Quantum-Safe Canada

Integrating Quantum-Safe Practices into Critical Infrastructure Cybersecurity

Integrating quantum-safe practices into critical infrastructure cybersecurity practices

The current and impending quantum threat increases the complexity of securing critical infrastructure and associated compliance.[1] Those employed in oversight and evaluation of industry or sector-based compliance regimes typically have a background in the regulated field and may not have had sufficient exposure to cyber-related requirements to conduct unguided assessment of critical infrastructure cybersecurity. As quantum threats are introduced, it exacerbates this challenge; it can be overwhelming for those who are not familiar with cybersecurity and quantum-safe practices.

Rather than seeing quantum-safe requirements as distinct from cybersecurity program requirements, organizational actions and those evaluating compliance should be oriented to a more holistic view that considers both the traditional cyber threats and emerging threats such as those posed by quantum computing.

The National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity,* broadly known as the NIST Cybersecurity Framework (CSF), consists of five concurrent and continuous functions - *Identify, Protect, Detect, Respond,* and *Recover* (figure 1). These functions provide a high-level, strategic view of the lifecycle of an organization's cyber-risk management.[2] This includes the identification of and response to compliance requirements. The NIST Cybersecurity Framework (CSF) also supports a common lexicon and taxonomy to:

1. Describe current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state; and
5. Communicate among internal and external stakeholders about cybersecurity risk.[3]

Quantum threats and quantum-safe requirements can readily be integrated into the NIST CSF (Figure 1), a proven framework for development and improvement of critical infrastructure cybersecurity, thus providing a simple framework to guide inquiries into organizational compliance.

---

[1] In Canada, there is pending legislation that would make it a requirement for selected critical infrastructure sectors to implement, monitor and manage a risk-based cybersecurity program. Notwithstanding, there are existing and emerging sector and industry-based compliance regimes that should be considered.

[2] NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf, p. 3

[3] Ibid, p. 2

Figure 1 – NIST Cybersecurity Framework Version 1.1[4]

Cybersecurity risk management is not 'one size fits all.' It is often complex requiring a thorough understanding of the business, technical and threat context, cyber risk management, and application of technical and non-technical security controls to help mitigate critical infrastructure cyber risks. There may also be other industry-dependent standards or compliance requirements that need to be integrated such as ISO/IEC or privacy requirements.

The NIST CSF can guide informed inquiry into the cybersecurity of critical infrastructure organizations. However, NIST has not yet explicitly introduced quantum threats or risks within the CSF guidance. The table in the Appendix represents an adaption of the NIST CSF to situate the identification and management of quantum risks within critical infrastructure organizations. This provides those employed in compliance oversight and evaluation with a single holistic framework that addresses both traditional and quantum-safe cybersecurity concerns.

[4] NIST is working on CSF Version 2.0. The adaption of the CSF in the following table has integrated some of the elements that will be introduced in Version 2.0. Once Version 2.0 is published, this document should be reviewed to ensure continued alignment with the new version of the CSF.

Appendix - Integrating Quantum-Safe Practices into Critical Infrastructure Cybersecurity

Function	Primary inquiry	Indicators - There is evidence that the organization has:
Identify	**What evidence is there that the organization manages cybersecurity risk including supply chain and quantum risks?**	☐ Cybersecurity governance that: ☐ establishes cybersecurity objectives that are aligned with organizational goals and objectives as well as expectations in the industry sector and consumers ☐ defines cybersecurity roles and responsibilities within the organization as well as those of third-party suppliers This includes the degree to which support quantum-safe practices are being integrated into third-party supplier products or services ☐ describes cybersecurity accountabilities ☐ identifies and integrates cyber and associated quantum risks, both tangible and intangible, into broader organization risk management ☐ A cybersecurity policy that: ☐ aligns with organizational cybersecurity strategy and goals ☐ defines high level cybersecurity requirements including regulatory and industry standards compliance requirements ☐ identifies other industry or sector specific compliance requirements or standards ☐ is explicit on the protection of sensitive data including personal information ☐ supports organizational migration to a Q-S environment within the identified threat timeline ☐ embeds crypto-agility into organizational practice ☐ An asset inventory that: ☐ includes *asset value* and *sensitivity* ☐ identifies *confidentiality, integrity and availability* (CIA) requirements of: ☐ data ☐ information system and devices including those managed by third-party providers ☐ operational systems and devices ☐ identifies cryptographic and encryption assets, the assurance or audit programs that have certified the cryptographic module, and how these assets are used to protect sensitive data and systems. ☐ supply chain interconnections, shared assets and assets in the cloud are identified ☐ A threat assessment process to define: ☐ current threats including potential impacts of the 'harvest now/decrypt later' quantum threat

Function	Primary inquiry	Indicators - There is evidence that the organization has:
		☐ future threats, such as quantum, IoT, AI, automation and robotics, depending on the business and sector ☐ A risk management framework that identifies and prioritizes treatment for critical cyber and associated quantum risks ☐ Allocated cybersecurity resources and investments based on prioritized risks including current and future quantum risks. ☐ Established a Q-S migration plan and means to monitor progress ☐ Conducted regular review of cybersecurity requirements, processes and practices that keeps pace with the evolving business, technical and threat context
Protect	**What safeguards / security controls have the organization implemented to ensure delivery of critical services?**	☐ Implemented effective risk treatments that address critical infrastructure risks, including quantum risks, to an acceptable level ☐ Monitored potential changes to assets as: ☐ they move through the asset lifecycle ☐ the threat evolves including changes to quantum threats ☐ Implemented cybersecurity controls that support: ☐ verification of personnel integrity and reliability including third-party supplier personnel screening processes ☐ separation of duties, including employees, contractors and third-party suppliers ☐ monitoring of physical access to organizational systems, software and data ☐ identity management and access controls based on the Principle of Least Privilege (PoLP) ☐ authentication of approved users, devices, and systems ☐ data security, including Q-S protections, for data in use, in motion, at rest and at end-of-life. ☐ patch and vulnerability management processes ☐ protection, monitoring and logging of: ☐ command-and-control system activity ☐ perimeter security ☐ internal critical interconnections ☐ end points ☐ operational technology that is internet connected ☐ third-party connections and APIs ☐ network, system and data segregation based on asset category and level of protection required ☐ remote, 'bring your own device (BYOD)' and IoT device operations policy and procedures including M2M communications ☐ encryption and cryptographic controls that meet required standards and anticipate quantum threats ☐ Q-S backups of critical systems, software and data

Function	Primary inquiry	Indicators - There is evidence that the organization has:
		☐ Change and configuration management controls including those that may impact Q-S technologies and processes ☐ Policies and processes in place to establish, monitor and measure technical and non-technical cybersecurity activities including: ☐ communications protocols on user cybersecurity requirements ☐ role-based security training and organizational cybersecurity awareness training ☐ review and reconciliation of third-party agreements against organizational requirements ☐ a Q-S migration plan that mitigates quantum risk within the quantum threat timeline as well as a means to monitor the progress of the migration plan ☐ maintaining a cryptographic inventory that is regularly checked against conventional and post-quantum security requirements including any compliance regime
Detect	**What systems and processes are in place to afford timely detection of cybersecurity events?**	☐ Systems are in place to continuously monitor and support timely discovery of cybersecurity events and anomalous activities connected to critical systems. This includes an indicator to detect cryptographic artifacts that are not quantum-safe ☐ Processes are in place to identify and prioritize organizational response to cybersecurity events including those posed by quantum threats ☐ If employed, third-party agreements that explicitly identify reporting thresholds and escalation protocols
Respond	**How is the organization prepared to respond to a cybersecurity incident?**	☐ A business and/or operational continuity plan ☐ Established cybersecurity incident response plan that is available on and offline that details: ☐ roles and responsibilities of response team ☐ roles and responsibilities of out-sourced or third-party services ☐ system authorities (shutdowns, severances, recovery, etc.) ☐ escalation protocols ☐ initial containment, mitigation and eradication protocols ☐ a process for responding to the availability of a quantum attack ☐ internal and external communications authorities and protocols ☐ critical contacts (e.g. law enforcement, insurer, legal counsel, provincial privacy commissioner, up and downstream supply chain, other key stakeholders) ☐ protocols for acquiring and engaging specialized services (e.g. mitigation, remediation, forensics, etc.) ☐ recovery protocols

Function	Primary inquiry	Indicators - There is evidence that the organization has:
		☐ post-incident analysis requirements and lessons learned ☐ Provided role-based training to those with specific incident response roles including detection, response and recovery activities ☐ Exercised the incident-response plan with different threat scenarios that are relevant to the business/sector
Recover	**What activities support organizational resilience, safe and secure recovery from a cybersecurity incident and continuous improvement?**	☐ Recovery protocols that prioritize critical systems and services ☐ Testing of data and system back ups ☐ Testing of recovery protocols to include robustness against quantum attacks ☐ Training in recovery protocols and processes ☐ Ongoing reporting and communications activities for internal and external audiences ☐ A post-incident analysis process that: ☐ includes all individuals with cybersecurity incident management responsibilities ☐ reviews and measures organizational response actions ☐ examines crypto-agility in the face of quantum attacks to determine required improvements ☐ identifies and acts on lessons learned ☐ supports continuous improvement