Quantum-Safe Canada

Quantum-Safe Training – Leadership Series

Tabletop Exercise (TTX) Participant Guide

Table of Contents

Published by:
Quantum-Safe Canada
31 March 2023

What is the purpose of this guide?

As a prospective tabletop exercise (TTX) participant within the Quantum-Safe Training – Leadership Series, you have received this guide explaining the role of the TTX and how it will be used to support your training.

What is a TTX?

A Tabletop Exercise or TTX is a scenario-driven activity that simulates an event with the intention of eliciting responses and discussion among participants as the event unfolds. Within cybersecurity, TTXs can be used to support:

- Training and education
- Plan development
- Policy development
- Process or procedural evaluation
- Individual or team assessment
- Organizational assessment.

In addition to being a flexible tool, the primary benefit of the TTX is that it is intended to be a learning environment where discussions can occur when not under threat or crisis, thereby giving participants the opportunity to think and talk through issues.

What are the goals of the TTX?

The Quantum-Safe Training – Leadership Series includes TTXs for different audiences. The TTX exposes participants to a progressive scenario that starts within the current-day setting and develops through exercise injects that provide new information or require discussion on potential decisions or actions.

While responding to the scenario and injects, participants have the opportunity to discuss plans, policies, processes, procedures and other factors related to the organization's capabilities and capacity to migrate to a quantum-safe (Q-S) environment.

The goals of the TTX vary based on the audience and the organizational cybersecurity context. However, in general the goals of the TTXs within this series are to:

- Move participant thinking about quantum threats from the abstract to concrete
- Provide participants with the opportunity to understand the potential impacts of quantum threats and what measures should be in place

- Encourage discussion around organizational capability and planning
- Assess existing preparations and plans relative to what may be required.

What is the participant's role in a TTX?

For the leadership series TTXs, there will be a **facilitator** who will be a senior cybersecurity or management professional who is familiar with quantum threats and risks and has a general understanding of quantum-safe strategies, technologies and processes. They will lead you through the TTX and facilitate discussions. There may also be **observers** who are from your organization or the TTX provider that are there to identify issues and support the exercise debrief.

As a **participant**, you are critical to the experience as you will be bringing your experience and perspective to the discussion. The TTX is a safe learning environment where issues and problems should be surfaced and discussed. Accordingly, everyone is expected to share their opinions and highlight opportunities for improvement. To ensure an effective TTX experience, you will be asked to:

- Assume your current or assigned organizational role.
- Engage in the discussions, think aloud and explain decisions or intended actions
- Accept scenarios and events at face value
- Provide your input to the exercise debrief.

How can I prepare for the TTX?

There are a few things you can consider in preparation for the TTX.

- Review your organizational context and your organization's current cybersecurity posture
- Know what systems are critical to operations and, in particular, which systems and processes rely on at-risk cryptography/encryption
- Identify other key roles. Even if they won't be participating in this exercise, they should be considered as potential actors in Q-S preparation and planning
- Come prepared to openly engage and discuss your perspective on the simulated event as it unfolds

As well, you are encouraged to review the selected resources to gain a better understanding of quantum threats and the types of activities that will help support organizational migration to a Q-S environment.

Useful Terms[1]

Cryptography	The process of making plain information unreadable, as well as to convert it back to a readable form. This includes constructs such as encryption, digital signatures, hashing, etc. that are used to authenticate the source and protect the confidentiality and integrity of information within and across a variety of information and communications technologies.
Cybersecurity	The protection of digital information and the infrastructure on which it resides. More specifically, cybersecurity includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.
Deliberate cyber threat	A cyber threat actor who, using the internet, takes advantage of a known vulnerability for the purposes of exploiting a network and the information the network carries.
Encryption	Converting (encoding) information from 'plaintext' to 'ciphertext' to hide its content and prevent unauthorized access or manipulation.
Quantum computing	Exploits quantum properties to store and manipulate information that enables mathematical, optimization, and search problems much faster than conventional computers.
Quantum threat	Quantum computers used in ways that can break or weaken widely used cryptographic schemes.
Quantum-safe cryptography	The use of new cryptographic tools, whether conventional or quantum in nature, designed to be resistant to quantum attacks.
Quantum-safe	A state of an information system where quantum threats have been mitigated through either traditional or new quantum-safe practices, processes and technologies.

[1] Adapted from the Canadian Centre for Cybersecurity (2023), Glossary, https://www.cyber.gc.ca/en/glossary and the selected resources which follow.

Selected Resources

Canadian Centre for Cyber Security, (2021). Preparing your organization for the quantum threat to cryptography - ITSAP.00.017, https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

Canadian Forum for Digital Infrastructure Resilience (CFDIR) (2022). Canadian National Quantum-Readiness: Best Practices and Guidelines. https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2022/cfdir-quantum-readiness-best-practices-v02-en.pdf

Mosca, M., Mulholland, J. (2017). A methodology for quantum risk assessment: Technical report. Global Risk Institute. https://globalriskinstitute.org/publications/3423-2/#:~:text=Quantum%20Risk%20Assessment%20Methodology,threats%20are%20likely%20to%20emerge

Mosca, M., Piani, M. (2022). Quantum Threat Timeline Report, Global Risk Institute. https://quantum-safe.ca/wp-content/uploads/2023/01/2022-quantum-threat-timeline-report-dec.pdf