by means of IKEv2. The PKI instance uses IKEv2.

- **Phase 3:** Risk Estimation

  Store now, decrypt later does not add additional risk to this instance. Real time attacks pose the largest threat. The enterprise estimated that a CRQC will be developed in the next 15 – 20 years. The enterprise estimates another 1 – 2 years before a capable threat actor has possession of a CRQC. The range for z = 16 – 22 years. The enterprise chooses z = 16 as its estimate for the threat realisation and labels it as a medium risk based on the following logic and table 4.1.

z = 16

  The enterprise estimates that it takes one year to roll out a new software patch to all existing systems that update IKEv2 to the IKEv2 with quantum resistance. For use cases purposes, we assume that a IKEv2 extension that provides quantum resistance has been standardised.

y = 1

There is no standardised security shelf life to provide figures for x but the enterprise determines equipment lasts for 10 years and that data should remain secure through its life time of 10 years. Therefore, x = 10.

x =10

x + y = 11

z = 16

11 < 16

The enterprise determines that this instance is at low to medium risk by using the proposed risk estimation table from CARAF (see below).

Timeline	1 – Low Risk	2 – Medium Risk	3 – High Risk	4 – Critical
x (Shelf-life)	5	10	20	20+
y (Mitigation)	0 – 5	6 – 10	11 – 20	20+
z (Threat)	20+	10 – 20	5 – 10	0 – 5

Table 4.2.3.1 CARAF Risk Levels (timeline risk estimate is in years)

The enterprise cost of implementing the risk mitigation, or the IKEv2 extension that provides quantum resistance, is calculated. The enterprise determines that the asset has a high level of crypto agility. The cost includes creating a software patch with the quantum-resistant IKEv2 extension and it can be included in the next scheduled update. The enterprise determines that as a low-cost mitigation method.

- **Phase 4:** Secure assets through risk mitigation

  1. Secure the asset by spending resources

  2. Accept the risk and maintain status quo

  3. Phase out impacted assets.

Given the low cost of the mitigation and the criticality of the system, the enterprise chooses option 1. Secure the assets by spending resources. The enterprise plans to upgrade the asset to the extended quantum-resistant IKEv2.

- **Phase 5:** Organisational Roadmap

  The enterprise must create a program to roll out the upgrade to the extended quantum-resistant IKEv2. A strategy and roadmap are created to ensure all systems are upgraded over the next year.

5 Risk Assessments w/ QCRA Best Practices

5.1 NIST RMF & CSF

5.1.1 Baseline

NIST Risk Management Framework (RMF) [2] is a multilayered organisation-wide approach to security, privacy, and cyber risk management activities as part of the system development life cycle. RMF is used across industries, systems, and technologies. In the case of organisations using NIST (or NIST-based approach) their long-term strategy is usually aligned with their determined Risk appetite and resource pool.

Figure 5.1.1.1 illustrates RMF steps.

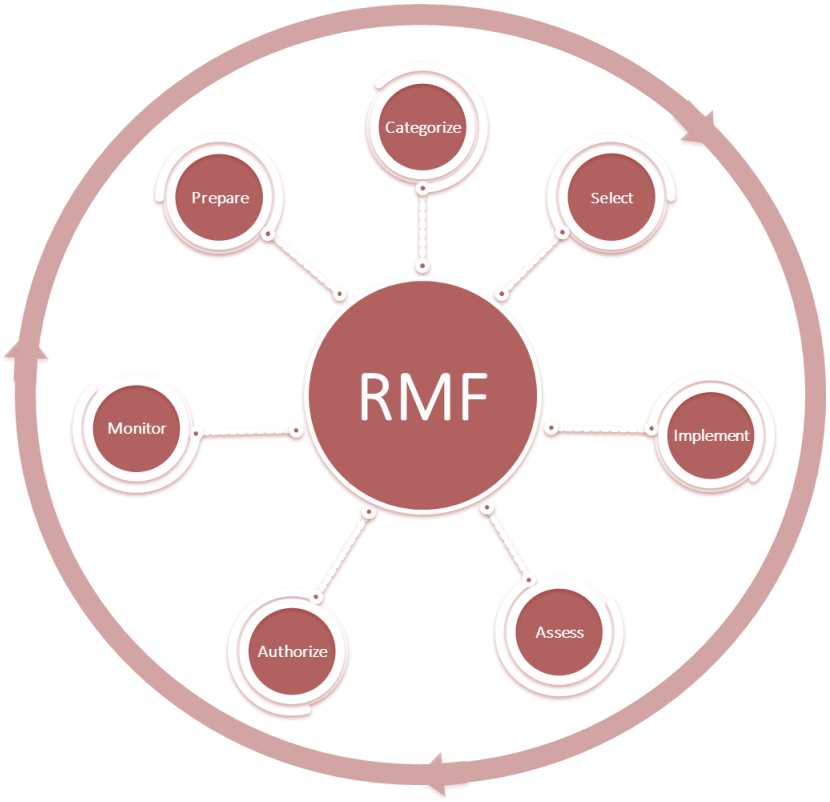

Figure 5.1.1.1 RMF steps.

There are several interconnected guiding principles for the organisations using NIST RMF. The key ones are:

- Understand and reduce Cybersecurity Risks through qualitative and/or quantitative risk management measures;
- Apply system development lifecycle (7 steps – add link to diagram/create new one);
- Integrate Cybersecurity risk management deliverables into Enterprise Risk Management.

A fourth principle, for organisations starting or migrating to the NIST framework(s), is recommended:

- Assess status and align to specific implementation tier (e.g. “as is” vs “to be”).

In parallel NIST Critical SF [4] is designed to an organisation’s cybersecurity program and posture, integrating and aligning cybersecurity risk management with RMF.

NIST CSF [4] is currently operating on version 1.1 and version 2.0 is expected in early 2024. Given that the update is expected to be a long process NIST encourages organisations to adopt v1.1 as backwards compatibility will be considered on the updated version 2.0. The CSF Functions are illustrated in the Figure 5.1.1.2.

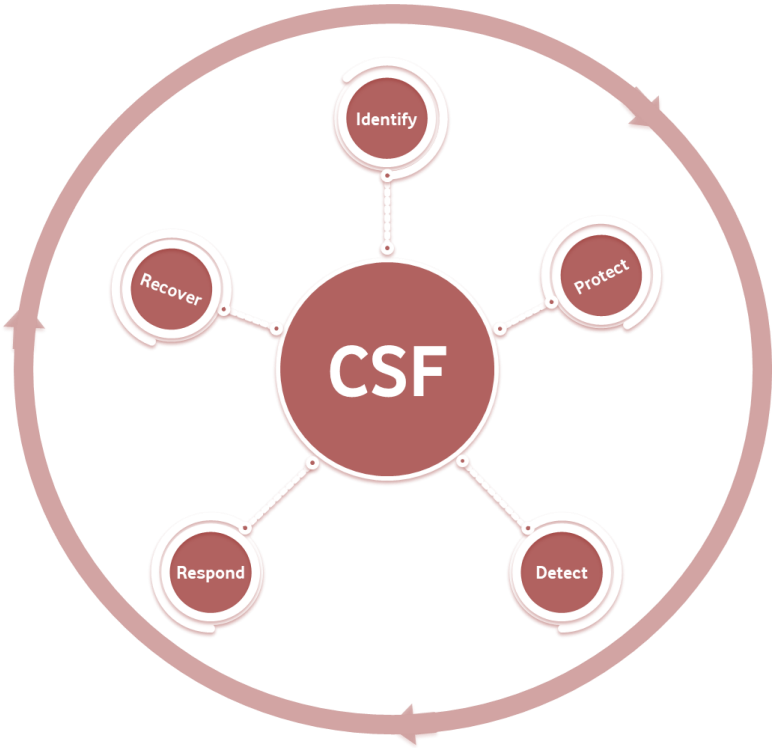

Figure 1.1.1.2 CSF Functions

5.1.2 Quantum-Resistant Cryptographic Algorithms (QRCA) Additions

As an organisation that enables innovation NIST is one of the most active stakeholders in preparing organisations, frameworks and industries for CRQC and QRM. Starting with their

work in quantum science [25], their efforts towards Quantum Resilience and QRCAs [26] and the upcoming special publication on Migration to Post-Quantum Cryptography [27], these initiatives pave the way towards quantum resilience across industries, especially telco.

5.1.3 Mapping and Managing Risk

Once the risk level is measured and mapped on an impact and likelihood matrix, also known as a heat map, it is managed through a specific response, adapted to the organisation's risk tolerance through acceptance, avoidance, reduction or sharing the risk.

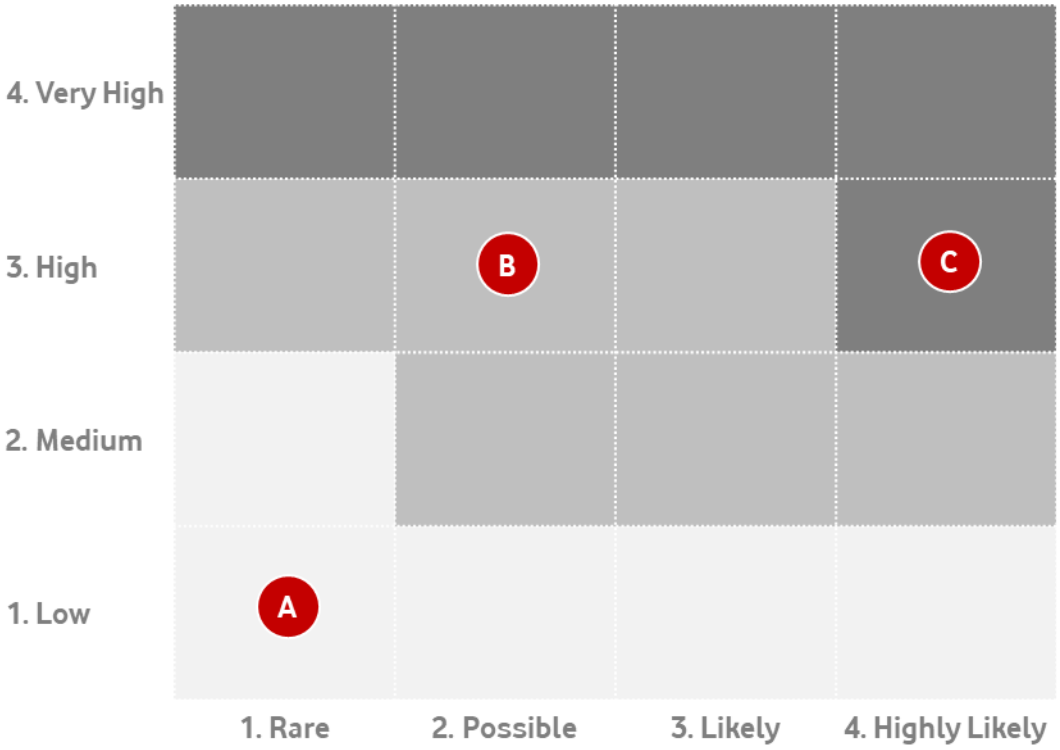

Figure 5.1.3.1 Mapping and managing risk

5.1.3.1 A. Data that will no longer be usable in 2030

- **Scenario:** Company Y is reviewing annual risk reporting and discovers a Rare risk with a low impact. The risk is aligned with the company's risk tolerance level.
- **Threat:** Unintentional data leak – Legacy telco policy on employee professional development.
- **Business impact:** Limited as information is labelled Internal but not Classified.
- **Risk decision:** The business decides to accept risk given low impact, rare likelihood and impacted data type (legacy).

5.1.3.2 B. Data that will only be of marginal value in 2030

- **Scenario**: Company W is reporting global levels for insurance purposes and finds a High Risk with a Possible likelihood. The risk is close to tolerance level.
- **Threat**: Destructive attack – Cyber-attacks may not be prevented or adequately managed.

- **Business impact**: Failure to adequately protect our customer information from unauthorised access/ removal of customer data. May result in the imposition of several fines as well as reputational damage.
- **Risk decision**: Telco decides to reduce risk through risk mitigation strategies.
- At the time of writing, new regulations from the US federal government are leading the way in establishing best practices in mitigation of threats from CRQCs [28] [29].

5.1.3.3 C- High Value Data in 2030

- **Scenario:** During the course of quarterly risk assessment Company Z is dealing with a Highly likely / High impact risk. The Risk is mapped outside the company's tolerance level.
- **Threat:** External Data Compromise – PCI information on existing customers
- **Business impact:** Failure to comply with data protection and privacy rules may result in the imposition of several fines as well as reputational damage.
- **Risk decision**: Assumption of accountability by the business regarding the implementation of appropriate measures to address this risk is key in applying the RMF. The business decides to implement alternative infrastructure in order to avoid the risk, by bypassing vulnerable components altogether. Business impact / Risk is avoided.

5.2 ISO/IEC 27000 Family

5.2.1 Overview

The ISO/IEC 27000 family of standards addresses how an organisation should approach risk management for information security. It covers the whole process from initiating a risk management process in an organisation that may not have previously had one, to certification. While the ISO/IEC 27000 family has similarities to other systems, such as the one provided by NIST, many organisations worldwide have chosen to adopt ISO/IEC 27000. For example, a 2022 survey found that 47% of UK business in the IT and information security space have ISO 27001 certification [31].

The core standard against which compliance is assessed is ISO/IEC 27001 [8] (the current version is 27001:2022). This formal framework includes scoping, risk assessment, gap analysis and the development of an Information Security Management Systems (ISMS), and the approach to certification. This standard adopts a risk-based approach to ISMS, with a focus on identifying, assessing, and treating information security risks, and protecting the confidentiality, integrity and availability of information assets. This is a standard to which organisations can claim compliance.

ISO/IEC 27002 [9] (Code of Practice for Information Security Controls) provides detailed guidance on assessing risks to an ISMS and applying mitigations i.e. implementing security controls. It is a practical guide to achieving the goals of ISO/IEC 27001.

5.2.2 ISO/IEC 27005

ISO/IEC 27005 focuses specifically on the risk management process for information systems.

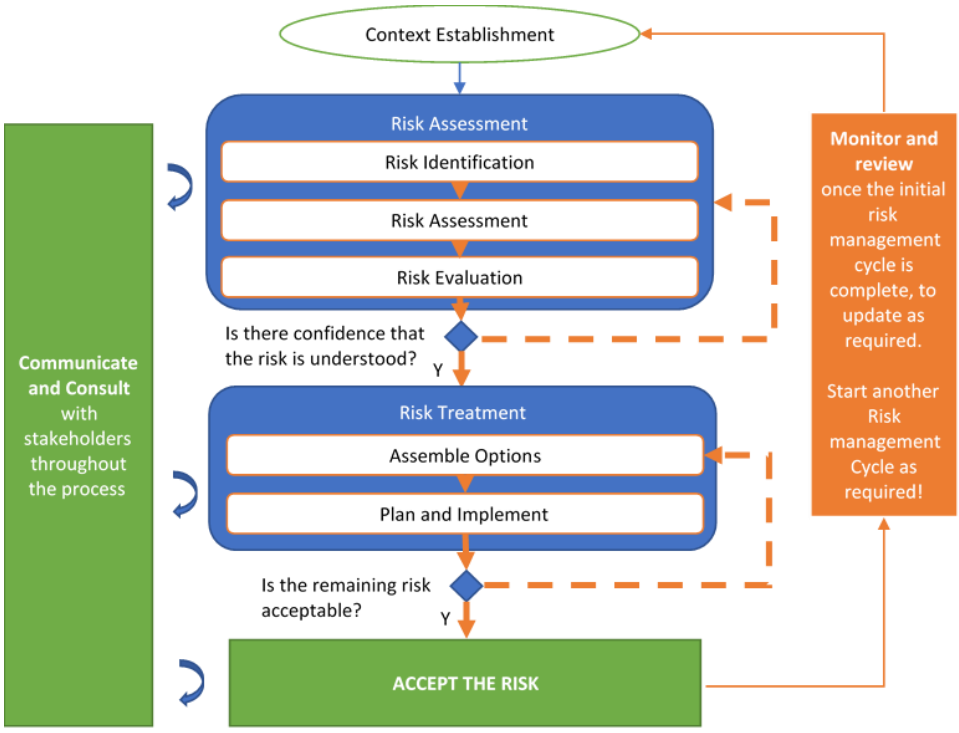

Figure 5.2.2.1 After ISO-27005:2022 Figure 1, Information Security Risk Management Process

The main steps and sub-steps in the ISO/IEC 27005 [10] risk management process are:

Context establishment

An initial step in the process in which the internal (the organisational) and external (the wider environment in which the organisation operates) context of the risk is established. This includes assessing the risk appetite of the organisation (including factors such as reputation, risk/reward profile, and human factors such as whether the organisation provides services to vulnerable people in the context of which high risk is not tolerable). It also considers the resources of the organisation (such as access to funding, and the transferability/extensibility of existing processes and staff). A set of risk criteria for risk acceptance and risk treatment, specific to the organisation, may be established in this step.

Risk Assessment

Risk assessment is the step in the process in which the risk is studied. It comprises the following sub-steps:

- Risk Identification: The risk is named and described.
- Risk Analysis: The risk is analysed, assessing its causes, likely severity, and likely consequences (impact).

- Risk Evaluation: An evaluation is made of the severity of the risk, and whether it falls within a risk criterion (from a set of criteria evaluated at the context stage) that is considered impactful to the organisation. A decision is made about whether this risk requires risk treatment at all, or can be accepted without treatment.
- Decision: is the understanding of the risk, and confidence in the assessment of the risk, sufficient to proceed to Risk Treatment? If yes, proceed.

Risk Treatment

- Assembling Options:

  This step involves drawing up a list of suitable options for risk treatment. These usually mitigate the risk with security controls (including procedural, detective and technical controls, for example). But the available options may include the option to avoid (not accept) the risk (and therefore not to carry out actions that incur the risk), as well as to share or transfer the risk e.g. by outsourcing an activity.

- Plan and Implement:

  A plan for which risk treatment options will be implemented is made. If this involves implementing security controls, then designs and or processes for these controls are drawn up. These are then implemented by the relevant professional staff, usually within the IT department.

  Decision: Assess Remaining Risk and decide if it is acceptable.

  Unless the risk has been avoided, after applying risk treatment, there is some remaining risk. An effort is made to assess what is this residual risk. (For example, if the risk is that an adversary opens a door, and the security control is a padlock, then the remaining risk is that the adversary forces open or picks the padlock). A decision is made whether the organisation can accept the remaining risk (with reference to the original context step, which studied the relevance of this risk to the wider organisation and external environment).

  Following this, there is a decision to either ‘Accept the Remaining Risk’ or return to another cycle of risk treatment to identify a better set of controls to further reduce the risk.

Communicate and consult

This step involves documenting and communicating with the stakeholders, particularly those involved with taking responsibility for the risk treatment actions, or with overall management of organisation risk. Feedback (consultation) may be sought from these stakeholders. This is an ongoing process that can be used at all stages of risk management.

Monitoring and reviewing

Once the first risk management cycle has completed, and a risk has been treated and accepted, the process is not over. Monitoring and reviewing is a continual process that initiates at this point, and can trigger a new risk management cycle for the risk at any time. This step involves monitoring and reviewing the risk and its assessment and

treatment. The assessment of a risk might change over time (e.g. its anticipated impact might increase in severity). Similarly, the treatment selected might prove to be not effective enough. If monitoring reveals this, this prompts a review, and possibility re-initiation of the risk assessment and/or risk treatment steps.

5.2.3 Application to QCRA

The context establishment step of ISO 27005 [10] is of particular importance in deciding how much resource an organisation deploys (e.g. a telecommunication provider) in preparing for the quantum threat (for example, in building and testing new versions of applications and services that use post-quantum cryptography). This step includes a realistic assessment of the different threats to the application or organisation, and the resources available to address these threats. For example, a smaller company may not have a sufficiently large IT or cybersecurity resource. In this context, the company must focus on basic security tasks; such as backups, monitoring and applying critical patches for systems and applications that are managed by the organisation, and potentially adopting a cloud-first [10] strategy with a reputable supplier. However, the majority of telecommunication providers would be expected to have sufficient resource to be able to dedicate responsibility for creating and implementing a quantum readiness plan.

5.2.3.1 Risk Assessment Step

The risk assessment step requires an understanding of the capabilities and limitations of quantum computers, as well as the bigger picture of practical security. The person or team making the risk assessment does not have to have the capability to program a quantum computer, but they must be able to fully understand the documents and guidance that explain the technical nature of the risk to cryptography.

5.2.3.2 Details of Risk Posed by CRQC

For example, a quantum computer may be able to accelerate a ‘brute force’ (exhaustive search) attack on a symmetric key encrypted cipher string with known plaintext, or find a collision for a hash value, but this is not an exponentially accelerated attack [12]. Similarly, the risk assessment team must be able to identify the aspects of security which are unaffected by quantum computers: e.g. an adversary, with no prior knowledge or other resources, who tries to guess a password to an online resource is not helped by possessing a quantum computer unless s/he can also gain access to the password file containing a password crypt or hash value and salts, where a quantum computer may provide advantage by accelerating (with Grover’s algorithm) an exhaustive search. We note that there is a risk that stronger attacks on particular symmetric schemes in some scenarios may emerge – for example [32].

The existence of effective quantum algorithms to break asymmetric cryptography such as RSA and Elliptic Curve based systems impacts all of the key pillars of information security: **confidentiality** (if encryption keys are recovered during key-exchange), **integrity** (if digital signatures can be forged, and if authentication can be spoofed) and **availability** (if these attacks can be used to disrupt and deny services).

5.2.3.3 Risk Treatment Step

In 2023 the risk treatment step is likely to include creating a plan which prepares for the growing future risk of quantum computational attack. It is likely to include a discovery phase

of critical systems, including inventories of cryptographic schemes used today by these systems. This step integrates with “monitor and review”, since both the velocity of the developing threat, and the success and practicality of the emerging approaches to combat it (such as the resilience of quantum-resistant algorithms, and the readiness of quantum key distribution satellites) are constantly evolving. The risk treatment is very likely to include development of prototypes that implement the emerging quantum-resistant standards, and the development of test processes (including reference models i.e. representative network testbeds), by which the performance and suitability of the quantum-ready prototypes are assessed before being deployed into the live network.

5.2.3.4 Impact on Supply Chain

New regulations, such as the UK Telecommunications (Security) Act 2021 [29], require that all vendors in the telecommunications supply chain are security assessed. In the near future, the vendor security assessment is likely to include understanding the roadmap towards a quantum-safe version of their product or service. Therefore, organisations should engage with vendors in the discussion of this issue early on, so that vendors can be prepared for the expectations of telecommunication providers to procure quantum-secure ready technology. Vendors can also work with telecommunication providers in evaluation of the resilience and performance of quantum-resistant versions of hardware and software in testbed environments.

5.2.4 Use Cases in Practice

Example: Securing sensitive customer data in managed services, for example medical and genetic data handling:

Many telecommunication providers offer managed services to customers, which may involve storing, processing and/or transporting sensitive data. The archetypal example is medical and genetic data. Where the managed service includes elements such as encryption, key management or secure storage of data at rest, then the telecommunication/managed service provider takes at least some responsibility on behalf of the customer for information security. The context in which risk to customer data is assessed should include the requirement for this data to remain confidential for decades, or (as in the case of genetic data), indefinitely. Such risk assessment discussions should take place between the managed service provider and the customer or stakeholder who holds ultimate responsibility for the data. The threats are two-fold – firstly the immediate threat of store now and decrypt later attacks, and secondly readying systems for the date that it is believed that a CRQC may exist, which may come quite suddenly. When a CRQC is available, the threat is not only retrospective decryption that exploits vulnerable key exchange methods, but also, for example, exploiting vulnerable authentication methods to enable man-in-the-middle attacks.

5.3 ISO 31000 Family

The ISO 31000 family focuses on providing principles, guidelines and techniques for effective risk management. It covers all types of risks faced by organisations, including strategic, operational, compliance, financial and geopolitical risks, and therefore both encompasses and goes far beyond the information security remit of the ISO/IEC 27000 family. It is designed to help organisations establish a structured approach to risk

management, enabling them to make informed decisions, in order to increase organisational resilience in a pragmatic and proportionate way.

The core standard is ISO 31000:2018 [13] (Risk Management guidelines). This publication is a guide to general risk management for an organisation, which considers the scope (objectives and activities of the organisation, the external and internal context in which those objectives are set, and the risk criteria including biases and uncertainties), the risk assessment (including likelihood, magnitude, complexity, connectivity and volatility) and the risk evaluation and treatment. A complementary publication, ISO 31000:2019 [14] (Risk assessment techniques), guides organisations in the selection of methodologies and tools to assess and analyse risks. Together the standards provide a realistic and holistic approach to the broad risks that an organisation faces, and which considers the resources available to the organisation, and the consequences of deciding to implement security-controls, in terms of usability and cost.

As an example of the broader risk context, consider a telecommunication provider with limited resources which faces severe risks to business continuity. This may be due to a conflict zone, regional political instability or natural disaster, which creates risks to the security of their business location, the uninterrupted supply of utilities and/or availability of critical components. The provider would typically prioritise treating these (crisis) risks before allocating resources to prepare for the quantum risk to information security. Sadly, 2023 has provided us with many examples of such operational environments.

This pragmatic approach is complementary to the guidance provided by ISO-27005 [10]. This risk framework is useful in helping individual organisation see the big picture of their risks and the impacts, to perform cost-benefit analysis, and to respond according to their resources and responsibilities.

5.4 Supply Chain and Business Partnerships

The focus of this paper has primarily been around the direct impact of a quantum risk for a particular organisation. However, through contractual relationships most organisations rely on the support of suppliers and business partners to do business. Introducing the concepts of quantum risk into these relationships should be included in an organisation’s overall risk plan. Whether that is through specific security requirements drafted into a formal agreement, or, at a minimum, a general requirement that suppliers and business partners be educated and aware of how quantum computing and a QCTA could adversely impact both companies through an integration, automated or otherwise.

Third party services and toolsets are also being developed to aid in the migration to quantum resistance or crypto agility.

Automated cryptographic discovery tools inspect source code, deployed applications and network connections to identify the uses of cryptography, and to classify the cryptography (symmetric or asymmetric) and its characteristics (algorithm and key length). This information is stored in a cryptographic inventory or Cryptographic Bill of Materials (CBOM). This allows organisations to understand and manage the deployed cryptography, and is the first step required to perform a QCRA, plan the migration to PQC, and monitor the on-going process.

Third party and open source tools are available for cryptographic discovery and inventory.

5.5 Store Now and Decrypt Later Attacks

To protect from store now and decrypt later attacks, high risk assets must be made quantum-resistant as soon as possible. Determining a useful shelf life, outside of security shelf life, helps to determine the risk. Information that has expired, changed, or is no longer relevant by the advent of a CRQC, does not present as much of a loss. Simultaneously, decrypting data pools, even with a CRQC, is a costly and time-consuming task. Only the most impactful data is targeted.

If a threat actor has already harvested highly critical data, the best option is to prepare for the exposure of this data and continue to migrate to quantum resistance. Like other business continuity and recovery plans, the enterprise should create a recovery plan and a strategy for dealing with potential unveiling of the data [15].

6 Conclusion

History has shown that technology evolves at a rapid pace, and quantum computing is no different. Today’s organisations must consider how quantum computing impacts their operations at the data level, the systems levels, and wherever else cryptography is implemented. This consideration typically takes the form of a risk assessment, either quantum-specific or adapted to incorporate the unique challenges that CRQCs bring to the table. While each organisation approaches the risk assessment process in its own way, building or educating the right teams who understand the quantum threats, impacts, and responses as well as formulating future-looking mitigation plans is key to preparing for the quantum future.

A.1 Risk Management Framework Overview

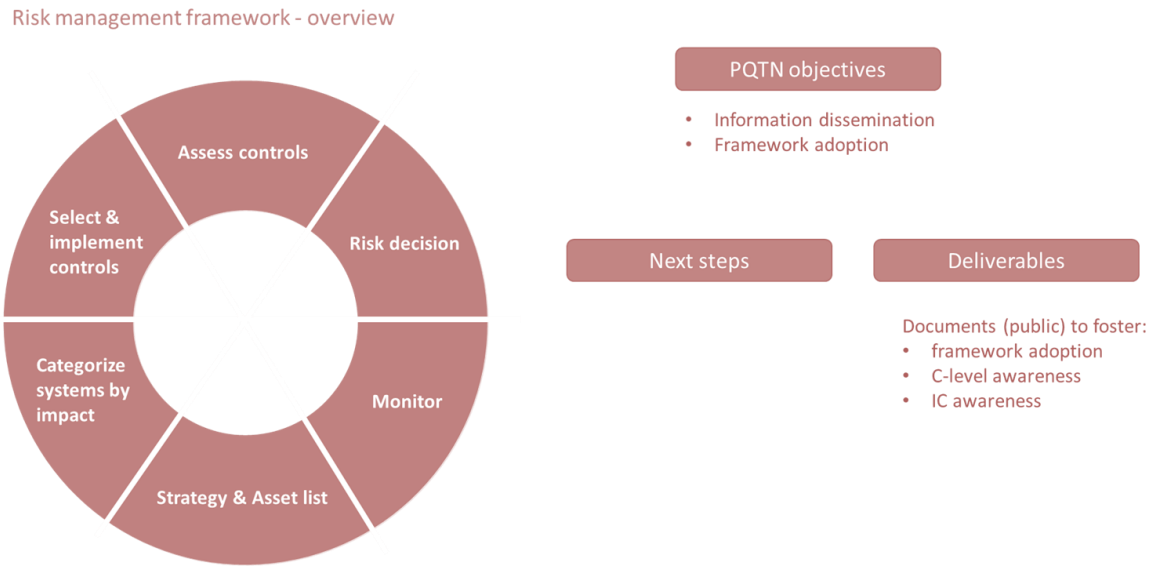

Figure A.1: Risk Management Framework Overview

Annex B Migration Considerations

Enhancing existing protocols with PQC is not a straight-forward process and involves code for new algorithms, new messages, modifications in message sizes and content, sequence of messages and processing considerations. The quality of the source code must also be considered in order to avoid potentially exploitable vulnerabilities such as side-channel attacks. This code injection can be a security vulnerability by itself. Adding PQC to IKEv2 or TLS can lower the probability of a successful attack with a CRQC, but increase the probability of an attack with a classical computer because of an addition in terms of new lines of codes. To manage the transition to PQC it is recommended to take the maturity of PQC implementations into account to determine the point in time to start the migration and to consider the use of hybrid keys.

Hybrid keys are mixed from keys obtained by two or more sources. Post-Quantum Preshared Keys (**PPK**) are an addition to the IKEv2 protocol to ensure that currently encrypted traffic which is stored is safe against future quantum computer decryption. A symmetric PPK is shared securely out-of-band and is used as an input into the SKEYSEED generation. This means that even if the Diffie-Hellman key exchange component of IKEv2 is compromised, an attacker cannot obtain the key material. The PPK method is specified in RFC8784 [17].

Leveraging PPK however comes at the cost of adding another layer of secure communication to distribute the PPK next to the pre-existing traditional key-exchange. This could be implemented by using an additional out-of-band key-exchange mechanism (e.g. Quantum Key Distribution (QKD) or courier).

Another option is to use an in-band "hybrid" key exchange. In this context, hybrid means the use of two key exchange algorithms based on different cryptographic assumptions, e.g. one traditional algorithm and one next-gen algorithm, with the purpose of the final session key being secure as long as at least one of the component key exchange algorithms remains unbroken. (See Reference [18]).

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	22 September 2023	First version	TG	Yolanda Sanz, GSMA

C.2 Other Information

Type	Description
Document Owner	PQTN TF
Editor / Company	Ariston Collander, AT&T Catherine White, BT Lory Thorpe, IBM Zygmunt Łoziński, IBM Taylor Hartley, Ericsson Kelly Richdale, SandboxAQ Yousif Targali, Verizon Luke Ibbetson, Vodafone Gabriela Radu, Vodafone Galina Pildush, Palo Alto Networks Gert Grammel, Juniper Networks
Supporting Companies	AKAYLA, Arqit, AT&T, Bell Canada, C-Spire, CK Hutchison, China Telecom, China Unicom, EE, Ericsson, Fortinet. G+D, HP, Huawei, IBM, Idemia, IMDA, Infineon, Infobip, Juniper Networks, Kigen, KT Corporation Maxis,, Nokia, NXP. Orange, Palo Alto Networks, PQ Shield, Proximus Belgium, Samsung, Sanbox SK Telecom,, STC, STMicroelectronics, T-Mobile, Thales, Telcel, Telefonica, Telstra, Telus, TIM, Verizo, Vodafone, Utimaco

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org

Your comments or suggestions & questions are always welcome.