# Quantum How

What every board member and executive leader needs to know to lead in the quantum era

Version 1.1, December 2025

# Table of Contents

# 1 Crossing the Quantum Threshold

## 1.1 Executive Brief

**Read this section to understand the thrust of this guidebook and to maximize the value of your time in engaging with it.**

**National call to action:** Quantum computing is no longer a distant possibility; it is an imminent reality.

Beyond exposing the direct opportunities and threats of quantum computing to any one organization, this document seeks to engage all economic stakeholders in a greater national strategy. Canada has built one of the most advanced quantum ecosystems in the world. We've proven we can lead. Now we must scale. Our government, defense and academic sectors have already committed to supporting this ambition. Canadian industries, and the Canadian financial sector in particular, must match its counterparts to fulfill this common national interest and ensure Canada's rightful and enduring leadership in next-generation technological innovation.

### Why Quantum Matters Now

- The signals of its emergence as a transformational technology are clear, yet many organizations remain unaware of its potential and many more, **dangerously unprepared for its impacts.**
- By the time some organizations look up, quantum computing will have **reshaped the digital, economic, and geopolitical landscape,** with late movers struggling to catch up.

### What Quantum Really Is

- Quantum computing is a new class of computer technology that leverages a distinctly **new approach to problem-solving.**
- It will enable us to solve complex problems that are **computationally prohibitive** for classical computer technology.
- Its impact will be **transformational and systemic**, generating benefits across industries.
- On the **positive side**, it will expand the frontiers of human knowledge by enabling breakthroughs in science, medicine, logistics, finance, climate science and beyond.
- On the **darker side**, it threatens current encryption[1] and authentication[2] standards and with them, the **very foundation of digital trust** that underpins the global economy and the exchange of information worldwide.

### Current State Quantum Computing

- First generation **quantum computers exist**[3] and are already being put to practical use for research and as test beds for commercial applications through partnerships with early industry movers[4].
- There is growing alignment across the quantum industry and expert opinions that **fault-tolerant quantum computers**[5] **could emerge by 2030.**

[1] Encryption is the process of converting information into a coded form that can only be read or accessed by someone with the correct decryption key.

[2] Authentication is the process of confirming that a person, device, or system is truly who it claims to be, typically using digital signatures or credentials.

[3] Called Noisy Intermediate-Scale Quantum (NISQ) computers, they are powerful enough for experimental and specialized tasks but are still prone to noise and errors.

[4] Well cited examples include JP Morgan, HSBC, Banco Santander, Merck, Johnson & Johnson, Roche, Amgen, Moderna, AstraZeneca, Sanofi, DHL, Volkswagen, BMW, Ford, and Airbus, but also the **Bank of Canada**. See Appendix for links to the 'The Quantum Index" for more.

[5] A fully error-corrected quantum computer capable of performing long and complex calculations reliably, marking the threshold for large-scale commercial use.

## Why You Must Act

- Quantum computing brings both transformative opportunities and disruptive risks and **as leaders, we must prepare** for both.
- Organizations that mobilize early can **seize the benefits** of this new technology and lock in **first-mover advantage**[6].
- At the same time, quantum computing introduces **intolerable levels of global systemic risk** and **immediate mobilization** is required to mitigate it.
- Organizations that **fail to take timely action** risk their competitive capacity and resilience, while contributing to the broader **global threats to digital trust and technological sovereignty**.

## Finance in Front

- The individual and collective leadership of the financial industry can determine whether the **quantum era begins in crisis or confidence**.
- Due to their vast cryptographic infrastructure and their track record of embracing sound prudential practices and role in the economy, **banks are the natural stewards of digital trust**.
- Their data and **systemic importance** to markets place them at the front of the line for early **quantum-enabled cyber attacks**.
- Banks have a longstanding relationship with physics[7] and stand to **benefit directly and early from quantum computing capabilities.**
- Banks have **global coordination capabilities through regulatory bodies**, which are experienced at institutionalizing resilience.
- **Early alignment from banks would create momentum**, as many other industries voluntarily adhere to their schedule and standards.

## The Leadership Gap

- Leadership is foresight in motion. It means **acting before consequences** become unavoidable.
- As quantum computing power grows, so does the risk and remediation **costs for those who do not prepare**.
- The **signals are clear**, and the stakes could not be higher; leaders have a responsibility to act. **Inaction will soon register as fiduciary failure.**
- But the complex nature of the inner working of quantum computers, and the broad and multi-faceted scope of their impacts, make it **challenging for leaders to grasp** what it all means.
- Leaders can be bold and brave, but they cannot act with confidence and clarity on what they fundamentally do not understand.

## Closing the Gap

- Only once the **imperatives of quantum computing are made clear**, can responsible leadership take hold.
- A **comprehensive and reliable source of information**, presented in a clear and actionable format, is needed to overcome the Leadership understanding-to-action gap.
- **This guidebook exists to close that gap.**

[6] First movers are building expertise, securing partnerships, contracts and supply chains that will yield long-term advantages in a world where expertise and infrastructure will be limited.
[7] The mathematics behind financial models, risk models, and trading algorithms are the same used in many areas of physics and many individuals with advanced mathematics and physics knowledge currently work within the financial industry.

## 1.2

# About this Guidebook

This guidebook equips leaders with the essential knowledge to lead your organization through the first stages of the new quantum paradigm.

Developed specifically for board and executive leaders, this guidebook delivers a clear message in the language you use to make decisions: **risk**, **trust**, **timing**, **strategy**, **governance**, **accountability**.

### Nontechnical language

Using only nontechnical language, it makes the imperatives of quantum computing readily **understandable** and **undeniably clear** to Leaders.

### Essential information

It includes the essential information every board and executive team needs to act with clarity, **appropriate urgency** and **confidence**.

### Next steps and long-term strategy

By clearly exposing the stakes and answering key leadership questions, this guidebook can be used to orient both your immediate **next steps** and **long-term strategy.**

### Fiduciary duty and national positioning

Follow it to meet your fiduciary responsibilities, protect our **digital & technological sovereignty** and maintain **Canada's leadership position** at the forefront of the quantum computing frontier.

## How was it developed?

This guidebook was developed and refined through collaboration and broad consultation across the quantum industry and the academic ecosystem and the broader business community. **The complete list of collaborators and endorsements is shared in Section 6.**

## Who is it for?

### Board directors and executive leaders

Board directors and executive leaders with fiduciary responsibility to protect their organizations and public trust are the primary audience of this guidebook.

### Large financial and public institutions

While relevant to all organizations, it is aimed primarily at large financial and public institutions where the stakes are higher and where momentum building can most impact national security, economic development, and with them, Canadian digital sovereignty.

## This guidebook is divided into 6 sections. The following is an overview of each section and how to put it into action.

**1**

**EXECUTIVE BRIEF**
(CURRENT SECTION)

Summarizes the thrust of the document and provides instructions to navigate the remaining material based on your baseline knowledge of quantum computing and experience with transformational technological shifts.

**Use this section for a quick overview and plan your approach to the document.**

**2**

**WHAT EVERY LEADER NEEDS TO KNOW**

Exposes the different facets of the quantum computing paradigm from an organizational, economic, and geopolitical perspective. It lays bare what is at stake and the case for action. It includes quick tools to change gears from passive to active leadership.

**Start here if you already have a basic understanding of quantum computing, how technological shifts are navigated, and seek an immediate understanding of what you need to do.**

**3**

**ADDITIONAL KNOWLEDGE FOR LEADERS**

Explains the fundamentals of quantum computers and what they can do, and answers some of the underlying questions you may have after reading Section 2.

**Start here if you are relatively new to the subject of quantum computing, less experienced with the dynamics of technological shifts or you prefer to start your journey from the beginning to build knowledge from the bottom up.**

**4**

**YOUR ROADMAP TO READINESS FOR THE QUANTUM ERA**

Establishes the guiding principles and presents the governance model to develop your organizations' leadership posture, quantum strategy, and step-by-step plan to move forward with confidence and clarity.

**Read this to fully invest and quick start the development of your organization's response or to gain insight into how you can ensure your effective oversight of your organization's existing quantum response.**

**5**

**APPENDICES AND TOOLS**

Includes a lexicon of terms and references to additional resources.

**Use this as a launchpad to deep dive into the topic and orient your inroads into the greater ecosystem.**

**6**

**CONTRIBUTORS AND ACKNOWLEDGMENTS**

Showcases expert contributors and the perspectives they bring to this document and field.

02

# What Every Leader Needs to Know

> The winners will be those who learn and act faster than the landscape changes.

**This section of the guide provides a high-level overview of the stakes and reasons to act. Subsequent sections provide greater reflection and depth.**

The momentum is unmistakable; it is no longer a question of *if* but *when* quantum computers will emerge as a transformational driver.

Quantum engineering breakthroughs are being announced at an ever-increasing pace; governments are jockeying to direct greater focus and investment to quantum technologies, while national security agencies are mobilized to secure sensitive data in anticipation of "**Q-Day**". Meanwhile, leaders in finance, pharma, energy, and logistics are testing quantum computing use cases, building roadmaps, securing key expertise, and partnerships. Yet despite this momentum, most organizations are neither prepared nor equipped to plan for its implications. In many cases, it's not even on their radar. By the time they look up, quantum will already have reshaped the ground beneath them, including across all three digital, economic, and political landscapes.

Quantum computing capabilities simultaneously inspire and threaten our future. On the positive side, they will speed up breakthroughs in science, solve complex industrial challenges, and may ease the growing strain that AI places on power systems. On the darker side, they enable the exposure of confidential information and have the power to disrupt global communications, economic stability, and national security systems through the collapse of digital trust.

**Q-Day** is the future moment when quantum computers become powerful enough to break many of today's widely used encryption and authentication methods, exposing previously protected information and compromising the very foundations of digital trust. This is because many of the mathematical foundations behind today's encryption and authentication methods are precisely the types of problems quantum computers excel at solving. Critically, while Q-Day is future-dated, **the risk is already present**, as sensitive information is already being harvested to be exposed and used later.

## Why is this different?

Like any tool, quantum computers are inherently neutral, reflecting the intentions of those who wield them. Whether this new technology is used to solve humanity's greatest challenges or to deepen inequality and harm depends entirely on the choices we make as leaders, innovators, and individuals. What is different this time is the **sheer magnitude of the risks** and the disquieting reality that control over who uses this new tool and how is beyond our reach.

To those on the ground, the imperatives are clear: **immediate mobilization is required**. To those in the seats of power with the fiduciary responsibility to act, the discussion is unintelligible, shrouded in technical jargon and concepts too obscure to grasp, let alone act upon.

Meanwhile, quantum computing power grows, Q-Day approaches, and so do the risks and impacts for those who fail to prepare. Only once the imperatives of quantum computing are made clear to boards and executives can leadership take hold. **Let's break it down.**

## 2.1 What's at Stake

**What seems like an overnight breakthrough is, in fact, the outcome of decades of disciplined research and strategic foresight. That same foresight now makes one thing clear: *the stakes could not be higher*.**

Here are some of the most important considerations of a quantum enabled future:

### Cyber Security

Fault-tolerant quantum computers will undermine many of today's encryption and authentication methods, putting at risk all data and communication channels that rely on them. The impact will be universal, touching every country, organization, and individual connected to the internet. This threat extends well beyond the confidentiality of information, it goes to the core digital identity integrity. A compromise at this level could **trigger a systemic collapse of digital trust -** the invisible bedrock that makes the global digital network viable for commerce, coordination, command execution, and decision-making.

### Strategic Advantage

Quantum computers will be able to solve problems that classical computers cannot, creating important strategic advantages for countries and organizations that are able to harness its power. These advantages will be available across industries, including finance, healthcare, energy, and logistics. Early movers are already securing partnerships, IP, and building talent pools, which will advantage them for years to come. Unlike the current AI transformation, which benefited from an existing supply chain and rapid scalability of existing infrastructure to meet growing needs, there is no existing infrastructure for quantum. **Late players to quantum will be shut out and unable to catch up.**

### Capability Gap

Preparing a country or large organization to face these risks and seize these opportunities requires years of groundwork. New expertise and capabilities are needed, which will need to be supported by a myriad of functions, policies, and processes, not to mention new tools and technology. Building new capabilities takes time. Just as few organizations can effectively deploy reliable and secure AI solutions 3 years after its emergence, **waiting until "quantum is ready" ensures you won't be.**

### Sovereignty

Because of its incredible potential, both as a threat and a strategic advantage, quantum computing has the power to reshape global economics and political dynamics. The development of national quantum expertise, industries, and ecosystems to fortify our **digital & technological sovereignty is essential** given political uncertainty and ongoing challenges of maintaining the global social fabric.

### Canada's Quantum Crossroad

Thanks to a generation of visionaries, Canada holds a rare lead position in the global quantum landscape. We have one of the highest per capita ratios of quantum scientists, engineers, and compagnies in the world. But we have been here before and history has taught us a sobering lesson[9]. Maintaining our edge demands more than academic excellence and an entrepreneurial spirit. It requires coordinated efforts in support of industrial innovation ecosystems. This includes the active engagement of large organizations such as banks, manufacturers, utilities, and government to translate our scientific strength into tangible economic power and through it, lasting political influence.

### Role of Finance

Finance is uniquely positioned and partially accountable to mobilize itself and other industries because it stewards the world's trust infrastructure. Unmanaged quantum risk threatens digital trust, which underpins the principles of transaction and market confidence. More than any other sector, finance can and must drive global quantum readiness by leveraging its internal expertise, international structures and influence[10] over trust networks to set standards and enable coordinated cross-border post quantum cryptographic migration.

## 2.2 Your Call to Action

**Immediate action is required not only because the stakes are high, but because the window for preparation is closing.**

Here are some of the most important considerations of a quantum enabled future:

1. **This is not a future risk but a present-day threat.**
Attackers can capture your encrypted data and digital certificates today to exploit later once full quantum computing power is available. The twin threats of "Harvest Now, Decrypt Later" and "Trust Now, Forge Later," put all information with a usable lifetime of more than several years at risk, including historical and legacy data.

2. **Your fiduciary duty may already be at stake.**
Privacy and data protection laws obligate organizations to take the necessary security measures to protect confidential and personal information. These includes provisions that hold directors directly responsible for omissions constituting an offence, while what constitutes *necessary security measures* evolves over time. Given that many recognized standard bodies have clearly highlighted heightened IT security risks[11] associated with advances in quantum computing, **inaction may soon register as a decision.**

3. **This time the consequences will be different.**
A sharp failure is different to a slow bleed. The impacts of AI unpreparedness have thus far been felt as a loss of competitiveness, inefficiency, and leadership frustration. The impact of quantum unpreparedness will be different: it risks a step-change failure, resulting in multi-year cybersecurity crisis management and remediation. Similarly, organizations who fail to build internal capabilities to leverage quantum's strategic potential will be challenged to compete for expertise, resources and partners later.

[9] Aerospace, Telecom and AI are areas where Canada demonstrated innovation and leadership early on, but which we failed to sustain over time.

[10] FS-ISAC (Financial Services Information Sharing and Analytic Services Center) is already working with many institutions at the international level, now is the time for us to organize and show collective leadership at the national level.

[11] e.g.: the National Institute of Standards and Technology (NIST), the Canadian Center for Cyber Security (CCCS) provide general guidance, while X9 and the Financial Services Information Sharing and Analysis Center (FS-ISAC) have published guidelines specifically for finance.

4 **Our national competitive edge at risk**.
Without mobilization at scale, not only will Canadian innovations be monetized elsewhere, but we also risk weakening national resilience, technological sovereignty and with it, your organization's access to critical skills, secured platforms, and reliable supply chains in the years to come. Innovation without commercialization leads us nowhere. We've proven we can lead but have a history of letting our leadership position slip away. **Let's not repeat this with quantum.**

5 **Organizations need time to mobilize.**
It takes decisive leadership and an average of 3+ years to build enterprise readiness for an important technological shift. Leadership must be educated and aligned, strategy must be shifted, funds must be reallocated, people must be trained, decision making must be adapted, and lasting capabilities must be built. None of this happens overnight, and does not include the migration itself, which will take much longer.

6 **Significant effort and complexity lie ahead.**
The migration of your cryptographic infrastructure is no small feat. For large organizations, it may be the **most complex technology migration ever**[12]. It is a discovery process with many unknowns and complexities taking you to the very root-of-trust. Multiple decisions lie ahead as you identify and evaluate the impacts of each change [13]. The scale and effort of the work will be significant for all organizations and financial institutions in particular.

7 **We have the tools we need to protect ourselves.**
*Post-quantum cryptography* [14] standards and the technology to enable them are already available. More than that, world-class expertise and leading products are being produced right here in Canada. Using cryptographic systems designed and built by Canadian companies reinforces our digital and technological sovereignty.

8 **Our quantum ecosystem needs you.**
Our universities and quantum industries have the talent and are building the solutions to help your organization capitalize on the potential of quantum computing, but the industry cannot develop in a bubble. Real world problems drive real innovation. We have reached the stage in quantum computing development where partnerships are essential and will produce a win-win impact on the ecosystem and on the organizations that engage with them.

9 **Overcoming traditional barriers.**
Collaboration and transparency among historically protective players will be vital to securing national sovereignty and creating value for all contributors. Given the breadth of needs that will need to be met to keep up with the quantum era, a traditional siloed approach of withholding strategic information and technical advantages from corporate competitors will leave the national ecosystem incapable of turning the corner and reaching quantum sovereignty.

10 **There is a roadmap.**
This guide provides you with the essential knowledge and the clarity you need to act, including a comprehensive step-by-step approach to navigate the different facets of quantum opportunities and threats: Imminent risk posture (0-12 months), Experimentation & Enterprise Capability Development (0-2 years), and Strategic Advantage (3+ years).

[12] See Quantum Readiness / PQC Migration Is the Largest, Most Complex IT/OT Overhaul Ever, Marin Ivezic for a broader understanding of the scale.
[13] See Appendix for CFDIR-QEWG best practices and guide for post-quantum cryptography migration clarity on the work ahead.
[14] Post-quantum cryptography (PQC) is designed to withstand attacks from quantum computers, ensuring the continued security of digital communications and data in the quantum era.

## 2.2.1 Urgency Compass

This Urgency Compass reveals how the pace at which you mobilize and the scope of your response determine whether your organization ends up leading or scrambling on Q-Day. Use it alongside **Mosca's Theorem**[15] to anchor discussions about your organizational vision and to communicate clear expectations to your quantum-readiness teams.

**The decisions you will make the next 0 –18 months determine which quadrant of the Urgency Compass your organization will be positioned on Q-Day.**


### Axes Explained

**Horizontal axis – How quickly you build your quantum capabilities**

Represents the elapsed time your organization takes to develop and execute your quantum strategy. The longer you wait to act and the longer it takes you to execute, the harder it becomes to secure the required skills and resources and mitigate your risks. **Early movers build capability deliberately; late movers are forced into costly reaction.**

**Vertical axis – How quickly Q-day arrives**

Represents the elapsed time before quantum disruption becomes material. The bottom of the y-axis represents an earlier Q-Day arrival, while the top represents a later Q-Day arrival. The sudden or early arrival of Q-Day **will leave late movers or those who failed to drive effective migration plans, scrambling or dead in the water.**

[15] Mosca's Theorem shows that long-lived data becomes vulnerable today if the time it must stay secure plus the time needed to migrate is longer than the time until powerful quantum computers emerge.

## 2.3 What You Need to Know

**This guidebook is designed to help directors and leaders deepen their understanding of how to act strategically and responsibly**

As a leader with fiducial responsibilities, here is what you should know:

- The implications of this new technology class on your organization and its potential global impacts, including both risks and opportunities.
- How the quantum landscape is evolving and how this evolution impacts the threats and opportunities that your organization is facing.
- Your role and responsibilities in navigating your organization in the face of technological disruption of this scale.
- Who is accountable for keeping you informed and developing your organization's response and do they have the necessary resources to do so effectively.

**Acting proactively costs less and creates value[16] while multi-year crisis management and remediation leaves generational scars on an organization.**

## 2.4 Immediate Next Steps for Leaders

As a board or executive team member, you must act with foresight and urgency in the face of quantum's risks and opportunities.

This section offers a pragmatic, high-level view of the work ahead. Use it as a quick guide to help you govern responsibly and position your organization to seize advantage as the quantum era unfolds. **Section 4: Your Roadmap to Readiness for the Quantum Era** offers more information on the scope of the work to be done to execute a truly successful and complete quantum readiness strategy.

**Year-one will be busy. Just remember, the sooner you act and the better you prepare, the less risk and cost of the work you will need to later.**

### Here's what you need to do:

Next 0-90 days

### Assume your Fiduciary Duty

**Don't wait for regulation**
Regulation is coming. The signals are abundantly clear. Waiting only puts you at a strategic disadvantage while increasing your risks and costs.

**Get educated**
Deploy a board and senior leadership education program[17] to ensure you understand the implications of this new class of technologies. Mandate ongoing training and briefing programs thereafter to stay informed and follow the evolution of the landscape.

**Secure key expertise**
You need talent across multiple domains[18] to guide your organization securely and strategically forward. No one has done this before, but some people have been thinking and planning for it for a long time[19]. Get some of those people.

**Mandate a post quantum defence strategy**
Direct management to launch a quantum-safe program to update your organization's cryptographic infrastructure. As a first deliverable, ask for their plan to make their plan.

[16] Beyond internal efficiency, early readiness also strengthens your organization's investor confidence as responsible, forward-thinking investors increasingly evaluate technology risk management and with it, quantum preparedness as part of stewardship and valuation criteria.
[17] Visit ldiq.ca for information on our board and executive leader training programs.
[18] Quantum educators, ecosystem liaison, post-quantum encryption experts, physics educated modellers, quantum aware policy makers and risk managers.
[19] The Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR) is a great example of Canadian pioneers in this area.

Next 90-180 Days

## Organize for Success

**Establish a "Quantum Readiness Team"**
There are many aspects and breadth to quantum computing readiness and different expertise will be required to address them all. Establish a multidisciplinary leadership response team to consolidate expertise, coordinate your response and ensure you don't work in a fragmented or siloed way.

**Commission a high-level risk and opportunity assessment**
The purpose is to obtain a first fuzzy picture of what is at stake for your organization, including your greater risk exposure, which goes beyond cryptographic urgency, as well as your high-level opportunity assessment.

**Implement formal governance and reporting**
Identify key decisions and accountabilities. Implement quarterly reporting on readiness milestones, risks, vendor alignment, and regulatory engagement to ensure accountability and long-term focus. Establish your position on digital and technological sovereignty and the role your organization will play in reinforcing it.

**Align on your defensive intent**
Identify which quadrant of the Urgency Compass you want your organization to be positioned in and your internal estimate of Q-Day. Develop and embed a clear discourse on what this means in your risk appetite, strategic priorities, and stakeholder communications.

**Connect with your industry peers**
The stakes are very high. We have more to gain by working together than in isolation when it comes to the questions of global digital trust and national sovereignty. Leverage industry forums and host peer events to share knowledge on post-quantum cryptography migration plans.

Next 180-270 Days

## Broaden the Field

**Publish your defensive roadmap**
It should include and lead with a stream to build crypto-agility as well as a stream to complete your migration to post-quantum cryptography, baseline assumptions, resource requirements and estimated timelines to complete your migration.

**Allocate budget**
Treat post-quantum encryption as a multi-year capital program, not a one-off project. Assign budget for cryptographic inventory, migration tools, workforce training, vendor contracts, and independent testing.

**Identify your quantum use case opportunities**
Use it or lose it. Build a qualified pipeline of value creation quantum use cases. Consolidate your quantum-savvy analysts and modellers into a centralized team and start building your quantum computing expertise.

**Engage guides and key partners**
If you have not already done so, now is the time to establish contracts and partnerships with quantum industry players. Demand will grow rapidly as awareness increases and Q-Day approaches. Act now to secure your place in the national supply chain and to ensure they survive and thrive to be able to support you later.

Next 270-360 days

## Leverage Your Leadership Position

**Update policies and compliance monitoring**
Many policies need to be reviewed including procurement, security, and third-party risk. Deploy monitoring and controls to put pressure on vendors to meet post-quantum cryptography standards. Require roadmaps and sovereignty posture in contracts and RFPs.

**Engage in the standards ecosystem**
Participate in national and international forums to shape standards and protocols, influence adoption timelines, and strengthen your organization's and our national position.

## 2.3 Key Questions for Leaders to Ask

The following is a list of questions that executive leaders and board members should ask to help you establish your organizational posture in relation to quantum computing readiness.

- Is this displacement of technology sufficiently elevated to warrant board-level oversight? (**Yes**)
- Are board and leadership team members sufficiently literate on quantum-related matters?
- What is our current exposure? What is our long-life data and when do we estimate the likely timing of Q-Day?
- Where can quantum technologies unlock new opportunities for our organization (e.g.: new financial products) or yield competitive advantage (ex: through early adoption)?
- What is our *quantum ambition* (e.g.: early adopters, followers, cautious observers)?
- On which quadrant of the Urgency Compass are we aiming to be on Q-Day?
- Have we inventoried all our cryptographic systems, data, and communication channels that rely on them? Do we know which are vulnerable?
- Do we have a roadmap to migrate to quantum-safe cryptography? Do we have sufficient resources and priority assigned to meet our milestones?
- Do we have a plan if quantum computing matures before we are ready?
- What is our position on digital and technological sovereignty, in general and specifically for quantum?
- What is our role on quantum technology ecosystem stewardship?
- What processes do we have for monitoring emerging standards, regulations, and threats in the quantum and cryptographic space?
- What legal or fiduciary implications may arise as quantum alters *reasonable oversight* expectations?
- Who within the executive team is leading our quantum readiness initiative?
- Do we have the necessary expertise to formulate our response?

*See the appendix for additional questions to ask once your initial posture is established.*

# 03 Additional Knowledge for Leaders

> Knowledge is power. But only through understanding do we acquire the confidence to use it.

This section of the document provides greater context and detail. Use it to consolidate your knowledge and increase your understanding.

## 3.1 What is quantum computing?

### 3.1.1 Q: What makes quantum computers different from classical computers?

The key differences between a quantum computer and a classical computer rest in the physical architecture and in the information models that they employ.

Classical computers store information in bits that exist in one definite state - either 0 or 1. Quantum computers use qubits, which can exist in multiple states at the same time through quantum mechanics properties. These properties make quantum computers more powerful for certain types of mathematical problems, like simulating molecular behaviour, compromising certain methods of cryptography, or optimizing complex systems. Quantum computers can dramatically outperform classical computers at solving these types of problems.

Importantly, they're not simply "faster" computers - they're **fundamentally different tools** that excel at certain tasks when compared to classical computers.

### 3.1.2 Q: Do I need to know quantum physics?

**No.** Quantum physics is deeply counterintuitive and notoriously hard to grasp. As an executive leader or board member, you do not need to understand quantum physics nor the technical details quantum computing beyond what is presented in this guide.

Stay focussed on strategy, on making sure you have the right team in place and ensuring they have everything they need to be effective, including the necessary knowledge, resources and funding.

### 3.1.3 Q: Which industries will benefit from quantum computing?

**Any sector that grapples with complexity, uncertainty, or optimization** stands to benefit from quantum computing. Its power to process vast, multidimensional problems and simulate reality at a quantum level will profoundly reshape how industries understand, design, predict, and decide.

## Pharmaceuticals and Healthcare

Quantum computers could revolutionize drug discovery and biomedical research by acurately simulating molecules and proteins, accelerating the identification of viable compounds and reducing the cost and duration of clinical trials.

## Energy and Materials

Energy companies could exploit quantum modelling to design new catalysts, superconducting materials, and efficient batteries, unlocking breakthroughs in energy storage, hydrogen production, and carbon capture. Quantum optimization could improve power-grid dispatching, balancing demand, generation cost, and carbon emissions in real time.

## Transportation and Logistics

Airlines, shipping companies, and logistics providers face inherently complex scheduling and routing problems. Quantum optimization could minimize delays, fuel use, and emissions in fleet scheduling, route planning, and supply-chain network design, all while improving resilience to disruptions.

## Manufacturing and Aerospace

By simulating atomic-level material properties, quantum computing can enable lighter, stronger materials, improved composites, and optimized manufacturing processes, contributing to safer aircraft, more efficient production lines, and sustainable product innovation. Quantum computers could potentially simulate turbulent flow and aerodynamic behaviour more accurately than classical computers, improving designs for wings, engines, and control surfaces.

## Climate and Environmental Sciences

Quantum simulations can improve weather forecasting, climate modelling, and carbon-capture research, enabling governments and corporations to make more informed adaptation and mitigation decisions.

## Financial Services

Last, but not least, the financial sector stands among the earliest sectors to benefit from and adopt quantum computing because of its inhouse skills and risk modelling and optimization needs. Potential applications include:

- **Portfolio Optimization and Asset Allocation**: Quantum algorithms could simultaneously evaluate thousands of correlated assets and constraints to identify optimal investment mixes that maximize return for a given level of risk.
- **Credit and Market Risk Modelling:** Quantum-enhanced simulations can capture complex interdependencies and tail-risk scenarios far beyond the reach of classical Monte Carlo methods, improving capital adequacy and stress-testing precision.
- **Fraud Detection and Anomaly Analysis**: By examining patterns across vast, high-dimensional transaction datasets, quantum-accelerated machine learning could detect subtle irregularities faster and with fewer false positives.
- **Intraday Liquidity and Collateral Optimization**: Banks and clearing houses could dynamically optimize collateral placement and liquidity flows across multiple currencies and jurisdictions, minimizing funding costs and operational risk.
- **Trade Execution and Routing**: Quantum optimization may improve algorithmic execution strategies, reducing slippage, latency, and transaction fees across fragmented markets.
- **Climate and ESG Risk Assessment**: Quantum simulations can integrate physical climate models and financial exposures to quantify long-term climate and transition risks with higher fidelity.

As transformative as these examples appear, they likely represent only the beginning. As quantum technologies mature and expertise spreads across industries, new and unforeseen applications will inevitably emerge, comparable in impact to the early days of advanced analytics and artificial intelligence.

### 3.1.4 Q: Will quantum computers replace classical computers?

**No**. Since the advantages of quantum computers are limited to certain types of problems, they are not viewed as a wholesale replacement for classical computing, rather a specialized tool that offers important advantages for specific types of problems. Classical supercomputers will continue to evolve and work side-by-side with quantum computers leveraging the best capabilities of each class of computing technology.

### 3.1.5 Q: What are the risks of quantum computing?

The greatest risk lies in the ability of fault-tolerant quantum computers to disrupt cybersecurity on a global scale.

Left unmitigated, this risk will have a very profound impact on every aspect of our lives, across the digital and into the physical plains. There are different layers to this risk. **It helps to unpack them one by one.**

#### First layer: Breach of confidentiality

This is the risk are that is most often cited. By virtue of their capacity to compromise existing cryptographic protections, quantum computers will enable the exposure of confidential information. This encompasses all data, including personal identifiers, trade secrets and defense-sensitive military information.

#### Second layer: "Harvest now, Decrypt later"

Connected to the first layer, this describes the real and present threat that nefarious parties are already collecting encrypted information with the intention of exposing it later using the power of future generation quantum computers. It demands immediate action and protection measures. All data with a sensitivity lifetime of more than a few years is at risk.

#### Third layer: "Trust Now, Forge Later"

Trust Now, Forge Later is the dynamic counterpart of Harvest Now, Decrypt Later. While the latter threatens to expose confidential of data, Trust Now, Forge Later threaten the legitimacy of digital certificates and signatures and the authentication processes they are tied to.  Forged identities give attackers a silent and legitimate-looking pathway into systems, allowing them to act with the same authority as trusted users. This digital identity threat is even more critical than the confidentiality threat, **as it compromises the fundamental nature of digital trust.**

### Why is Digital Trust so Critical?

Digital trust is the invisible bedrock that makes the digital world reliable for commercial transactions, secured communications, and everyday life. It is the foundation of the Internet, and all connected systems that run modern society depend on it, including commercial, public and personal devices.

Just as a personal ID and signature are used to authenticate an individual and certify a transaction, digital certificates and signatures authenticate our presence and actions online. In the digital world, they extend to computer systems.

The ability to forge a digital certificate or signature would allow nefarious parties to invisibly penetrate digital networks under usurped identifies, challenges ownership of information, but also to act on industrial controls, critical infrastructure, healthcare systems, transportation, and defence. In these sectors, a loss of integrity is more catastrophic than a loss of confidentiality.

Quantum-enabled digital forgery capabilities could disrupt essential services, compromise entire supply chains, and create cascading physical consequences across our deeply interconnected digital-physical world. While the confidentiality risk raised by the Harvest Now, Decrypt Later has been widely recognized, **it is the digital identity threat that poses the biggest risk.**

**Once you understand the threat to digital trust[20], it is impossible to ignore the urgency of immediate mobilization.**

### Risk Summary

A broader risk perspective includes[21]:

1. **Risk of loss of trust across the digital economy ("Trust Now, Forge Later")**
2. **Risk of exposing confidential data ("Harvest Now, Decrypt Later")**
3. **Risk of loss of sovereignty over critical technology or services**
4. **Risk of loss of opportunity and quantum-based advantage to competitors**

## 3.1.6 Q: What is post-quantum cryptography?

**Let's start with cryptography as a whole.** Cryptography is the system that allows information to remain secure by ensuring that data, messages, commands, and transactions can only be accessed or executed by authorized and verifiable parties. It encompasses a suite of mechanisms, including encryption, digital signatures, authentication certificates, and secure key exchange protocols.

A critical component of our cryptography system is the Public Key Infrastructure which enables the creation, management, distribution, use, and revocation of digital certificates and cryptographic keys at a global scale. These keys are the foundation of secure digital functions such as encryption, digital signatures, and authentication.

[20] For more depth on the topic of digital trust, see A Quantum Leap That Breaks Trust, Not Just Code, Marin Ivenic
[21] See the Appendix for more information on the broader risk perspective.

**Robust post-quantum cryptography migration plans consider all dimensions of the solution architecture, including hardware.**

Cryptographic systems depend on mathematical algorithms. For a cryptographic system to be secure, its underlying algorithms must be computationally infeasible to break in a reasonable amount of time using current and foreseeable technologies. For the past three decades, most cryptographic algorithms have relied on certain classes of mathematical problems that could not be viably solved by classical computers. These problems will be solvable with the advent of sufficiently powerful quantum computers.

**Post-quantum cryptography** represents the next generation of cryptographic algorithms. They are based on mathematical problems for which no quantum advantage is known today and for which experts believe none is likely to emerge. It does not rely on quantum technology; it is designed to run efficiently on classical computing systems.

To preserve digital trust in the quantum era, all digital systems will need to migrate to post-quantum cryptographic standards and methods. **This transition can and must begin today**.

**This is much more than a software upgrade.** It is a common misconception is that post-quantum migration is a simple update or just a *vendor problem*. Cryptographic systems are complex and go to the root of your network architecture. Even small changes in cryptographic exchanges can ripple through an organization's infrastructure in unexpected ways. Ensure your team knows and is equipped to understand and tell you the full story of your organization's post-quantum cryptography migration needs and plan.

### 3.1.7 Q: What is crypto agility, really?

The golden age of cryptography, when a single set of algorithms could safeguard the digital world for decades, is over. The unbounded power of quantum computing and growing sophistication of AI ensure that cryptographic complacency will never be possible again.

More than a one-time migration to post-quantum cryptography, we must build the capacity to adapt our cryptographic infrastructure continuously and dynamically. Updates will be required, adversaries will refine techniques, and new vulnerabilities and standards will emerge. So must our ability to keep pace.

The FS-ISAC[22] defines **crypto agility** as "an organization's ability to adapt cryptographic solutions or algorithms (including their parameters and keys) quickly and efficiently in response to developments in cryptanalysis, emerging threats, technological advances, and/or vulnerabilities." But also, and importantly, as "a design principle for implementing, updating, replacing, running, and adapting cryptography and related business processes and policies with no significant architectural changes, minimal disruption to business operations, and short transition time."

**"Agility" is the ability to move swiftly in an assured way. It is achieved through the combination of awareness, flexibility, and core strength.**

**What this means:** Achieving crypto agility is not a technology problem; it is a capability and operating-model design problem. New operational frameworks must be established to provide the professionals who manage cryptographic systems (1) fine level visibility on organizational assets and threat monitoring capabilities (awareness), (2) autonomy of action and decision-making latitude (flexibility), supported by (3) clearly defined communication channels, guidelines, and risk-based controls (core strength) to manage cryptographic system updates in an agile way.

**Going forward, all organizations must ensure their crypto agility. It's time to listen to your IT, Cyber and Cryptographic teams.**

[22] FS-ISAC: The Financial Services Information Sharing and Analysis Center is an industry consortium dedicated to reducing cyber-risk in the global financial system. Serving financial institutions and in turn their customers. The FS-ISAC has over 5,000-member firms with users in 75 countries.

### 3.1.8 Q: What is the relationship between quantum computing and AI?

Quantum computing and AI have historically evolved as separate disciplines, but they are now increasingly converging in ways that allow each field to accelerate the other. Broadly, the quantum–AI relationship can be grouped into three categories, each with its own maturity level:

1. **AI for Quantum (Current Reality):** AI is already playing an essential role in advancing quantum technologies by helping design better quantum hardware, optimize how quantum systems operate, and create more reliable ways to correct errors. For example, machine learning methods are used to design and optimize quantum circuits, characterize and mitigate hardware noise, and enable practical quantum error correction.

   **Status and impact:** This is the most mature and impactful intersection today, with active deployment in research laboratories and early industrial tools. AI for Quantum makes quantum systems more efficient and reliable for practical use.

2. **Quantum-Inspired AI (The Bridge):** Quantum-inspired AI adopts ideas from quantum physics to make certain machine learning and optimization tasks more efficient on today's classical computers. For example, tensor networks, originally developed to represent and simulate quantum many-body systems, can compress parts of some large models and reduce memory use and computational cost, often with little loss in accuracy.

   **Status and impact:** Quantum-inspired AI approaches are being used today, most notably in commercial optimization tools and model compression for machine learning, making them a near-term bridge between today's AI systems and future quantum-accelerated workflows.

**Quantum many-body physics** studies systems where many quantum particles interact and collective behaviour emerges. This matters because many key phenomena underpinning modern quantum technologies are inherently many-body in nature.

**Tensor networks** are a mathematical framework for representing complex systems in a compact, structured way. Think of them as high-efficiency compression for relationships within data: instead of storing every possible interaction explicitly, which can grow exponentially, tensor networks break the system into smaller building blocks (tensors) connected in a network that captures only the essential dependencies.

3. **Quantum for AI (Future Potential).** A promising long-term goal is to run parts of AI workflows directly on quantum processors. This emerging field, known as Quantum Machine Learning, explores whether quantum states and operations can accelerate or improve specific learning tasks, and whether certain well-structured workloads may benefit from quantum resources.

   **Status and impact:** Quantum Machine Learning is still in the research and prototyping stage. Theoretical advantages exist for specific, carefully constructed tasks, and in the long term quantum processors could offer lower energy consumption per computation if scalable, fault-tolerant hardware becomes practical. However, real-world performance gains over state-of-the-art classical AI have not yet been demonstrated.

### 3.1.9 Q: What quantum computing capacity is available today?

As you read this, low fidelity, limited scale quantum computers exist. The industry refers to this current period as "NISQ era computers" (Noisy Intermediate-Scale Quantum). Noise in this case refers to the high degree of error associated with these current quantum computers.

These devices operate with a limited number of qubits. Much of the work ahead is to transform these noisy, error-prone *physical qubits* into error-corrected *logical" qubits*[23]. As the number of logical qubits increases, we move closer to scalable, fault-tolerant quantum computers and with it machines capable of delivering all that is possible.

First movers in finance, pharma and logistics are already leveraging noisy quantum computers to test the potential of quantum computers in their different fields. And, several quantum computer manufacturers offer guided experimentation and even packaged proof of concept initiatives with solutions tailored to different industries.

It is, in fact, **quite easy to get your feet wet at this time**. Also quite advantageous, as relationships and partnerships formed with quantum computing industry members now will provide invaluable access to knowledge, talent, and hardware when fault-tolerant quantum computers emerge. At that time, expect a rush to access these highly specialized and limited resources.

### 3.1.10 Q: When will fault tolerant quantum computers be ready?

Different estimates exist, with the investor community being more bullish and certain academics more reserved. What is certain is that the race is on.

From an industry perspective, many quantum industry players' roadmaps coalesce on a 5-year horizon, culminating in 2030. From a defensive posture, the Canadian Centre for Cyber Security has mandated all public agencies to secure their critical systems by the end of 2031. With these in mind, a reasonable risk view is that **Q-Day could arrive by 2030**, with the probability rising each year thereafter.

This provides organizations **less than 5 years** to build the necessary capabilities to complete the high priority elements of their transformation. Already an aggressive timeline, meeting it does nothing to protect against the twin "Harvest Now, Decrypt Later" and "Trust Now, Forge Later" threats, which, for many, may already be too late.

### 3.1.11 Q: How much of this is noise vs. substantive?

As with any emerging technology cycle, there is speculation and noise but there are also clear, indisputable signals that quantum technologies are approaching the point of readiness.
Here are the signals to look for:

**As of Q4 2025, all these signals have clearly and verifiably emerged.**

**It's not just noise.**

- Significant investments and strategic commitments from establish industry players.
- Policy and standards emissions.
- Government programs, investments.
- Mandatory transitions and target dates.
- Roadmap commitments and alignment among big vendors
- Peer-reviewed results illustrating important performance gains.
- Pilots using real-world problems that achieve quantified benefits.
- Sector consortium momentum and playbooks.

[23] Certain qubit architectures may require 1000 physical qubits to create a single logical qubit.

## 3.1.12 Q: Is this another Y2K moment?

**Yes, and No.**

But before we explain, let's reframe the paradigm: Where Y2K became a *non-event* should be recognized as a positive and not derisive result. Disaster was avoided because leaders acted early with clear ownership, budgets, and cross-industry coordination. The same foresight, action and coordination that made Y2K uneventful is what we need to make the quantum transition resilient to disruption.

With that in mind, let's compare.

Attesting to some of the similarities and significance of these two events, the term "Y2Q" made a brief appearance online in November 2025. It remains to be seen if it will become popularized.

### Yes, because

**It carries global systemic impact**
Y2K affected all systems across all industries around the globe. Ensuring the Y2K mitigation required every country to mobilize.

**The solution is enterprise driven**
Each organization plays a role in mitigating the risk and systemic impacts by correcting its own platforms and tools. Like Y2K, we need the think globally, act locally.

**It requires global synchronization on standards**
Albeit simpler, navigating Y2K required us to align on common standards and coordinate complex migrations between interconnected systems.

### No, because

**It is bigger**
The internet was in its infancy in 1999, and information and operational technology was nowhere near as pervasive as it is today. We are degrees of magnitude higher in terms of the number of connected devices we have now.

**It is an ongoing threat**
Y2K had a specific expiry date and required only a one-time correction, whereas the timing of Q-Day remains unknown, and the threat will never go away. The yet unbound advancement of quantum and AI technologies means that organizations must continuously stay ahead of the threat through crypto agility.

**The risk has already materialized even if it impacts cannot yet be felt**
The dual threats of Harvest Now, Decrypt Later and Trust Now, Forge Later mean that some information may already be compromised. We can limit our exposure by migrating to post-quantum cryptographic technology as quickly as possible but cannot eliminate the risk as was the case for Y2K.

**We can act more strategically**
Y2K was a first exercise in global technology risk at a time when IT risk management methodology was immature; it is probable that some corrective Y2K work was unnecessary. Current IT risk management practices are much more sophisticated, which means that we act more strategically to prioritize our highest risks and eliminate unnecessary work more effectively.

## 3.1.13 Q: What is the scope of my fiduciary duty?

Under the Canada Business Corporations Act (CBCA), directors and officers have two principal duties: a duty of care and a duty of loyalty. The duty of care imposed by CBCA requires that each director and officer of a corporation, in exercising their powers and discharging their duties, must exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances.

The duty of care requires that directors and officers make sufficient inquiries to inform themselves and consider all material information available to them prior to acting. The CBCA also imposes a fiduciary duty of loyalty that directors and officers act honestly and in good faith with a view to the best interests of the corporation. In considering what is in the best interests of the corporation, the Supreme Court of Canada has held that directors may look to the interests of, among other things, shareholders, employees, creditors, consumers, governments and the environment to inform their decisions.

One of the principal roles of board members is risk management and oversight, including approving and overseeing the implementation of a risk appetite framework and a corresponding internal control framework. Increasingly, privacy and data protection laws impose positive obligations on enterprises to take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information. Many such laws include provisions that hold directors directly responsible if they ordered or authorized the act or omission constituting an offence.

An assessment of what constitutes *necessary* security measures has evolved over time. Increasingly, recognized standards bodies, such as NIST, are highlighting heightened IT security risks that may result from advances in quantum computing. In other words, advances in quantum computing are resulting in *known risks* for many corporations. It is important for directors to start overseeing how corporate officers are assessing the risks and opportunities of quantum computing for your enterprise now, before it is too late.

### 3.1.14 Q: What new capabilities does my organization need to build?

As with any major transformation, the organization must evolve.  This means developing new operational capabilities to ensure not only the transition, but also your long-term success under the new quantum paradigm. Key areas to focus on include:

#### Governance and Risk

Policies must be updated to ensure that all vendors move to post-quantum cryptographic systems and controls must be in place to monitor compliance.  Roles, decision rights and sovereignty considerations must be re-examined. New risk indicators must be deployed.

#### Cybersecurity

New capabilities are required to monitor and meet a whole new category of threats. Crypto-agility must be developed to ensure your organization stays current with cryptographic standards. Already at maximum velocity, cyber security output needs to accelerate.

#### Strategic Partnerships

Preparing for the quantum era means building a new ecosystem, forming strategic partnerships, trusting new vendors, engaging in standards, collaborating with universities, and cultivating a community ready to innovate and respond together.

#### Asset Management

New dimensions of metadata must be defined to catalogue and distinguish long-life confidential data vs. short-life concerns.  IT asset identification and management must be updated to monitor vulnerabilities.

#### Processes and Controls

must be updated to consider new quantum risks and comply with new policies and standards. A dedicated quantum use-case pipeline should guide the selection, assessment, and funding of quantum opportunities.

#### Expertise and capacity

The quantum era requires new skills: quantum algorithms, cryptography management, quantum literacy, and updated risk management, along with the capacity to deliver a high-velocity PQC migration.

### 3.1.15 Q: How will this impact the environment?

**The news is promising.** At maturity, quantum computers are expected to require less energy than classical systems for the tasks where they perform better[24], making them a powerful tool for energy conservation at a time when AI-driven demand threatens global electricity supplies.

Beyond the direct impacts of energy consumption efficiency, the benefits of more reliable climate modelling results, energy grid management capabilities, and the potential for new sustainable and superconducting materials developed from quantum driven research amplify its potential environmental impact.

### 3.1.16 Q: How does Canada compare to other nations in this field?

**Incredibly well.** Canada is widely regarded as a global leader in quantum science and considered a nation that *punches above our weight* in terms of quantum expertise, industries and readiness. Thanks to the forward thinking of a generation of scientists, entrepreneurs, and policymakers, we are home to a vibrant ecosystem of quantum technology entrepreneurs[25], mature and highly regarded educational programs[20] and one of the highest numbers of quantum SMEs per capita[26] globally. We are also one of the few countries with a coordinated national plan for quantum security and our Canadian Institute for Advanced Reasearch (CIFAR) program helped lay the groundwork for international collaborations, giving Canada a voice in shaping the global quantum agenda.

While we are clearly positioned with an early lead, **we have been here before** (aerospace, telecom, AI). In terms of commercialization, we face intense competition from larger players like the United States, China, and the European Union.

Honouring the work of those who lay the foundation and seized the opportunity of our early lead requires your engagement and support in the ecosystem to help translate this advantage into tangible, sustained economic benefits and from that, political influence.

***See Appendix for a list of Canadian companies who are developing quantum computers.***

### 3.1.17 Q: How do first movers gain an advantage?

First movers gain advantage by being aware and learning earlier than their counterparts, securing scarce assets including talent, partnerships, and IP before the market tightens. Because of their early positioning, they participate in shaping standards, procurement terms, and ecosystem roadmaps to their benefit.

Early integration and the securing of important contracts establish their credibility and lock in relationships with scarce suppliers, which slows and disadvantages competitors, while credible leadership earns confidence from regulators, customers, and investors, unlocking approvals and trust capital to propel them forward.

These early relationships and access to resources are all the more important with quantum technologies because they are new. Unlike the case of AI, where scaling up our capabilities was enabled by augmented capacity on existing infrastructure, we have no existing quantum infrastructure to build off. It's akin to laying new tracks instead of just adding trains to meet the increase in passenger loads.

[24] Energy-Consumption Advantage of Quantum Computation, Florian Meier, Hayata Yamasaki

[25] In their June 2025 Quantum Technology Monitor, McKinsey ranked Canada second to the US in the number of Quantum Technology startups.

[26] See Quantum Industries Canada website

## 3.1.18 Q: Why must the financial sector lead the quantum transition?

Few industries are as well positioned, as motivated, or as obligated to lead the world in quantum capability building and standard setting as the financial sector, and banks in particular. Here's why:

### They are among the most at risk

The high-value nature of their information and global connectivity make banks prime targets for early quantum attacks. Because of their interconnectedness, a successful cryptographic breach at one major institution could cascade rapidly across the financial network.

### Banks have a reputation to uphold

Quantum readiness signals operational maturity, technological leadership, and governance excellence, which are the very qualities that most banks strive for.

### Banks have the necessary expertise

Banking has had a long-standing association with physics. Many of the banks employ physicists as part of their financial modelling teams (often in Risk Management and Trading). They also manage vast cryptographic infrastructure.

### Banks sit at the core of the global digital trust network

Banks maintain digital connections to every other major financial institution through clearing, settlement, and capital markets. This interdependence means banks have the systemic reach to drive standards globally.

### Banks are experienced at global coordination

Banks are a globally regulated industry and are already required to act to ensure their resilience. These same regulatory bodies are equipped to coordinate alignment and dissemination of regulations to which all banks must adhere.

### What banks do quickly becomes the standard

While all banks must comply with banking regulation, many other industries automatically align to them. They also carry a lot of clout. When a major bank demands post-quantum compliance in vendor contracts, the entire ecosystem moves.

### Within change lies opportunity

Beyond risk mitigation, first movers in finance will capture strategic advantage, including better risk models, higher performing portfolios and the opportunity for new quantum-secure products (post-quantum wallets or transaction verification).

Institutions like Banco Santander exemplify the type of forward-looking leadership required to guide the financial sector through the quantum transition: actively forming partnerships, developing internal capabilities, shaping standards across the global ecosystem and openly sharing their knowledge with others.

## 3.1.19 Q: Why are standards so important?

In the context of emerging technology, standards turn scientific breakthroughs into usable, interoperable, and commercially viable systems. They define common terminology, metrics, and interface protocols, ensuring that devices, algorithms, and security mechanisms developed by different parties can work together reliably. Without them, the quantum ecosystem risks fragmentation, incompatibility, and loss of trust in results.

Standards extend beyond technology to include things like migration timelines, decision-making forums and authoritative sources of information. Collectively, standards are what will enable a coordinated post-quantum cryptography transition rather than chaotic, isolated responses.

Being present and contributing to the development of standards ensures that your organization's (and our national) needs and realities are reflected in the rules. Early movers can seize advantages by influencing standards that advantage them during their development.

## 3.1.20 Why is sovereignty an important topic in the quantum era?

Sovereignty is the ability to make independent decisions and maintain control over what is essential to your organization and to our national interest. It has many dimensions, with the following as particularly relevant to the context of quantum computing.

**Digital sovereignty** has been a growing concern for some time. It refers to the ability to control, govern, and protect our data, but also digital identities and digital interactions. It answers a core question: Are our data, digital identities, and digital infrastructure secure, private, and truly under our control?  It covers topics including identity frameworks, data residency, and the integrity of authentication, certificates, and cryptography. At its heart, digital sovereignty is about preserving **digital trust.**

**Technological sovereignty** is the ability to source and evolve the critical technologies we rely on, including hardware, software, their underlying supply chains, as well as our R&D capacity and innovation ecosystem. Its central question is: Can we build or reliably source the technologies we depend on without strategic vulnerability?  In the quantum era, this includes quantum technologies, post-quantum cryptography hardware, their key enabling technologies such as cryogenic systems and lasers, as well as quantum research and intellectual property.

**Our level of digital and technological sovereignty determines our resilience and our ability to convert today's quantum intellectual capacity and leadership into tomorrow's economic power.**

04

# Your Roadmap to Readiness for the Quantum Era

> Luck is not a strategy -*Michele Mosca*

Quantum readiness won't happen by accident. Strategy and careful planning are essential. This section provides a comprehensive roadmap to build the capabilities, governance, partnerships, structures and safeguards needed to secure your organization and position it decisively on your targeted quadrant of the **Urgency Compass.**

4.1

## Guiding Principles

Guiding Principles ensure that decisions remain consistent, and priorities stay relevant, even as the landscape evolves and circumstances shift.

We propose the following as principles:

### Anchor in Purpose and Risk

The roadmap and your key performance and advancement indicators must reflect and monitor your advancement across the following three dimensions:

1. Fiduciary duty: leadership and governance in the face of change
2. Risk posture: quantum as a security threat
3. Long-term competitiveness: quantum as a future enabler of advantage

### Make Security Non-negotiable

Risk must come before reward. Prioritize threat mitigation to protect data, safeguard trust, and demonstrate responsible governance even as the threats and standards evolve.

### Build Lasting Capability

Go beyond one-off events and pilots. Build crypto-agility, embed cryptographic threat mitigation into day-to-day operations, not on a 30-year cycle. Invest in quantum literacy, governance, skills development, and vendor management to develop enduring organizational muscle that compounds over time.

## We're stronger together

The stakes are high. Possibly higher than they have ever been. We have more to gain by working together than in isolation when it comes to the questions of global digital trust and national sovereignty. Let your quantum strategy be driven by collaboration with industry peers rather than a competitive posture.

## Act with both certainty and optionality

You need flexibility and certainty in your plan. The rules are different depending on which stream you are acting on. Start by understanding where and why you will use each.

### Advance with cryptographic system certainty

In cryptography, standards are paramount. Robust cryptographic systems are not strong because they are secret; they are strong because they have been publicly scrutinized, tested, and proven by the global cryptography community. Treat your cryptographic architecture as the bedrock of your ecosystem. Stick to defined standards and go with the most robust, comprehensive tools available.

### Advance with qubit architecture optionality

It is too soon to tell which quantum computing technology will emerge as market standards and not all capabilities are transferable across different qubit architectures. Diversify partners and technologies as you explore quantum computing use to ensure you don't get left on the wayside of market standards.

## Think Globally, Act Locally

Engage globally to shape regulation and standards, but invest locally to grow talent, fuel innovation, protect sovereignty and build resilience into local supply chains, partnerships, and infrastructure.

## 4.2 Next 0–1 year: Imminent Risk Posture

All actions presented below are intended to run in parallel.

### 4.2.1 Get and Stay Informed

#### Provide Board and Executive training

Develop and deliver board and leadership training on the risks and opportunities of quantum computing[27].

- By virtue of their fiduciary accountability, board members are a key vector in ensuring management acts with appropriate urgency.
- An educated and engaged board is a tremendous asset and strategic differentiator in times of disruption.

#### Implement a rigorous reporting program

Keep your leadership and board informed and holding your delivery team accountable for providing pertinent and transparent information.

- Elevate PQC migration to a board-approved program with explicit fiduciary framing: protection of data and trust.
- Put thought into the information you want to use to report on your progress and the types of information that needs to be brought to the Board.
- A well-designed reporting mechanism is the best way to ensure you maintain focus on the right priorities and invest your resources where they bring the highest value and impact[25].

#### Take stock of Lessons Learned

The AI era revealed the cost of ungoverned acceleration. The quantum era demands foresight and control. Leverage your experience with AI Readiness to do things right this time.

- Where did you hit or miss your mark with AI strategy and readiness (governance and policies? risk management? talent? processes? decisions? data? leadership?)
- Use your past experience to shape a more deliberate and forward-looking approach to quantum readiness; one that acts strategically, with intention, and positions your organization to lead rather than react.

### Why This Is Important

The next several years will be tumultuous. Without informed leadership and disciplined reporting, organizations risk underestimating the pace of change and missing critical windows to protect their assets.

An educated board is a strategic asset in times of disruption. A well-briefed board is both a steering mechanism and an accelerator. Ensuring they are thoroughly prepared enhances your organization’s ability to respond swiftly in a crisis.

[27] This guide provides an effective framework and the essential content as the basis for this training.

## 4.2.2 Structure for Success

### Establish a "Quantum Readiness Team"

There are many dimensions to quantum computing readiness and different disciplines need to work together to prepare. To ensure you don't work in a fragmented or siloed way, you must create a coherent structure to consolidate expertise, and coordinate your response The Quantum Readiness Model illustrates the type of organization you will need.

- At its heart, lies your Quantum Readiness Team that brings together experts and leaders from your Business Strategy, IT, Risk, Cybersecurity, and Analytics sectors to lead your quantum strategy and coordinate organizational readiness.
- They work together to capture and share knowledge and maintain alignment on key dates and imperatives, while maintaining two distinct areas of focus:
  - **Post-Quantum Security Focus:** Led by the CISO and made accountable for the development and realization of your defensive strategy.
  - **Quantum Advantage Focus:** Lead by the Chief Analytics Officer and made accountable for the development and realization quantum inspired value-creation strategy.

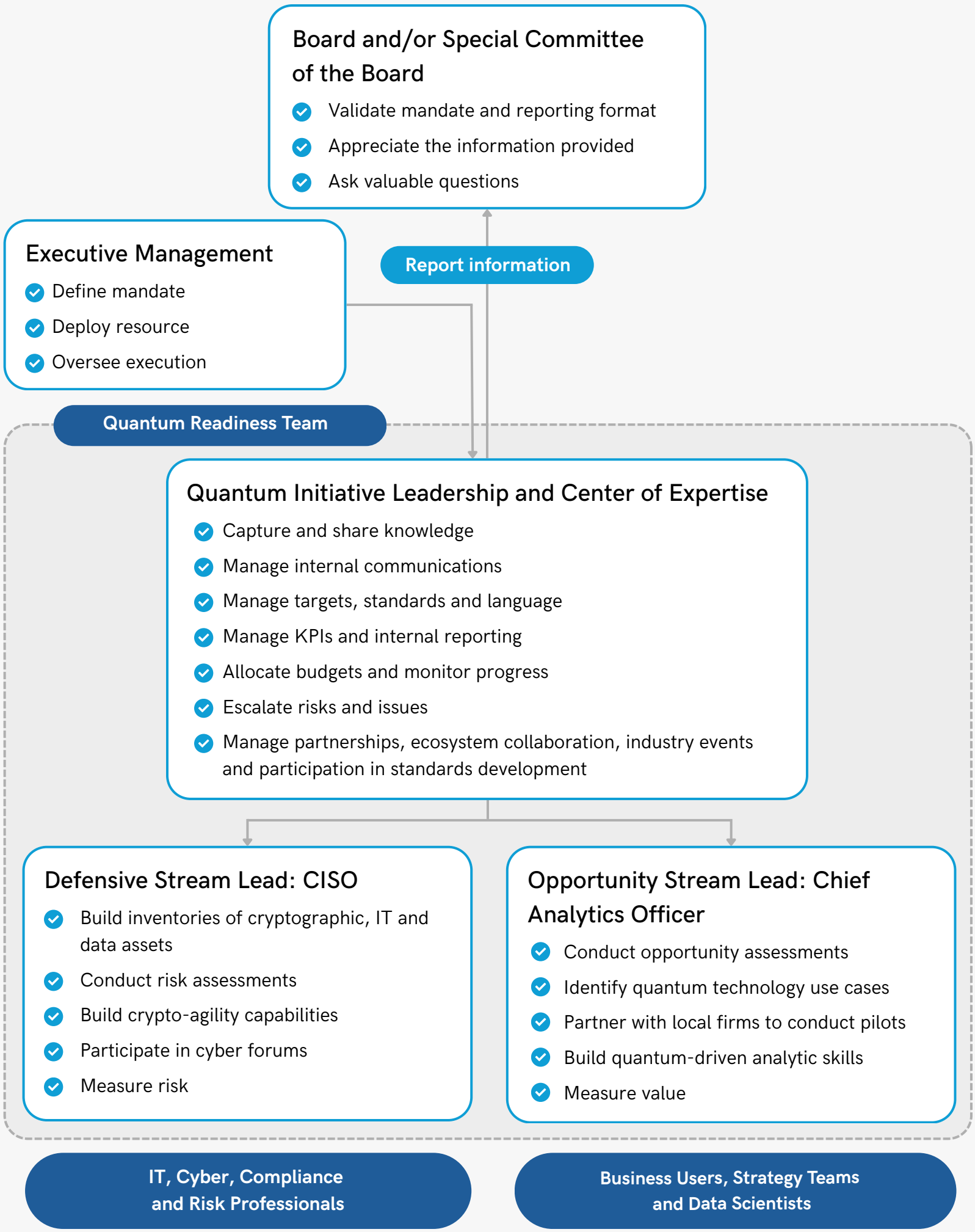
**Do you have people with advanced degrees in physics or mathematics in your organization?** Physicists can help cut through hype and distinguish meaningful quantum progress from noise. They are uniquely positioned to identify and evaluate high-value quantum computing use cases and challenge unrealistic vendor claims. Mathematicians bring deep expertise in cryptography and can help your cybersecurity team assess quantum-resistant security options and transition risks. Together, they help your organization ask the right questions, validate assumptions, and guide executives toward decisions grounded in technical reality rather than marketing promises. Many financial institutions already employ such experts, typically in their Risk Managemegement and Trading functions.

### Why This Is Important

Quantum readiness is not a single initiative but a multidisciplinary transformation. Without a coordinated structure, organizations duplicate effort, miss synergies, and dilute accountability. A Quantum Cell creates coherence and momentum.

## Quantum Readiness Governance Model

Running an effective readiness program requires organization. The following schema illustrates what an effective governance model should look like.



### 4.2.3 Assess Risk Exposure & Opportunity Timelines

#### Commission a high-level risk and opportunity assessment

The purpose is to obtain a first fuzzy picture of what is at stake for your organization specifically.

- Your **risk exposure analysis** should address both cyber threats and market threats, including market disruption and global impacts.
- Your **opportunity assessment** should identify your industry's and your organization's top use cases for quantum computing capabilities.

#### Determine lead time for preparation

Using information provided by your Quantum Readiness Team:

- Determine your target readiness date based on your risk exposure. Organizations with highly confidential long-life assets at a high risk of attack will want to move more aggressively.
- Identify the signals that this is approaching or shifting, and monitor put in place the mechanisms to update it regularly.

### 4.2.4 Define your Defensive Quantum Strategy

#### Align on your defensive intent

Identify which quadrant of the Urgency Compass you want your organization to be positioned on Q-Day.

- Develop a clear discourse on what this means and ensure it is embedded into enterprise risk appetite, strategic priorities, and communication with regulators, investors, and employees.

#### Define your defensive roadmap

It should include two distinct but intersecting delivery streams.

1. **A stream to build crypto-agility in your organization, including.**
   - A capability maturity assessment and capability gaps.
   - Clear actions to build these capabilities and close these gaps, including operating model, skills, capacity, training, process updates and long-term tooling.
2. **A stream to complete your migration to post-quantum cryptography, which includes:**
   - An inventory of where cryptography is used across the enterprise, the complexity and effort associated with the migration of each instance, and the estimated time to completion.
   - An assessment of cryptographic dependencies across external providers and third-party critical infrastructure and a plan to assess their readiness and compliance.
   - How you will phase critical assets by priority (ex: top-tier systems first, then lower-risk ones)?
   - Baseline assumptions, resource requirements and estimated timelines to complete your migration.

### Allocate Budget

- Treat post-quantum cryptography migration not as a one-off project, but as a multi-year capital program and long-term operational need through extended crypto-agility capabilities.
- Include budget categories for cryptographic inventory, migration tools, workforce training, vendor contracts, and independent testing.

#### Why This Is Important

Achieving quantum readiness requires a shared understanding across leadership of what needs to be done, by when, and why. Understanding both exposure (where you are vulnerable) and opportunity (where you can win) is critical to setting realistic priorities and timelines. Having a common target and timeline allows you to align strategy, resources, and accountability around a unified plan of action.

## 4.2.5 Secure External Partners

### Engage guides and key partners

Now is the time to secure external expertise, as the demand will grow rapidly as awareness increases and Q-Day approaches. Look for firms and individuals with IT risk management, cybersecurity, and large-scale digital transformation experience with knowledge and relationships with knowledge of your local ecosystem.

## 4.2.6 Set Policy and Compliance Monitoring

### Update

- **Update Policy** requiring all vendors to provide PQC roadmaps in contracts and RFPs.
- **Update Risk Monitoring:** Add PQC migration milestones into your risk register, audit frameworks, and information technology refresh cycles.
- **Update and ensure alignment with enterprise risk appetite**, including ESG/resilience reporting, and regulatory expectations.

# 4.3 Next 1–2 years: Experimentation and Capability Building

## 4.3.1 Develop Your Quantum Strategy – Strategic Use

- **Identify** priority use cases with clear business relevance and measurable potential.
- **Secure** dedicated funding and resources to ensure continuity and delivery.
- **Establish** a monitoring function to track use case performance
- **Set vision** and boundaries framed by a forward-looking statement (e.g., *By Q-Day, we will be able to…*).

### 4.3.2 Prioritize and Fund Your Strategy

- **Apply** guiding principles to evaluate competing quantum enabled use case opportunities and risks.
- **Select** top priorities (X initiatives) that align with strategic goals and available capacity.

### 4.3.3 Build for the Long Term

**Assess your organization maturity and needs for the quantum era**

- **Identify** your capability requirements and assess your gaps across all dimensions. Including :
  - **Strategic partnerships:** with enterprises, vendors, universities, and industry groups.
  - **Expertise:** clarify which skills must be developed internally and which can be sourced externally.
  - **Governance:** define roles, decision rights, sovereignty considerations, and set KPIs/KRIs.
  - **Data:** ensure secure access, quality, and availability for quantum and hybrid use cases.
  - **People:** recruit and develop talent; design training programs to scale literacy across functions.
  - **Processes:** formalize pipelines for use case selection, risk assessment, and funding approvals.
- **Develop** gap-closing strategies across the following dimensions:
- **Assign** clear accountabilities for each initiative and secure board approval for funding.

## 4.4 Next 3-5 years: Strategic Advantage

The plan starts to thin out in this timeline, as it should. Current and rapidly changing conditions make it hard to see this far out.

However, if you did everything in this plan this far, and you stuck to your principles, you will certainly be better positioned with a future that is brighter than most.

### Key considerations for this period

- Continued close monitoring and support of your post quantum cryptography migration plan
- Leverage the groundwork you put in testing your quantum use cases.
- Look after and protect your talent pool.
- Ongoing nurturing of partner ecosystems and alliances.
- Ongoing industry collaborations and standards shaping.
- Embed quantum advantage in your business model.
- Prepare to measure your ROI and long-term value.
- Capture Lessons Learned from your quantum readiness response.

# 05

## 5.1

# Appendices and Tools

## Glossary of Terms

| Term | Definition |
|---|---|
| **Crypto-Agility** | The capability to rapidly update or replace cryptographic systems as new algorithms, threats, or standards emerge. |
| **Digital Trust** | The confidence that digital interactions and transactions are secure, authentic, and reliable across connected systems. |
| **Fault-Tolerant Quantum Computer** | A fully error-corrected quantum computer capable of performing long and complex calculations reliably, marking the threshold for large-scale commercial use. |
| **Quantum error correcting codes (QECCs)** | Quantum error correction codes protect qubits from noise, interference and state decay, helping quantum computers detect and fix errors to keep information accurate. |
| **Fiduciary Duty** | The obligation of boards and executives to anticipate and mitigate emerging quantum-related risks and opportunities and to protect stakeholder value, data integrity, and public trust. |
| **Harvest Now, Decrypt Later (HNDL)** | A threat model in which encrypted data is stolen today to be decrypted once quantum computers can break existing encryption. |
| **Trust Now, Forge Later (TNFL)** | A related threat scenario where attackers capture authentication data now and later forge valid credentials once cryptography is broken. |
| **Internet of Things (IoT)** | Refers to the network of "every day" physical objects embedded with software and connectivity that enable them to collect, exchange, and act on information over the internet without direct human intervention. |
| **NISQ (Noisy Intermediate-Scale Quantum)** | The current generation of quantum devices with limited qubits and significant error rates—useful for research and experimentation, but not yet for mission-critical applications. |
| **Post-Quantum Cryptography (PQC)** | Cryptographic algorithms designed to resist attacks from quantum computers while remaining compatible with today's digital systems. |
| **Operational Technology (OT)** | OT refers to the connectedness of industrial technology such as found in manufacturing plants, energy grids, rail systems, or water treatment facilities. It typically runs on proprietary networks, but these may not always be fully isolated from the broader Internet. |
| **Public Key Infrastructure (PKI)** | The framework of technologies, policies, and processes that manage digital certificates and encryption keys to secure identities, communications, and transactions. |
| **Q-Day** | The day when quantum computers become powerful enough to break today's public-key encryption, exposing sensitive data and communications worldwide. |
| **Quantum Advantage** | The point at which a quantum computer outperforms the best classical computers for a specific, practical task. |
| **Quantum Capability Maturity** | A measure of how advanced an organization's structures, skills, and governance are in integrating quantum considerations into strategy and operations. |
| **Quantum Cell** | A small, cross-functional team responsible for monitoring quantum developments, assessing impact, and coordinating readiness initiatives. |
| **Quantum Ecosystem** | The network of governments, research institutions, startups, and corporations collaborating to advance quantum science and commercialization. |

| Term | Definition |
|---|---|
| **Quantum Key Distribution** | A method of secure key exchange using quantum physics, where any interception attempt is immediately detectable and fixable. |
| **Quantum Literacy** | The foundational understanding of quantum concepts that is required for leaders to make informed strategic and risk decisions. |
| **Quantum Readiness** | The degree to which an organization understands, prepares for, and is equipped to manage both the risks and opportunities of quantum technologies. |
| **Quantum Sovereignty / Technological Sovereignty** | The ability of a nation or organization to develop, control, and secure critical quantum technologies without dependency on foreign entities. |
| **Quantum Use Case** | A practical application where quantum computing or sensing provides measurable advantage over classical methods. |
| **Quantum-Enhanced AI** | Artificial intelligence systems that leverage quantum algorithms or hardware to accelerate learning, optimization, or problem-solving. |
| **Qubit** | The basic unit of quantum information; unlike a classical bit, a qubit can exist in multiple states simultaneously, enabling massive parallel computation in some cases. |
| **Qubit Architecture** | The physical and engineering design used to build qubits,such as superconducting circuits, trapped ions, or photonic systems, each with distinct performance trade-offs. |
| **Urgency Compass** | A visual framework illustrating how readiness and timing interact—showing the outcomes of acting early versus delaying response. |

## 5.2 Details on Select Concepts Presented in the Document

### 5.2.1 Other Quantum Technologies

Quantum computing is just one class quantum technologies. The following section provides a brief overview of the other two classes.

#### Quantum Sensors

Quantum sensors exploit the fundamental properties of quantum mechanics to detect and measure extremely small changes in physical quantities (time, gravity, temperature, magnetic and electric fields) with a level of precision and sensitivity that classical sensors cannot achieve.
Advanced quantum sensors are already delivering significant benefits across medicine, materials discovery, and even everyday life. By harnessing quantum effects, they enable entirely new ways of observing the world, detecting infinitesimal variations in gravity, electromagnetic fields, temperature, pressure, or motion. Several quantum sensing technology-based products are mature and fully commercialized. For example, quantum gravimeters and accelerometers based on cold-atom interferometry enable ultra-precise navigation and underground resource mapping without GPS. Diamond-based quantum magnetometers can detect tiny magnetic fields generated by electrical activity in the heart or brain, opening the door to new medical diagnostic techniques and breakthroughs in scientific research.

#### Quantum Communications (QKD)

Quantum Key Distribution is a quantum-based technology that uses special hardware and quantum physics principles to securely distribute encryption keys between physical sites. It is considered very secure and not susceptible to being broken by quantum or classical computers. But there are technological roadblocks and no clear path to its widespread adoption as a direct substitute for current encryption methods.
It will be a limited use, complementary cryptographic technology until these barriers can be overcome on an industrial level.

### 5.2.2 Broader Risk Information

#### Loss of opportunity (competitive and mission impact)

| What it is | Why it matters | Signals you are at risk |
|---|---|---|
| Falling behind as peers lock in talent, IP, partners, first access and ready their organization to capitalize on this new technology; missing early wins left with slower learning curves and higher costs later. | Reduced growth, weaker margins, and diminished credibility with customers and investors; harder to recruit and retain top talent. | No executive sponsor, no quantum strategy, no funded pilots, no value-ranked quantum use case backlog; passive stance in standards consortia. |

## Risk of exposure (security and compliance)

### What it is

Direct risks to your organization include exposure of your data assets, increased cyber attacks and fraud. Third party and vendor noncompliance with post-quantum cryptography standards amplifies your risk. Global ecosystem risks include the breakdown of digital trusts that underpin the use of the internet.

### Why it matters

The ability to trust or authenticate a third party underpins every digital act. Impacts include breach of confidentiality, loss of data integrity, loss of digital channels and the ability to transact digitally. At best, this could result in regulatory penalties and downstream litigation. At worst it threatens the integrity of your operations and impacts the global economy and political landscape. Exposure windows will last for years and are already active due to "Harvest now, decrypt/forge later" tactics.

### Signals you are at risk

Management is not able to produce a reliable, detailed inventory of cryptography keys tied to business and IT processes that use them. Vendor and partner contracts do not include clauses that force PQC adoption, no processes are in place to validate your company or vendor compliance. Lack of urgency or mobilization at the global scale. Faster than expected development of fault-tolerant quantum computers.

## Risk of sovereignty (control over critical capability)

### What it is

Strategic dependence on foreign hardware, cloud access, libraries, standards, and scarce talent; data residency and export-control constraints; fragmented or immature domestic quantum ecosystem.

### Why it matters

Loss of bargaining power, higher costs, slower access, and vulnerability to geopolitical shocks. For public sector and regulated finance, this can impair mission delivery and national priorities.

### Signals you are at risk

Single-vendor dependencies; critical IP created under partner terms; no government programs to develop local industries, no local academic programs to educate the workforce; no local research/industry links; unclear data-residency stance, data located outside national boundaries or under licenced with entities subject to foreign access.

### 5.2.3 Types of Qubit Architectures

As previously defined, qubits can take on different forms of physical architecture. Each qubit architecture targets a specific type of quantum phenomenon and is unique in comparison to other architectures.

Understanding qubit architectures is not mandatory, but it will be a major asset for first movers. Particularly since not all assets and competencies built for one qubit architecture are readily transferable to another architecture.

When considering different qubit architectures, think unique hardware, unique talent pools, unique supply chains, and unique software milestones.

For example, from an operational standpoint, superconducting qubits requires advancements in dilution fridges, ion traps require advancements in ultra-high vacuum chambers and photonic qubits require better single-photon emitters/detector. The need for each of these developments being industrial opportunities in-of themselves.

While avoiding the nitty-gritty, it is important to understand that roadmaps will be distinct between architectures, and that comparisons between roadmaps must not be done in a naive fashion.

As with other nascent technologies, once it achieves maturity, these individual architectures will not be of concern to end users and organizations. This being said, understanding the breadth of the architectural landscape will be paramount in establishing a *first-mover* advantage, from supply-chain positioning to talent acquisition. We recommend taking the time to understand each approach and how each player in the ecosystem you seek to target is positioned.

### 5.2.4 Canadian Quantum Computer Providers

| Company Name / Location | Qubit Architecture | Distinctive factors in their approach |
|---|---|---|
| **Nord Quantique** Sherbrooke, QC | Superconducting | Using bosonic modes held in cavities to enable error correcting qubits without requiring physical redundancy. Building fault-tolerant quantum computers that are efficient and useful for a wide variety of applications. |
| **Xanadu** Toronto, ON | Photonic | Using photons as qubits encoded in integrated photonic chips and optical circuits, enabling modular quantum computing with high connectivity and near-room-temperature operation. |
| **D-Wave** Vancouver, BC (now global) | Superconducting | Using a specialized type of quantum computing, called quantum annealing. Using superconducting qubits to find solutions to complex optimization problems by naturally settling into the lowest-energy state. |
| **Anyon** Montreal, QC | Superconducting | Proprietary quantum hardware including modular quantum processors, cryogenic systems, and quantum control electronics using superconducting qubits (similar to IBM or Google's approach) |
| **Photonic, Inc.** Vancouver, BC | Photonic | Quantum computing platform based on silicon spin qubits (“T centers”)that are connected through photonics Their approach combines three key elements: computing (using spin qubits), networking (via photons), and memory. |
| **Open Quantum Design** Waterloo, ON | Trapped ions | Non-for-profit organization committed to radical transparency and full-stack open access, with a Trapped-Ion Architecture as a core technology: Individual ions as qubits, held in place by electromagnetic traps in a vacuum and manipulated with precise lasers. |

## 5.2.5 Internet of Things (IoT)

Internet of Things refers to the network of physical objects, such as devices, sensors, vehicles, and machines that are embedded with software and are able to collect, exchange, and act on information over the internet without direct human intervention.

**Here are some examples of IoT (Internet of Things) applications across different domains:**

### Smart Homes

- Thermostats that automatically adjust temperature (e.g., Nest)
- Smart lighting systems that respond to occupancy or daylight
- Voice-activated assistants like Amazon Echo or Google Home
- Home alarm systems and video recording devices

### Healthcare

- Wearable fitness trackers and smartwatches that monitor heart rate and activity
- Remote patient monitoring devices for chronic conditions
- Smart pill dispensers that track medication adherence

### Transportation

- Connected cars that send diagnostic data and enable predictive maintenance.
- Fleet management systems with real-time GPS tracking and fuel optimization

Each example illustrates how IoT connects our physical and digital worlds, generating data and providing capabilities that improve efficiency, personal safety, and decision-making but that also presents a point of risk if digital trust fails.

## About Operational Technology (OT)

Conceptually similar to IoT, Operational Technology refers to the connectedness of industrial class machines such as found in manufacturing plants, energy grids, rail systems, or water treatment facilities. While Operational Technology often runs on proprietary networks but is not always fully isolated from the broader Internet, leaving them also at risk should digital trust be compromised.

**Examples of Operational Technology include:**

### Industrial / Manufacturing

- Quality control monitoring systems
- Sensors monitoring machinery vibration, temperature, and performance
- Predictive maintenance systems
- Automated inventory and logistics systems

### Agriculture

- Soil and moisture sensors for precision irrigation
- Smart drones for crop health monitoring
- Livestock tracking using connected collars

### Smart Cities

- Connected streetlights
- Waste bins that signal when they're full
- Transportation system monitoring and controls

## 5.2.6 Additional Questions for Leaders to Ask

Once you have established your organizational posture and launched your preliminary response, you may explore the following questions:

- Which long-shelf-life data and certificates do we have that risk be harvested today and decrypted or forged later?
- What are our third-party services, cloud providers, and ecosystem partners' PQC migration plan?
- How would we respond if a quantum "breakthrough" happens earlier than expected?
- How do we build optionality (flexibility, modularity) so we can pivot when quantum capabilities mature?
- What is our tolerance for performance or throughput degradation that may come from PQC transition?
- Do we have a governance structure (steering committees, working groups) for quantum/crypto transition?
- What KPIs or metrics will we use to track quantum readiness (e.g., % systems on PQC, inventory completeness, use cases identified, risk exposure)?
- What regulatory mandates or compliance regimes might require quantum readiness (in our industry or jurisdictions)?
- Are there adjacent or emerging business models that quantum could unlock (e.g., material discovery, logistics, drug design, new financial instruments?)
- What are leading indicators or "trigger events" that will move us from planning to execution?

## Additional Questions for Leaders to Ask

- Are we participating in shaping those standards through industry consortia and working groups?
- Which external partners, supply chains, or third parties may become weak links if they are not quantum ready?
- What competitive or strategic alliances should we form now with academia, government, quantum technology firms to position ourselves advantageously?
- Do we have or can we recruit personnel with quantum science, computing and post-quantum cryptography expertise?
- What training, education, and capacity-building initiatives should we launch now for C-suite, security teams, architecture teams, operations?
- What partnerships with universities, quantum labs, and research institutions can we cultivate?
- How do we foster an innovation culture and allow safe experimentation with quantum or hybrid prototypes?
- What is our risk tolerance for "bleeding-edge" experimentation in quantum?
- Are we proactively aligning with national or regional initiatives to ensure our organization's interests are protected as quantum and AI ecosystems evolve?
- What budgets should be set aside now (R&D, pilots, hardware, consulting)?
- How do we measure cost vs. benefit? Is quantum-safe readiness an insurance cost, an enabler, or a source of differentiation?
- What is our fallback or contingency plan if timelines slip or quantum breakthroughs accelerate unexpectedly?
- More to come…

## 5.2.7 Standards Landscape

Many initiatives related to the development of standards for quantum computing or quantum-risk response are underway. The following is a brief introduction to some of the most important ones from a Canadian-participation perspective.

### A Canadian standards / mirror committees: SCC's mirror for ISO/IEC JTC 3

- The ISO and IEC established a new joint technical committee, ISO/IEC JTC 3 – Quantum Technologies. The scope of this committee includes standardization across the field of quantum technologies, including quantum computing, quantum simulation, quantum sources, detectors, communications, and metrology.
- The Standards Council of Canada (SCC) hosts mirror committees which allow Canadian individuals/organizations to follow and influence international standards. For example, the mirror committee MC-ISO/IEC JTC 3 (Quantum Technologies) is listed on the SCC website. The SCC's mandate includes accrediting Canadian standards-development organizations and representing Canada in ISO/IEC.
- This means Canadian stakeholders (including your organization) can engage in international quantum-standards work via the SCC network.

### B Canadian federal guidance and timelines – Canadian Centre for Cyber Security (Cyber Centre) / Treasury Board of Canada Secretariat (TBS) / Shared Services Canada (SSC)

- The Canadian Cyber Centre has published a "Roadmap for the migration to post-quantum cryptography" for the Government of Canada (GC) non-classified IT systems. Canadian Centre for Cyber Security. It sets concrete milestones: initial departmental migration plan by April 2026; high priority systems by end 2031; remaining systems by end 2035.
- The guidance emphasizes standardized post-quantum cryptography (PQC) and the need for transition planning, governance, vendor assessment, cryptographic inventory. The GC strategy signals national priority for "quantum-safe" transition.

### C The Canadian Forum for Digital Infrastructure Resilience (CFDIR)

- The Canadian Forum for Digital Infrastructure Resilience (CFDIR) is a voluntary, consensus-based and action-oriented public-private collaboration formed to enhance the resilience of the Canadian critical digital infrastructure, resulting in a trusted digital economy for Canadians and a thriving cyber security industry.
- One of the Forum's working groups provide an annual update to their report on Quantum Readiness Best Practices to help Canadian Critical Infrastructure sector stakeholders and others to take actions now, to plan and prepare for how they will transition their digital systems to use new quantum-resistant cryptographic technologies and solutions; and shorten learning curves by offering tangible advice and examples that illustrate "how to" undertake the recommendations made herein, so as to reduce the need for organizations to "start from scratch".

### D International Telecommunication Union (ITU) – Quantum-Key-Distribution / QKD Network Standards

- An example of a published standard: Recommendation ITU-T Y.3800 "Overview on networks supporting quantum key distribution (QKD)" (version 1.1, July 2020).
- This is more specific (quantum communications rather than full quantum computing) but shows quantum-safe / quantum-enabled standardization in the telecom domain.

### Summary Table: Major initiatives and organizations

| Standards/Organization | Focus | Canadian relevance |
|---|---|---|
| **SCC mirror committees** | Canadian participation mechanism in international standards (ex: ISO/IEC JTC 3 Quantum Technologies) | Enables Canadian firms to influence and stay aligned at the global level |
| **Cyber Centre / Government of Canada roadmap for post-quantum cryptography (CCCS)** | National quantum-risk response (cryptography migration) timelines. | Direct Canadian policy and timelines relevant to both public/private sectors |
| **Canadian Forum for Digital Infrastructure Resilience (CFDIR)** | How to prepare for the transition their digital systems to use new quantum-resistant cryptographic technologies | Direct, application ready techniques to accelerate post-quantum migration at the enterprise level. |
| **ITU-T Y.3800 (QKD networks)** | Quantum communications standard (QKD networks) | International standard impacting Canadian communications / crypto infrastructure |

## 5.2.8 Advanced Cryptographic Concepts

While this guidebook is not meant to replace or duplicate the excellent technical literature available on cryptography, the following section provides specific insights for readers with deeper expertise or interest in the subject.

### Random Generation

For several years now, it has been possible to purchase quantum random number generators from multiple manufacturers. These are strongly recommended for any cryptographic application requiring randomness (such as encryption or digital signatures). Unlike software-based pseudo-random generators, quantum devices produce truly unpredictable output, which significantly improves the security and quality of the cryptography deployed.

### Computational Security

All public-key encryption systems, as well as symmetric systems such as AES, share a common weakness: at any moment, a fundamental attack could be discovered that enables all messages encrypted with that system to be decrypted. This is essentially what happened with Shor's algorithm; fortunately, quantum computers did not yet exist when it was published imagine the damage otherwise. This highlights the importance of caution when using these encryption systems.

### Two-key Public Key Encryption

For highly sensitive information, it may be prudent to use two different public-key encryption systems to transmit the symmetric encryption keys. This allows you to secure the keys using the stronger of the two systems; if one is broken tomorrow, the keys will remain confidential as long as the second system is still secure. The trade-off is messages (key encapsulation messages, KEMs) that are twice as large. (It is highly unlikely that both CRYSTALS-KYBER and HQC would be broken at the same time.)

## 5.3 Supplements to this Guide

If you found this guide useful, you may be interested in the following supplement and companion guides which we are in the process of developing.

1. Post Quantum Cryptography migration Work Units, Risk and Advancement Measures
2. Quantum Capability Maturity Model and Assessment Templates
3. Quantum Risk Assessment Template
4. Quantum Readiness Monitoring-Executive Reporting Template
5. Quantum Use Case Identification Guide and Feasibility Assessment Guide

## 5.5 References and Continued Learning

| Source and Link | Overview of the Content |
|---|---|
| **Strategy & Industry Perspectives** | |
| **World Economic Forum: Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders"** | Explores how financial leaders can leverage quantum innovation responsibly while managing risk, compliance, and trust. |
| **WEF Quantum Industry Initiative** | Explores how quantum computing can be leveraged by other industries (see above for Finance.) |
| **Canadian Quantum Positioning** | |
| **Quantum Computing & Quantum Technology Initiatives in Canada** | The history of Canada's quantum computing ecosystem and analysis of national positioning (from 2024 but still very pertinent). |
| **National Quantum Strategy roadmap: Quantum computing** | The Government of Canada National Quantum Strategy (NQS) |
| **Natural Sciences and Engineering Research Council of Canada - Impact Analysis - Quantum Edition** | A look at the people, research and innovations that make Canada a world leader in quantum research: academia, industry, quantum science, cybersecurity, and next-generation communication systems. |
| **Quantum industries Canada** | Quantum Industry Canada (QIC) is the country's business-led consortium whose mission is to translate Canada's quantum capabilities and strengths into global business success and national prosperity. |
| **Quantum Technologies & Market Landscape** | |
| **The Quantum Insider – "Top Quantum Computing Companies (2025)"** | Profiles the leading global quantum companies and startups, including major Canadian players. |
| **The Quantum Index** | A global database tracking quantum startup, investors, research hubs, and partnerships across the emerging ecosystem. |
| **Quantum Risk & Cybersecurity** | |
| **An Interview with a Canadian Cryptography Pioneer by Kyle Briggs** | Highlights Canada's pioneering role in cryptographic research and the strategic importance of post-quantum readiness. |
| **Best Practices for Quantum Readiness** | Written by the Quantum Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR). it provides bes practices for quantum readiness and post-quantum cryptography migration, including detailed uses cases |
| **Quantum-readiness for the financial system: a roadmap** | An excellent overview on cryptography as a whole as well as concrete steps global alignment of banking institutions published by the Bank of International Settlements. |
| **Global Risk Institute – "A Methodology for Quantum Risk Assessment"** | Provides a structured framework for assessing quantum-related risks in financial institutions, emphasizing crypto-agility and fiduciary accountability. |
| **Post Quantum Cryptography (PQC) Building Cryptographic Agility in the Financial Sector** | Written by the FS-ISAC Post Quantum Cryptography Working Group, it explains crypto agility detail and provides guidance and advice to become crypto agile. |
| **Post-Quantum – "Practical Steps to Quantum Readiness"** | Outlines pragmatic migration and resilience strategies for organizations preparing for post-quantum cryptography. |

# 06 Acknowledgments

## "Thought Leaders & Endorsers" whose voices elevate the reach of this book.

This guidebook was shaped by the insight and conviction of leaders who recognize the urgency of preparing organizations for the quantum era. Their perspectives, guidance, and belief in this work were fundamental to its clarity, credibility, and reach.

**Claude Crépeau**
**Professor, Department of Software Engineering and IT, École de technologie supérieure - ÉTS Montréal**

*"This guide is the must read introduction everyone concerned with securing transactions. Scientifically accurate, it bridges the gap between academia and the financial world."*

**Marc Frappier, Ph.D., professeur**
**Research Chair in Post-Quantum Cybersecurity, Scientific Director of the Intact Cybersecurity Expertise Center, Université de Sherbrooke**

*"Becoming quantum safe is a strategic goal that organisations need to consider now. This guide will help executives and board members to start planning for the transition to post-quantum cryptography. This is a major overhaul that will need careful planning and coordination, because cryptography is a critical component of any IT asset."*

**Joni Brennan**
**President, Digital ID & Authentication Council of Canada (DIACC).**

*"Quantum How is timely and relevant. It explains what's at stake for digital trust and identity verification in the quantum era and provides a clear path to protect the trust Canadians rely on."*

**Christian Sarra-Bournet, PhD**
**Directeur Exécutif de l'Institut quantique de l'Université de Sherbrooke**

*"I support this initiative because decision-makers and leaders in large organizations must recognize the urgency: inaction in the face of quantum cryptographic threats could compromise the very integrity of our critical infrastructure, while also causing them to miss the opportunity to secure a competitive advantage in their respective sectors."*

**Anne-Marie Hubert**
**Senior Fellow CIRANO, Chair of the Canadian Chapter or the Human Technology Foundation**

*"The opportunity to join an ecosystem where government, investors, scientists and businesses work together to leverage the Canadian leadership advantage to solve some of the most complex problems of our time and drive real ROI for business and sustainable growth for Canadians is now. An opportunity we must capture."*

**Charles Morgan**
**Member of Advisor Board (Past President), International Technology Law Association (iTechLaw), Board Member of the Canadian Chapter or the Human Technology Foundation**

*"Quantum computing represents the next-generation of disruptive technologies, with the potential to be a game-changer. This guide brings into focus many of the key factors that corporate boards must begin to consider when overseeing corporate response to the risks and opportunities of quantum computing."*

**Suzanne Gouin**
**Chair of the Board of Managment of the Canada Revenue Agency, Member of the board of the Laurentian Bank and Polykar**

*"As boards, it is essential to recognize that quantum computing will soon revolutionize our relationship with technology. This book serves as a wake-up call for boards to grasp what is at stake, understand the technology and the time- line and prepare to tackle this emerging challenge and seize new opportunities."*

# Expert Reviewers & Advisors

## Ensuring accuracy, depth, and clarity

These individuals contributed their time, expertise, and critical feedback to review and improve the content. Their thoughtful comments strengthened the rigor and practical relevance of the guidebook.

- **Martin Laforest:** Managing Partner, Quantacet, VC and Quantum Tech Incubation
- **Marin Ivezic:** CEO Applied Quantum, Emerging Technologies Risks Researcher & Author*
- **Bruno Couillard:** Crypto4A, CEO, Quantum Cryptography Technology Leader
- **Kit Dalaroy:** President, Dalaroy Conseil, Strategic Growth Advisor
- **Nicolas Tran:** Subject Matter Expert - Financial Services Operational Risk
- **Alexis Arévalo:** Executive Perspective - Quantum-Banking Synergies

# Writing & Production

## The hands and hearts behind the words.

My heartfelt thanks to **Valérie Boissonault**, whose early conviction was the catalyst for this initiative; to **Anne-Marie Hubert**, whose drive and support propelled it forward; to **Christian Sarra-Bournet** for his thoughtful guidance throughout; and to **my son**, whose clarity, questions, and edits helped shape ideas into their strongest form.

Finally, "hats off" to **Laura Poulin**, Founder, Laura Childs Art for her incredible design work.

# About the Author

### Louise Davey, Founder of LDIQ

Louise Davey is a **Business Transformation Architect and Leader** with **30+ years of executive and advisory experience**. She helps public and private institutions develop new capabilities, increase operational agility, strengthen corporate governance, manage risk and develop resilence through the thoughtful adoption of advanced technologies.

A former **CTO and COO, MSc in Physics** from McGill, **Board Director and IT Committee Leader**, Louise is able to translate complex technological concepts (data, cybersecurity, AI, quantum) into measurable business outcomes, risk, resilience, and agility.

Most recently, Louise's work focuses on converting quantum and cryptography complexity into **decision-ready, actionable information** translating post-quantum risk and opportunity into terms such fiduciary **duty, business impact, and actionable next steps** to empower leaders to take action.

* Extra recognition goes to Marin Ivezic for the quality, clarity and generosity of his many publications (www.postquantum.com).

Please help promote the circulation of this guidebook by engaging in the dicussion on LinkedIn

You can share your feedback directly here: ldiq.ca