Quantum-Safe Canada

# Preparing for quantum threats in critical infrastructure

Any critical infrastructure organization that relies on cryptographic systems or encryption must consider the potential threats posed by quantum computing; not just when quantum computing becomes a reality, but also current harvest now/decrypt later threats. Your cybersecurity program should include, at a minimum, a quantum-risk assessment and a plan to migrate to quantum-safe practices within the quantum threat timeline.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 1.1 can be used go guide actions across the five concurrent and continuous functions - Identify, Protect, Detect, Respond, and Recover. The following table provides some initial considerations to support planning and migration to a quantum-safe environment for each of these five functions.


| Function | Critical questions |
|---|---|
| **Identify** | • What changes to cybersecurity governance and related policies are necessary to address quantum threats?<br>• What planning activities should be in place to support migration to a quantum-safe environment within the threat timeline?<br>• What cryptographic and encryption systems are in place and what data /systems do they protect? Are these reflected in your asset inventory?<br>• What are your current and potential quantum risks? |
| **Protect** | • What actions will help mitigate 'harvest now/decrypt later' risks?<br>• What safeguards / security controls need to be implemented to meet the threat timeline?<br>• How will you know that protections are sufficiently robust against quantum threats?<br>• How are you logging, monitoring and auditing processes going to change? |
| **Detect** | • What systems and processes are in place to afford timely detection of cybersecurity events such as a compromise to cryptographic systems or encrypted data?<br>• What escalation and initial containment protocols are in place? |
| **Respond** | • What are potential quantum-related incidents that may occur?<br>• What changes may be required to your incident response plan?<br>• How is the organization prepared to respond to such an incident?<br>• How will third-party cybersecurity services be leveraged? |
| **Recover** | • What recovery protocols may be needed for cryptographic systems and encrypted data?<br>• How are recovery protocols and backups tested?<br>• What post-incident activities are required to support continuous improvement? |