Quantum-Safe Canada

Quantum-Safe Training – Leadership Series

Critical Infrastructure Regulator Tabletop Exercise (TTX)

Table of Contents

Published by:
Quantum-Safe Canada
31 March 2023

Purpose and Applicability

This guide supports cybersecurity and management professionals in tailoring and facilitating tabletop exercises for regulators that may include federal employees, contracted resources, or federally approved contractors responsible for the administration, oversight and/or assessment of compliance within Canadian critical infrastructure. This can span responsibilities from program directors to those conducting virtual or on-site compliance assessments.

This tabletop exercise features a progressive quantum-threat scenario that orients the audience to identify common cyber threats including quantum threats, risks to critical infrastructure cybersecurity and typical organizational challenges.

This guide should not be provided to participants. Rather, they should be provided with links to the selected resources at the end of this guide.

TTX Tailoring and Preparations

A TTX can have many goals and support different functions. It can be used to:

- Educate or train participants
- Support short, medium or long-term planning and preparations
- Assess processes and procedures
- Evaluate communications and workflows
- Help solve complex problems.

This guide provides a framework for the conduct of a TTX based on a quantum-threat scenario that is intended to both educate and support regulators in their responsibilities to oversee, administer and conduct evaluations of critical-infrastructure cybersecurity. As each regulating agency may have different processes and capabilities, the TTX can be tailored to suit organizational requirements and other goals.

Further, the needs of different critical-infrastructure sectors can vary. Accordingly, this TTX is generic in nature and the elements such as exercise foreground and injects can be adapted to suit a particular sector, industry or business environment as well as a public, private or non-profit organizational context.

If tailoring is required, the facilitator should:

- Define the target audience – Who are the participants and what roles do they fill within the organization(s)? The TTX can apply to roles such as directors,

senior managers, coordinators, administrators, or evaluators. It can also apply to a specific group or team.
- Identify client goals and outcomes – Why does the client want the TTX and what do they wish to achieve or learn from the TTX?
- Determine any specific parameters for the TTX – What are the potential client or delivery constraints? This includes the media used, timeline, location, scenarios, known issues, or processes to be assessed.
- Establish the current state of the organizational processes – What is the organization's general cybersecurity posture and maturity? This will help define both the goals and the elements required in the TTX that will enable discussion and feedback.

Prior to delivery of the TTX, the facilitator should:
- Adjust the scenario to address client goals
- Add, delete or amend injects to support the scenario
- Check timely insertion of injects and the overall TTX timing.
- Create or amend visual aids that are needed to support the TTX
- Conduct a dry-run of the TTX to ensure that it flows well and meets the time requirements.

TTX Roles

Facilitator - The facilitator should be a cybersecurity or management professional who is familiar with cyber-risk management, quantum threats and risks and has a general understanding of quantum-safe strategies, technologies and processes. Detailed technical knowledge is not required as the TTX activities pertain to organizational decision-making, risk, planning, and appropriate allocation and/or acquisition of resources to address the quantum-threat. Education, training or experience in cybersecurity compliance, audit or assessment would be beneficial.

Participants – Depending on the TTX goals, participants may contribute to the TTX discussions in their current role, an anticipated role or an assigned role. As the intent of this TTX is to support participant ability to oversee and/or evaluate the cybersecurity program of a critical infrastructure operator, they should:
- Play their own or assigned role
- Take the scenario at face value
- Be encouraged to 'think aloud,' describe their thought process and disclose assumptions behind decisions or proposed actions.

Observers – While the facilitator will be guiding the exercise, the client may wish to have observers for the TTX. These observers can help to provide some objectivity and support critical analysis as the TTX unfolds. They can also offer their observations and insights during the debrief and any follow up actions.

Master Event List

The Master Event List (MEL) is a chronological representation of facilitator-led actions (injects) to prompt participant activity and discussion. It ensures that events happen in a sequence that will support achievement of the TTX objectives. In addition to the injects, the facilitator may include expert commentary or ask questions about the situation or context that support participant learning and decision-making.

This TTX is planned for a duration of two hours from initial introduction to debrief including 15 minutes for introduction, a 10-minute break mid-exercise and 15 minutes for debrief. Depending on the organizational goals, added elements, and discussions, the TTX could be extended. However, given the general goal of this TTX, the intensity of the activity, and the potential target audience, it is recommended that the exercise not exceed three hours.

This Master Event List (MEL) below is tailored to a quantum-threat scenario that includes an initial timeline based on a conservative estimate of when organizations are likely to experience a cryptographically relevant quantum threat. At mid-exercise, the timeline is accelerated, and the threat is realized several years earlier. This is intended to help demonstrate the uncertainty of the threat timeline and support contingent planning and preparation. The injects / activities are designed to be supported by a presentation or discussion guide with example correspondence, articles and other simulated materials which should be labelled as 'for exercise only'.

Timing (mins)	**Inject / Activity**	**Topics/content**	**Suggested discussion points**
0000-0015	Introduction	Personal introductions Goals of the exercise Ground rules for the exercise Initial scenario read-in Critical definitions:	

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		• Cybersecurity program • Cyber risk • Quantum risk • Quantum threat • Quantum-threat timeline • Cryptographically relevant quantum threat • Quantum-safe environment	
0015	Exercise starts		
0015-0020	Current day quantum threat timeline article (if desired an actual article can be use if permissions have been granted)	Excerpts from technical magazine article (current day): *"How safe is our critical infrastructure from the quantum threat?"* "*While experts have yet to agree on exactly when the quantum threat will be realized, conservative estimates hover around 15 years. Many experts suggest, however, that it could be considerably sooner given the level of investment and innovation within certain nation states and the private sector.* *"While the cybersecurity community is grappling with this new threat, our critical infrastructure is of particular concern."*	What information systems or data might a critical infrastructure (CI) have that could be subject to the quantum threat? What exposures or risks to CI would this create. As the threat is 15 years out, what are your immediate concerns if any?
0015-0025	Email from the ADM	"The topic of quantum threats came up in a presentation from the Canadian Centre for Cyber Security. Having considered this, I'm wondering how well we've	What is your initial response to this request? What types of investments do you think might be required to support a critical infrastructure

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		integrated quantum threats and corresponding cybersecurity actions into our understanding of critical-infrastructure cybersecurity. While the threat from actual quantum computing may be 15 years out, I would like to better understand what areas our regulating operators would need to invest in to plan and prepare for quantum threats. If possible, I'd like a short briefing note on the topic before my planning meeting next month.	organization's migration to a quantum-safe (Q-S) environment? What expertise do you have access to get information needed to help you prepare the brief?
0025-0040	A note from the DG	In addition to addressing the ADM's original request, I'd like you to also look into a more pressing issue. You might have heard of it, here is a threat known as the harvest now/decrypt later strategy that cybercriminals may employ. This involves them hacking into existing systems and taking encrypted data now with the intention of decrypting once the quantum capability becomes a reality. While it's not likely an issue for many, we already know that critical infrastructure is a target of some nation state adversaries that could pose a significant challenge as they are all working intently on developing quantum computing capabilities.	What are your first thoughts about this type of threat? What data or information do CI organizations currently have that may pose a risk if exposed in the future? Which CIs may be at higher risk? (Prompt, if needed) Consider requirements that pertain to protection of: - sensitive information - corporate / national secrets - IP - Source codes - AI- or control-system data channels and configurations - Digital interfaces with equipment that are protected by existing encryption

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		Let me know about this and we'll include it in the scope of the ADM's note.	
0040 - 0050	Requirement to enhance their job aid	As a group, you've been tasked to pull together a checklist to support the role of inspectors and evaluators in assessing CI organization's cybersecurity to include identifying and mitigating quantum threats.	Capture what they should be looking for on a screen or whiteboard. Possible points may include: - Cybersecurity-program governance - Risk-management process that includes cyber risks - Quantum-risk timeline - Data and information asset inventory – critical digital assets and their classification / categorization. Includes an inventory of vulnerable cryptographic systems and encryption processes including upstream and downstream supply chains - Identification and prioritization of cyber risks, quantum risks including supply-chain risks - Cybersecurity-control implementation plan - Costed plan for identification, integration, implementation and management of Q-S technologies and processes - Coordination of security controls with partners / suppliers - Contacts for cyber and Q-S technical exercise

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
			- Ongoing role-based training for employees - Lifecycle management to maintain cyber and Q-S posture
0050-0060	Break		
0060-0080	Accelerated quantum-threat new release six-months later [reword as per previous]	"Breaking news. *The tech world has been rocked with the recent statement by a medium-sized technology firm that indicated that they are confident that they will have quantum capability within the next five years. While many have their doubts and suggest that this is an attempt to attain more investment, government officials have assessed the evidence and agree that quantum computing could be a reality sooner than we thought."* The word has come down from the ADM that this has been verified.	How does this change your plan? What should your first steps be? Possible responses: - Reach out to the Public Safety Canada and the Canadian Centre for Cyber Security for advice and additional guidance - Review what CI organizations have been instructed relative to Q-S threats - Verify critical quantum risks and any implications on existing compliance requirements - Prioritization of CI engagement based on national/public risk - Identity the expertise that would be needed to include potential to support a surge of CI requirements to support program guidance and oversight
0080-0090	Article – state of quantum computing in	Excerpts from a national paper (three years in the future): *"State of critical infrastructure – Are we prepared for the emerging quantum threat?"*	Forecasting out to this time and understanding the evolution of cybersecurity across CI, what are your perspectives on this?

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
	Canada three years later	*"…the Government has been actively engaged in ensuring that Canada's CI has been adequately protected. But how have we done?"*	What challenges might there be over the next five years that you'll need to consider? Possible responses: - Other changes to the cyber threats landscape including investment in capabilities to counter AI enabled threats - Increasing demand for expertise / talent - CI organizational changes that will necessitate other tech investment to stay relevant or comply with evolving standards and legislation (e.g., CI requirements, privacy, industry standards) - Remaining agile - Broadening regulatory requirements to the remainder of the CI supply chain
0090-0100	The future in retrospect	How would you like to see yourself and the CI community once quantum-computing and related quantum threats become a reality?	
0100	Exercise completed		
0100-0115	Debrief	Having completed the exercise: What are your primary concerns? What near term actions do you think you should take?	

Timing (mins)	Inject / Activity	Topics/content	Suggested discussion points
		Were there any other things that you learned that you consider valuable?	
0115-0120	Feedback	How did you think the exercise went? What suggestions for improvement do you have to offer?	

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

National Institute of Standards and Technology (NIST) (2022). Post-Quantum Cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography

NIST (2022). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

National Security Agency (2021). Quantum computing and post quantum cryptography FAQ. https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQ-S_20210804.PDF