Quantum-Safe Canada

Quantum-Safe Training - Leadership Series

Curriculum Enhancement Workshop for Educators

Table of Contents

Published by:
Quantum-Safe Canada
31 March 2023

Purpose and Applicability

This workshop is intended primarily for computer science, IT and cybersecurity educators from colleges or universities that are considering integrating quantum-safe content into their courses and programming. It is also applicable for other disciplines such as management and business.

The ability to develop and teach students about the processes related to migrating quantum-safe cryptography does not require a deep understanding of quantum-computing or quantum cryptography. It does, however, require a good understanding of organizational cybersecurity[1] and application of cryptography and encryption Further, if integrating content into a technically-oriented course or program, a sound knowledge of cryptographic systems, encryption processes and current Q-S standards is needed.

While this workshop can be conducted as a standalone training activity, it leverages information from and is complementary to the Quantum-Safe Canada publication *Organizational migration to quantum-safe cryptography – A curriculum guide (2022).*[2]

Workshop Objectives

This workshop orients educators to general Q-S curriculum requirements and helps them identify how they can implement Q-S topics and practices into their course or curriculum. Upon completion of this workshop, participants should be able to identify and create a plan to integrate Q-S content into their program.

Facilitator Qualifications

The workshop facilitator should be an experienced cybersecurity professional who:

- Is also an experienced instructional facilitator
- Has post-secondary curriculum-development experience
- Demonstrates comprehensive understanding of:
    - organizational cybersecurity management

[1] Organizational cybersecurity is differentiated from more general cybersecurity in that the focus is on establishing and managing security controls. The broader understanding of cybersecurity is as an interdisciplinary field of study that includes various areas of research and inquiry that extend beyond actions taken within an organization.
[2] Available through Quantum-Safe Canada

    - cybersecurity strategy development and planning
    - common industry standards and compliance requirements
    - cybersecurity best practices for organizations
- Demonstrates general understanding of:
    - cryptographic systems and encryption
    - quantum-risk assessment process
    - quantum threats and their potential impacts
    - the current status of quantum-safe standards and technologies
    - quantum-safe migration activities
    - technical and non-technical security controls to mitigate the risks associated with current and future quantum threats

Workshop Overview

Curriculum-enhancement activities are intended to supplement rather than to supplant existing programming. That said, a critical component of the workshop is identifying risk-based trade-offs within the curriculum where Q-S content may have to be weighed against the value of retaining or revising existing content.

This 3-hour discussion- and activity-based workshop will explore Q-S content requirements and how Q-S content can be introduced into existing curriculum while minimizing the revision requirements and programming impact.

Timing	Topic	Timing (mins)
Pre-requisites	Scan: 'Selected resources' Read: Q-S Curriculum Guide and curriculum models - *Organizational migration to quantum-safe cryptography – A curriculum guide (2022)* Do: Identify common graduate work roles and related cybersecurity workforce requirements.	-
Introduction	Introductions Objectives Workshop overview	10
Orientation to quantum-safe curriculum requirements	The educational imperative for inclusion of Q-S content	45

	Identifying / prioritizing curriculum based on program-relevant value. Includes identifying alternative learning opportunities (e.g., eLearning, self-study, job aids, etc.) Overview of organizational migration to Q-S cryptography - Key concepts and processes A role-based perspective on migration to a Q-S environment Scoping Q-S requirements in your curriculum	
	Activity: Identifying curriculum scope based on anticipated graduate roles	15
Break		10
Integration of Q-S content: a practical approach	Guided curriculum-based activity (independent or in groups): • Reviewing current curriculum and how cybersecurity and cryptographic requirements are situated within your program • Identifying applicable Q-S elements based on anticipated graduate roles • Establishing Q-S knowledge, skill, ability (KSA) required of graduates based on workforce needs • Determining how Q-S KSA requirements correspond to or interrelate with existing curriculum content	50

	• Assessing impact of Q-S content integration relative to other content
	
	• Prioritizing integration of content based on:
	  • anticipated roles for graduates
	  • degree of urgency
	  • institutional capacity to implement the changes	

Break		10
	Activity: Formulating a plan – integrating Q-S content into your curriculum	30
Conclusion	Review objectives Primary requirements Feedback	10
		180

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

Quantum-Safe Canada (2022). Organizational migration to quantum-safe cryptography: A role-based framework, learning outcomes and curriculum model.

Quantum-Safe Canada (2022). Organizational migration to quantum-safe cryptography – A curriculum guide.