

## Supplier Requirements for - Quantum-Safe Training: Leadership Series

### **Background**

Expert estimates on the emergence of a cryptographically relevant quantum threat is between 5 and 30 years.<sup>1</sup> However, the fact that private-sector organizations and several nation states are actively engaged in research focused on generating quantum-computing capability suggests that the threat could be realized far closer to the near end of that timeline. This means that organizations should be planning now to ensure that they are able to make the required cybersecurity investments within a realistic timeline.

Further, there is a significant misconception that the response can wait until the quantum threat emerges; there are known threat actors that are currently exfiltrating sensitive encrypted information with the intent to decrypt it once they have cryptographically relevant quantum-computing capability. Colloquially termed 'harvest now, decrypt later', this strategy puts all existing encrypted information at risk. So, for organizations concerned about this threat, cybersecurity strategies should be in place now to help reduce the risk of compromise in the future.

### **Q-S Training Requirements**

Quantum-Safe Canada and other organizations have created several resources that guide organizations through risk-based processes that support migration to quantum-safe (Q-S) cryptography and help ensure organizational cybersecurity in a post-quantum computing environment.

An informed cybersecurity professional can use these resources and apply them to their work context. However, most organizations do not have ready access to this type of professional and are not yet prepared for the quantum threats.

Accordingly, Quantum-Safe Canada is soliciting suppliers to support the tailoring and delivery of the Quantum-Safe Training: Leadership Series. This training is intended to stimulate initial Q-S planning and actions across four key audiences.

1. **Organizational Decision-Maker TTX** - A 2-3 hour tabletop exercise that features a progressive quantum-threat scenario that challenges the senior organizational decision-makers to identify quantum risks and potential mitigations within the quantum-threat timeline.

---

<sup>1</sup> Ibid, p. 8

2. **Technical Advisor and Senior Technical Manager TTX** – A 2-3 hour progressive quantum-threat scenario intended for technical managers to aid them in identifying quantum threats to digital systems and data, technical implications and potential mitigations to support quantum-safe (Q-S) migration.
3. **Regulator TTX** – A 2-3 hour tabletop exercise featuring 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.
4. **Curriculum Enhancement Workshop for Educators** – This 3-hour workshop orients educators to general Q-S curriculum requirements and helps them identify how they can implement Q-S topics and practices into their courses and curriculum.

Suppliers can bid on delivery of one or more of the above training products.

For all bids, suppliers must include an estimated level of effort to support both **tailoring** and **delivery** of content.

### **Travel and miscellaneous expenses**

The delivery may include virtual or in-person sessions depending on geographic location. Suppliers may also incur other office expenses and insurance costs or similar. Quantum-Safe Canada does not allow for reimbursement of travel or other miscellaneous expenses. Accordingly, all supplier fees must factor in these expenses.

### **Mandatory criteria**

The selected provider for these training requirements will demonstrate the following mandatory criteria.

<b>Element</b>	<b>Criteria</b>
Cybersecurity experience	Minimum 5 recent years experience providing advice and guidance on organizational cybersecurity.
Instructional facilitation experience	Minimum 3 years experience in provision of instructional facilitation as an instructor, professor or teacher in an adult-learning environment.
Ability to advise on use of cryptography and encryption in business or industrial environments	Experience in working in or advising on cryptographic systems or processes and encryption. Deep technical knowledge in cryptography is not required.

## Weighted criteria

The following weighted criteria will also be used to evaluate bids.

Element	Criteria	Point allocation	
Bilingual delivery	Demonstrates access to qualified English and French speaking facilitators	-	5
Instructional design capability and experience	Evidence of instructional design experience that will aid in tailoring training to meet different learning audiences.	5+ years	5
		2-4 years	3
		1-2 years	2
		0 to 1 year	1
Administration	Dedicated ability to coordinate engagement, participant registration, delivery and evaluation of training sessions	High	5
		Moderate	3
		Limited	2
		None	0
Delivery capacity	Primarily based on the number of readily accessible facilitators that are able to tailor and delivery training to diverse audience groups	Over 5	5
		4-5	3
		2-3	2
		1	1
Delivery to diverse audiences	Access to facilitators with different expertise or abilities to address audience diversity	All audiences	5
		3 audiences	3
		2 audiences	2
		None	0