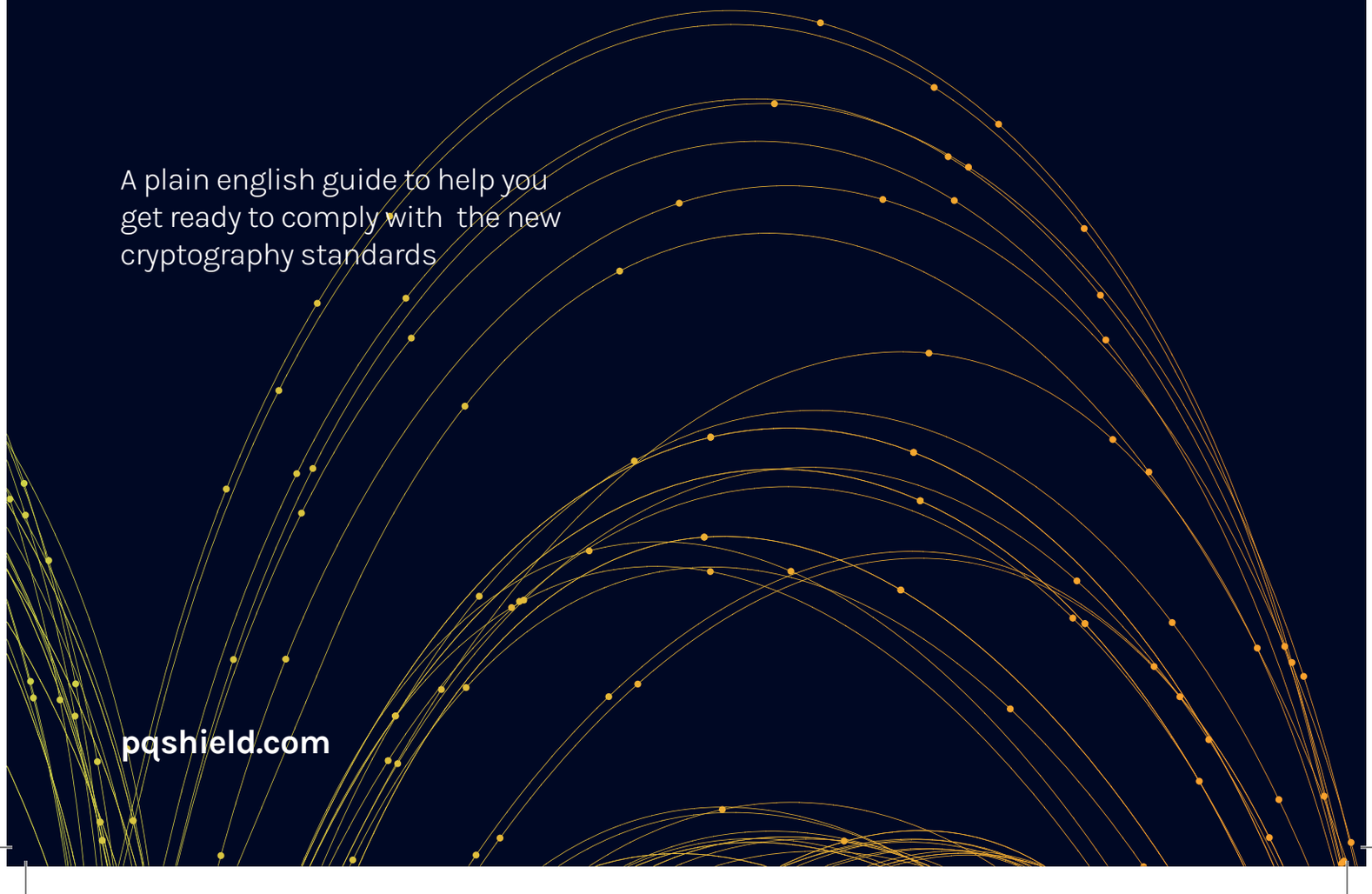
PQ SHIELD

Cryptography Modernization Part 1:

Where is your cryptography?

A plain english guide to help you get ready to comply with the new cryptography standards



pqshield.com

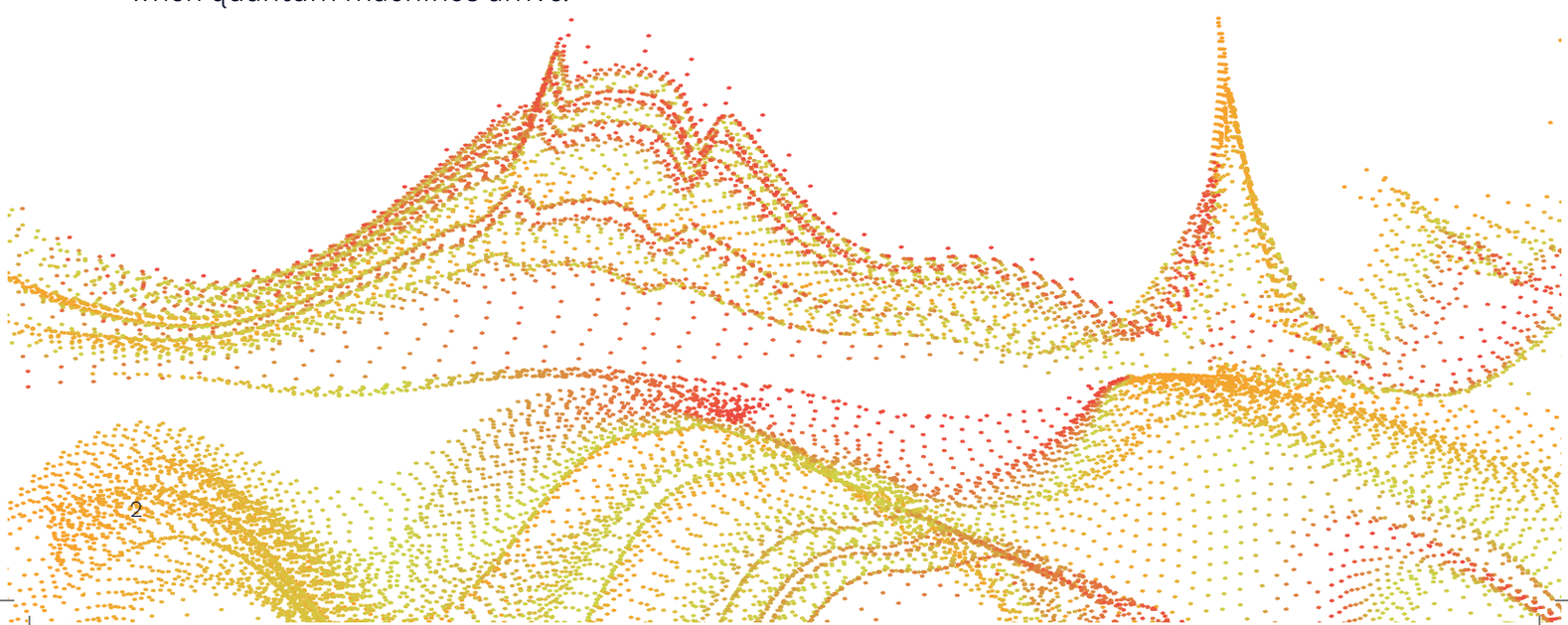
Foreword

We all know that strong encryption underpins the security of the digital world and is a key enabler of global commerce. Without it, most organizations would not be able to function. But because cryptography is a complex subject there is a natural tendency to see it as a long term risk, best left to deep mathematical experts and governments. That is no longer a viable approach.

The development of quantum computers, which are likely to be available over the next decade, means that every organization should now be giving this urgent attention. The US administration, in its recently published National Cybersecurity Strategy, set as a strategic objective the introduction of quantum-safe cryptography to public networks.

The strategy called on the private sector to “follow the government’s model in preparing its own networks and systems for our post-quantum future”. It seems likely that governments will increasingly demand quantum-safe encryption in their own supply chains and in critical sectors of the economy.

Put simply, as this white paper explains, quantum computing has the potential to make the encryption we most commonly use to protect our data, devices and systems ineffective. It could reduce the time taken to break common encryption from thousands of years of computing power on classical machines, to days or even hours on a quantum computer. And this is not only a future threat: it will also be applied retrospectively. Data encrypted now will be readable when quantum machines arrive.



PQ SHIELD

The good news is that governments, private sector experts and academics have been working for some years to develop encryption that can withstand quantum computing power. These quantum-safe cryptographic standards are now available. The challenge for all organizations is to work out the risks they are carrying through their current encryption and how best to move towards encryption which uses the new standards.

This white paper sets out a very practical approach to understanding and assessing the risks an organization is carrying and a pathway to mitigating the threat. It has the great advantage of being written by some of the experts who have helped to shape the quantum-safe encryption standards which governments will be rolling out. But it also reflects the authors' real-world, practical experience of applying the new standards in diverse companies across a wide range of sectors. In an area where it is often difficult to know where to start, this is an excellent and authoritative guide.

Robert Hannigan,
CyberSecurity Adviser; former Director GCHQ who established the UK National Cyber Security Centre

Introduction

Quantum computing poses a significant threat to many traditional cryptographic systems. The cryptography that's keeping your organization safe today could easily be redundant tomorrow.

This urgency has included a focus on creating international PQC standards, as well as strategic plans for migration of legacy systems, mandated by governments around the world. For example, the White House released memorandum M-23-02 as part of the National Cybersecurity Strategy, outlining a roadmap to resilience. ANSII in France have focused heavily on PQC transition in their recent series of papers, and organizations such as the NCSC in the UK, and BSI in Germany, have recently published updated recommendations for action.

With the ongoing development of these new standards, it's clear that compliance, compatibility and interoperability of cryptography and PQC are also becoming major issues for business continuity.

Typically, the strategy for PQC migration should include:

- **Preparing an inventory, and risk assessment of systems that use cryptography**
- **Prioritizing the inventory - which systems will you migrate first?**
- **Assessing the funding required**

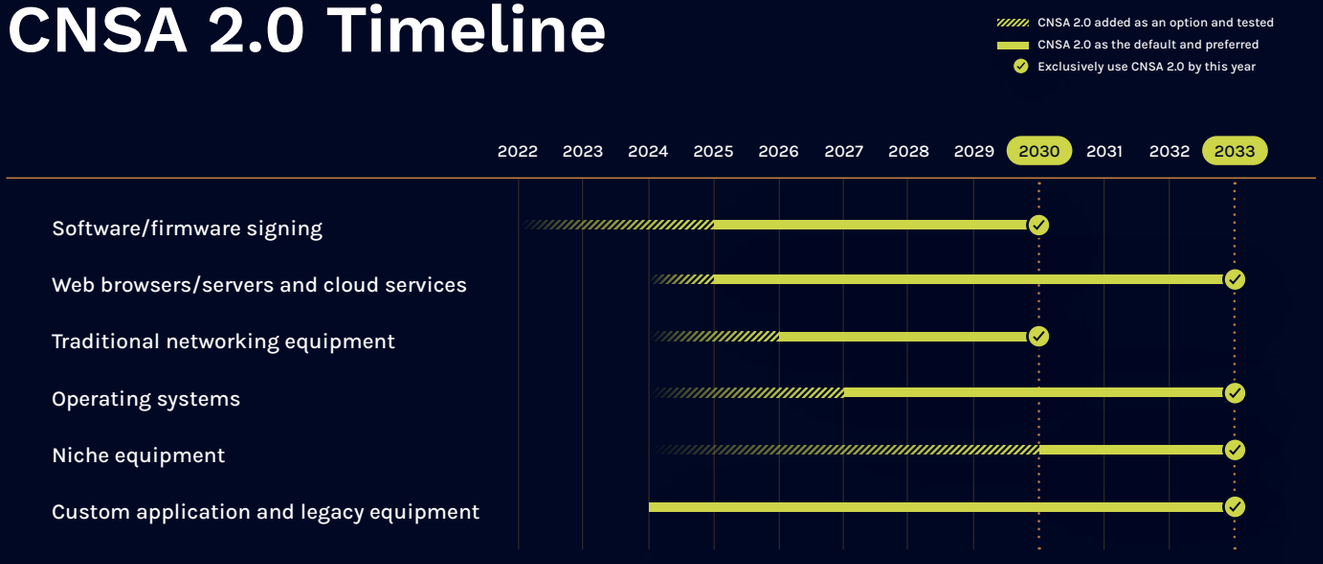
Legislation in many countries now recommends that the private sector follows the same model in preparing its own networks for quantum resistance, and alignment with the new PQC standards.

Your organization will need to comply, and soon.

For example, CNSA 2.0 (released by the NSA to recommend including the use of PQC), highlights that frameworks supporting PQC should be deployed by default in the following systems:

- **Software signing and firmware signing, by 2025**
- **Web browsers/servers and cloud services, by 2025**
- **Networking, by 2026**
- **Operating systems, by 2027**
- **Niche systems, by 2030**
- **All systems, by 2033**

CNSA 2.0 Timeline



Unfortunately, there is no way to predict the moment when quantum computing becomes a real-world threat. The message for organizations is both clear and urgent: the time to start preparing for migration to PQC is now, and that preparation involves assessing and prioritizing an inventory of systems that use cryptography, and are candidates for migration.

Prioritization matters because replacing traditional algorithms with quantum-safe alternatives is not necessarily an easy task, as PQC has differing demands for power, storage, and bandwidth, which might clash with legacy protocols or latency requirements.

But where do we begin? For many of us, the project could be a daunting prospect. In fact, the task of migrating to quantum-safe encryption is now being described as ‘crypto modernization’ to reflect just how complex a process this is.

In this article, we look at some of the areas you need to think about, whether your organization is involved in critical national security, or your data and intellectual property is too important to be put at risk of a future attack. For example, the telecom industry has already started assessing the impact of PQC migration, as have many others. You can find out more about this specific example in the GSMA Post-Quantum Telco Network Impact Assessment whitepaper.

PQShield has been at the forefront of the effort towards quantum-resistance, developing technology that will be used for decades to come, as well as contributing to the development of the standards that define how quantum-resistance is established.

Where to Start

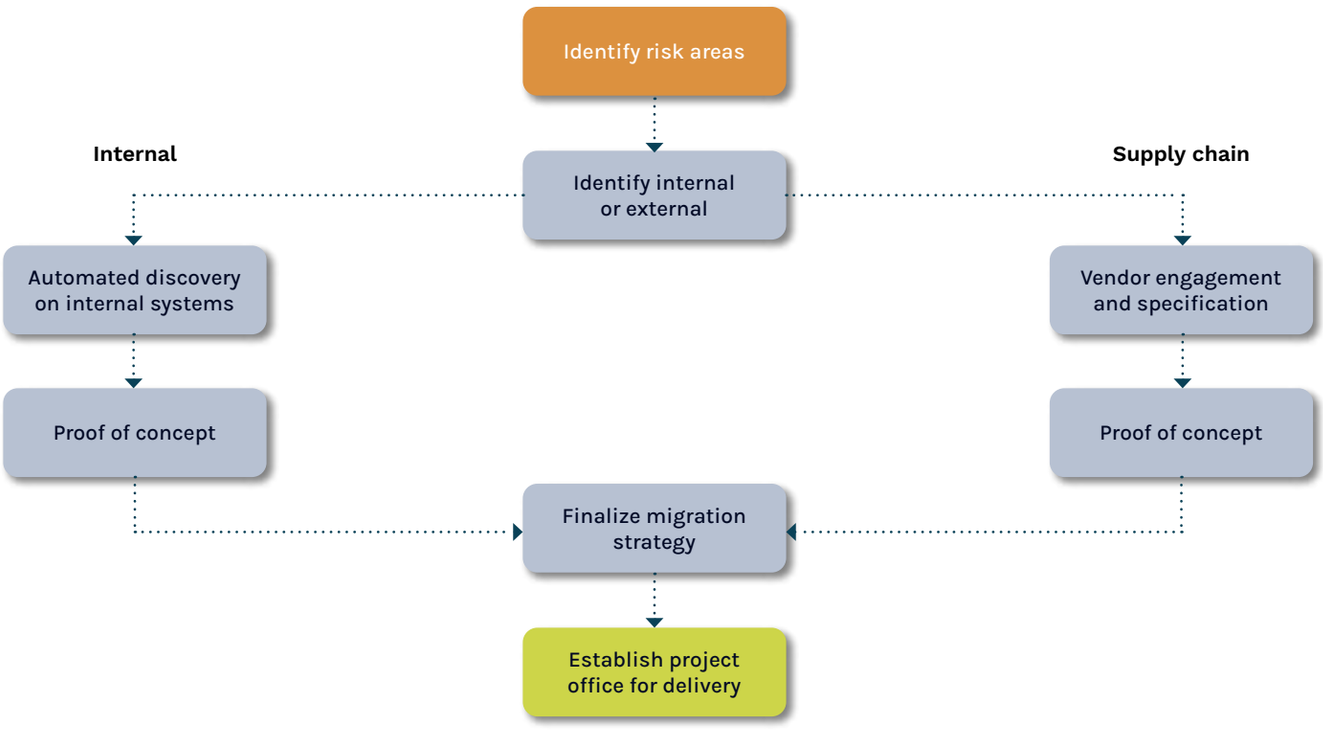
You need to know where cryptography is being used in your organization.

It's important to think about not only what's in use to protect your data now, but also how to handle systems, services and products that will form a legacy, even in five to ten years' time.

Additionally, you'll need to think about how your roadmap includes the adoption of quantum-safe technology, even if the systems in question can't immediately be fully replaced.

A great first step might be to interview your internal system owners and experts. This will help you understand which vendors and suppliers you need to talk to about PQC, and also ensures that your business is fully aware of the need to migrate.

The following diagram shows an outline of how you might want to proceed.



Identifying Risk Areas

Essentially, you need to think about the nature of your data, where and how it's stored, and how it's communicated into, out of, and through your organization.

In this section, we're going to look at some of the strategic areas of operation we think it's important to focus on when considering migration to PQC.

For example, your communications network is likely to be a high priority as it's a prominent target for attackers. Additionally, your databases, storage, cloud provisioning and authentication services will need particular focus as part of your infrastructure.

In addition to identifying systems that contain cryptography, you should also consider:

- **The sensitivity of data being handled by these systems - how is your data classified?**
- **For how long that data is expected to remain sensitive**
- **Whether a system is public-facing**

All of this information can then be used to build a first-draft prioritized list of systems to migrate.

You will need to think about which vendors and suppliers you need to talk to, and which questions to ask them in relation to the cryptographic methods used in their products. This, along with your internal systems, should give you a list of prioritized candidates for migration.

Once this first-pass prioritized list has been compiled, a second round can be passed on the top candidates, to collect any additional information and make determinations about which pilot projects make the most sense.

Even systems that are not top candidates after the second round should become discussion tasks with suppliers of those systems to understand and track the supplier's timeline for migration to PQC.

In Industry-Specific Considerations, we're also going to consider specific industry sectors, and how PQC might impact them. You can find out more below.

- Medtech/healthcare
- Financial services
- Regulatory technology
- Embedded Systems and Manufacturing
- Defense and CNI
- Retail
- Telecommunications
- Logistics
- Media

Your Infrastructure

Your organization's central infrastructure consists of multiple components that are essential to the way you connect machines, users, sites, and data. When it comes to thinking about security, your network, database, and access management systems will almost certainly be a high priority.

Infrastructure components form the basis for using cryptography in other applications, providing security for traffic through networks, data resting in databases and federated identity management providing access to those applications. In many cases, infrastructure security (and its underlying cryptography) are a first line of defense in protecting other systems (defense in depth). Updating infrastructure will convey some level of protection against quantum attacks for applications and systems that are supported by the infrastructure.

Many of the infrastructure components will need to be updated early, to support a hybrid of PQC alongside legacy cryptography. This hybrid solution enables migration of applications that are dependent on PQC, while still supporting components that are yet to migrate.

Area	System	Implications and Questions
Network	Routers	Does your router support a PQC VPN? VPNs use cryptography. Any device with firmware signing will also need to be considered.
	Switches (management)	Firmware signing needs consideration.
	Network access	Cryptography is often used to access networks. Do you have PQC-ready machine identities?
	Zero trust access	Machine identities/certificate identities.
	WiFi access	Access control/access points, wpa2 uses a shared password and EAP protocol potentially uses firmware at access points.
	Application delivery controllers	Do the controllers support PQC-ready TLS?
	Firewalls/WAF	Requires PQC-ready TLS, PQC-ready VPNs.
Database	Access	Does your database support PQC-ready identities?
	Data encryption	Is the database key management and encryption of your data PQC-ready?
Identity	User identity	Are my user credentials/secure identification processes (2FA, etc) ready to support PQC?
	Machine identity	Certificates are used to verify machine identities.
	PKI	Can my PKI (public key infrastructure) issue both PQC-certificates and hybrid certificates?
	SSO options	Does Single Sign-On work with PQC credentials?
	Signing solutions	Docusign, PandaDoc, and other digital document signing tools need to be considered. This is likely to be a discussion with an external supplier.

Area	System	Implications and Questions
Security	Code signing	Does my code-signing process support PQC certificates?
	Container signing	Does my container-signing process support PQC certificates?
	Software BoM	SBOMs (Software Bill of Materials) are nested inventories that help defend against an attack on a software supply chain. SBOMs use signatures that need to be PQC-ready.
	Key management	Does my key management solution support PQC keys?
	Security analytics/IDP	These solutions need to be able to decrypt traffic, and therefore need to support PQC certificates, TLS, etc.
	Privileged access management	Storage of encrypted credentials - identities and SSH keys need to be PQC-ready.
	Secrets management	Similar to privileged access management but for programs/applications using hashed, for example 'secret' keys. These identities must be PQC-ready.
Storage (network/cloud)	Data at rest protection	NAS/cloud storage can be encrypted and so asymmetric keys used for storage need to be PQC-ready.
	Data access	User credentials when accessing stored data (NAS, etc.) must be PQC-ready.
	Digital rights management (DRM)	Credentials are required for file protection and for recipients downloading or streaming the file, and both must be PQC-ready.
Cloud	Multi-cloud key management	Multiple cloud service providers might require common encryption keys that are generated independently of those clouds. These keys need to support PQC. Does the management tool support the use of PQC-ready cryptography for transportation?

Operational Tech

Organizations often have a combination of hardware and software in operational use, such as manufacturing controls, security systems, building controllers and graphical user interfaces. Often, these systems help run day-to-day operations.

Operational tech has become a significant target for attackers. Understanding what cryptographic methods are deployed in these systems, and the associated risk, will enable you to prioritize updates and begin working with suppliers early.

Area	System	Implications and Questions
SCADA systems	Secure boot	Are you using PQC-ready signatures for secure boot?
	Secure update	Secure updates will also require PQC-ready signatures.
	Data protection	Traffic of data between systems/controllers uses TLS, which will need to be PQC-ready.
Physical securit systems	Cameras/ devices	Traffic of data between devices/controllers uses TLS, which will need to be PQC-ready.
	Physical access controls	Traffic uses TLS - needs to be PQC-ready.
	Building control systems	Traffic between secure systems such as eco controls uses TLS which must be PQC-ready.
	Fire control systems	Traffic between control systems uses TLS which must be PQC-ready.

Communications

Communications have always been a key target because they can be a relatively easy way to gain access to sensitive information or networks. A secure communication channel is the first line of defense, protecting many other systems from interception, and is therefore a high priority when migrating to PQC.

Area	System	Implications and Questions
Secure messaging	Secure boot	Depending on the solution, you need to check the way your secure messaging tool uses encryption. For example, some will use TLS, while some have more complex ways of encrypting traffic. Check the authenticity of the solution, and that the encryption method being used has a path to PQC-readiness.
VPN	Identity	Are your user credentials PQC-ready?
	Channel encryption	Does the channel encryption specifically use PQC?
Email	Secure SMTP	S/SMTP uses TLS - you need to check that the implementation supports PQC (sendmail).
	Secure IMAP	S/IMAP uses TLS - you need to check that the implementation supports PQC (mailbox).
	E2E message encryption S/MIME	Uses certificates that will need to support PQC.
	Message signing	Uses certificates that will need to support PQC.
Remote desktop	SSH	Identity and encryption for SSH. Does your SSH implementation support PQC-ready credentials and encryption?

Area	System	Implications and Questions
	RDP	Does your RDP implementation support PQC for encryption?
	Web based	Is the TLS PQC-ready?
Virtual conferencing		For example, Zoom, Google Meet, Teams. Check support of PQC-ready protocols such as TLS.
Voice comms		For example, Skype, VOIP. Check support of PQC-ready protocols such as TLS.

Applications

In addition to connectivity, network and site management, there will also be a number of business specific tools in use that you will need to consider in your inventory. Many of these are likely to be supplied by a third-party, and so the PQC conversation will involve contacting vendors to determine risks, priorities, and a timeline.

Industry-specific Considerations

When thinking about your infrastructure and prioritizing your systems, the chances are, your needs will depend on the industry your organization operates in.

The following considerations are not exhaustive, but they might help you think through which systems are used, who you need to involve in the conversation, and which suppliers you need to contact.

Medtech/Healthcare

Cyber attacks are already a significant risk for healthcare companies and providers of medical equipment. Even with today's technology, security incidents pose a threat, not just to business operations, sensitive data and devices, but also to patients themselves, whose lives may be put at risk.

Responding to these challenges requires not only the implementation of robust security measures to protect from today's risks, but to protect from future attacks too. Healthcare records have a long period in which they remain protected under law, and data stolen today could easily be decrypted sometime in the future, potentially while still protected by those laws.

That's why planning migration to PQC needs to be taken seriously.

Area	Description	Considerations
EMR	Electronic Medical Records are shared securely between multiple points and involve the storage and transfer of personally identifiable information (PII)	How much difficulty would it cause if all your patients' PII or Private Health Information (PHI) data was suddenly at risk? To ensure continued data security today and in the future, you will need to consider how EMR data is stored and exchanged across systems.
Billing and payment processing	Secure data is shared between multiple systems	There are severe consequences for organizations when Payment Card Industry (PCI) data is put at risk. How is your customer payment and billing information stored and managed? How is it exchanged between systems?
Prescription issuing	Personal data is shared between multiple systems and practitioners	Prescription data needs to be stored in and exchanged across multiple sites, for example pharmacies, hospitals, surgeries. What would be the impact of patient data being intercepted or copied as part of an external attack?
Patient monitoring	Sensitive data is shared, potentially between on-site and remote devices or practitioners	Remote health-monitoring devices such as insulin pumps, pacemakers and medical implants can transmit data to a system, and are currently protected by lightweight security protocols. It is important to consider devices with extended life, as many of these will outlive the technology used to keep them secure.

Pharmaceuticals

Area	Description	Considerations
Supply chain communica-tions	Ordering, payment, scheduling, involving storage and transfer of Personally Identifiable Information (PII), sensitive and financial data	Which vendors and suppliers are you using? Which companies are you supplying to? Make sure your connections and processes in your supply chain are secure in order to protect your data, equipment, accounting, and Intellectual Property (IP).
Controlled substance handling	Secure data, physical controllers such as ecosystem regulators and devices	Safety will certainly depend on how secure these systems are, and you should consider how protected they are from malicious interception. Consider protection against digital signature forgery to prevent criminal ordering of controlled substances.
Patient trial data systems	Storage of PII, transfer of sensitive information between networks	What is the process/lifecycle for managing personalised data from patients? How is the information managed between systems? What would be the impact if this data was stolen or manipulated?
Laboratory systems	Physical controls, machines and user identities	Laboratory systems are likely to depend on authentication of users and machines, as well as secure communication of critical data between machines, users, and networks. Lab results are also considered PII and need to be protected at every step of the process.

Financial Services (Fintech)

Fintech has evolved considerably over the last few years, transforming the way payments are managed and processed. Much of this transformation has been due to the advent of blockchain – a digital ledger that stores data in encrypted blocks.

Blockchain uses asymmetric encryption – a type of security that could potentially be deciphered in minutes, if not seconds, by a quantum computer. Consequently, the financial services industry is vulnerable in the post-quantum world. Coupled with the fact that financial institutions experience significantly more cyber attacks than other organizations, security for the post-quantum era is an imperative.

Area	Description	Considerations
Accounting/ auditing	Secure financial data is stored and shared between systems	What would happen if a competitor could access your audited data? What would happen if a criminal could move money between accounts? Security is essential for any platform that relies heavily on data, and there could be devastating consequences in a major attack.
Authentication/ online banking	Access data, sensitive Personally Identifiable Information (PII) is stored and managed by a number of secure systems	Current methods of authentication could easily be bypassed by a quantum computer, and require protection by post-quantum cryptographic methods. What would be the impact to your business if customers were no longer able to access their accounts securely?

Insurance Technology (Insurtech)

Technological innovations are reinventing insurance. These digital technologies bring new efficiencies and enable far better data traceability, management and privacy. Blockchain, meanwhile, is leveraged to allow processes such as claims and fraud management to be decentralized, keeping customer and insurance data protected.

Quantum computing has the potential to turn this digital-first sector on its head. Without adequate protection using PQC, the data that is used to digitize transactions, improve underwriting decisions and speed processes, is under threat.

Area	Description	Considerations
Online application software	Transfer and storage of Personally Identifiable Information (PII) typically managed with public key infrastructure	Customers reveal personal information in applying online for insurance. That information could have a long shelf-life and could be used in multiple different ways - putting it at risk from future decryption by a quantum computer.
Contract management systems	Contract portfolio data is commercially sensitive and stored securely	Today's leading contract management solutions encrypt data and ensure privacy. However, this encryption would not stand up to a quantum attack.
Data analysis platforms	Storage of a large amount of customer data for analysis	Any company using customer data has an ethical and legal responsibility to keep it safe. A data analytics program must be quantum secure.

Regulatory Technology (Regtech)

An increasing number of firms are turning to regtech – solutions that use AI, ML and other advanced technologies to automate a whole host of regulatory functions. Not only can businesses meet their regulatory reporting requirements more effectively, but they can also achieve more efficient risk management, identity management, compliance and transaction monitoring.

However, while regtech is meant to provide an organization with more security, failing to prepare for a post-quantum world could have the opposite effect. That's because today's regtech platforms have not been designed with tomorrow's threats in mind. Quantum computing threatens to break the encryption that currently underpins interactions in regtech platforms.

With all this in mind, it's essential to implement PQC that can keep pace with the growing regulatory complexity of today, and also protect against the quantum threats of the future.

Area	Description	Considerations
Contract management systems	Contract portfolio data is commercially sensitive and stored securely	Today's leading contract management solutions encrypt data and ensure privacy. However, this encryption would not stand up to a quantum attack.
ERP	Enterprise Resource Planning - inventory management, performance metrics, sales quoting, scenario planning	Highly sensitive data about your company is stored in this collateral. What would be the impact if it were leaked or altered? Potentially an attacker could add false information to the system.
Accounts Systems	Payment processing, order fulfillment	Regtech solutions connect to account management to help monitor transactions, but this could become a pathway for an attacker to leverage, accessing or manipulating your highly sensitive commercial information.

Embedded Systems and Manufacturing

Quantum-readiness in hardware usually begins with the original equipment manufacturer (OEM). These products, chips and devices can be long-lasting - for example, today's vehicles could still be on the road in twenty years' time, and are essential to many products across multiple industries.

The increased connectivity of OEM and industrial products leads to the inescapable fact that safety depends heavily on the security design choices of the manufacturing process and tools, as well as the underlying security software and hardware that's embedded in end products.

In manufacturing, durability, compliance with standards, and quality, are correlated, and they can also be distinguishing factors between leading OEMs. Long-lifecycle products not only need to comply with current cryptography standards, but also with upcoming ones. This is where PQC solutions can play a major role. However, several engineering challenges arise.

PQC algorithms work in different ways to classical cryptography and thus have larger key sizes, longer signatures and require more memory, so could easily clash with the limited resources (memory, bandwidth, computing power) embedded legacy systems provide. Many industrial protocols, for example CAN bus, might not be ready to deal with these larger parameters and may need to be updated. The required PQC changes to infrastructure are all part of the new concept of 'crypto modernization'.

Automotive

Area	Description	Considerations
In-vehicle secure boot/ updates	Software uploaded to a vehicle from a network	What would happen if someone had access to all the information on your connected device? Secure boot ensures that only valid security can run, and prevents malicious actors from intercepting the device. With the advent of automated driving, and the potential for more dependence on in-vehicle systems, it's important to make sure this process is secure.

Area	Description	Considerations
Vehicle communica-tions	Communication between remote points and network, or communications between vehicles	Secure communication across the Internet requires confidence that end-to-end encryption cannot be intercepted, or allow messages to be modified. In vehicles, an attack could interfere not only with sensitive data but also the safety and operation of the vehicle itself.
Service systems	Diagnostics, downloads, connection from a vehicle to network	It will be increasingly important to consider how to protect stored diagnostics as well as the connection between vehicles and networks.

Manufacturing

Area	Description	Considerations
Production planning, floor IT and floor control systems	Secure data/IP shared between multiple points and networks	Automated assembly lines, plant floor safety, IP, physical assets and processes all depend on secure transfer of information and large amounts of data transferred between multiple systems. It will be increasingly important to think how your assets are secure in the post-quantum era, particularly as they are likely to be dependent on long-lasting, expensive or critical systems and equipment.
Point of manufacture identity injection systems	Inserting a digital ID into a new device as part of the manufacturing process. This ID is used to securely communicate with the device once it is in use	This process helps prevent counterfeiting and prevents malicious entities replicating or assuming an identity. What would be the consequences if an attacker were able to duplicate or insert an ID into your manufacturing process?

Area	Description	Considerations
Point of manufacture firmware install	Secure identification of firmware at point of installation	It's critical to ensure that your firmware is securely authenticated before installation to prevent malicious firmware. What is your process for identifying firmware? Which vendors are you relying on?
Supply chain communica-tions	Ordering, payment, scheduling, involving storage and transfer of Personally Identifiable Information (PII), sensitive and financial data	It's likely that your processes involve multiple other vendors and suppliers, including sensitive commercial information and PII. Make sure these processes are secure in order to protect your data, equipment, accounting and IP.

Defense and Critical National Infrastructure

Critical National Infrastructure (CNI) includes everything from defense systems, energy systems, nuclear power, telecommunications and transport, to healthcare, finance and government.

Each of these areas is supported by people, assets, and systems that need to be kept secure.

The classified data held by defense and infrastructure businesses can have a long shelf life, and will still be of value in the post-quantum era. CNI data now is at risk of interception and future decryption. Protecting sensitive data and critical infrastructure must be a priority for CNI. PQC solutions can help them upgrade their hardware (such as vehicles, sensors and hardware security modules) and software (such as public key infrastructure, transport layer security and virtual private networks) to become crypto-agile and quantum-resistant.

Defense

Area	Description	Considerations
Intelligence and secure data	Classified critical data shared between networks, user identities, devices and machines	What methods of storage and data collection are currently in use? What would be the impact of intelligence data being intercepted?
General communica-tions	Operational communications and standard communication channels	Administrative functions will need to be protected as well as more sensitive communication channels. General communications are likely to include different levels of classified information, and involve different encryption techniques.
Mobile, fixed and tactical communica-tions	Satellite systems, ground systems, Unmanned Aircraft Systems (UAS)	What would be the impact on national security if these assets were somehow compromised? It's likely that different levels of encryption exist to protect against this threat, and each encryption method will need to be considered carefully.
Mission Command, Command and Control (C2)	Secure data shared between networks, user identities, machines, command and control systems	Communications channels used in simulated or conflict situations need to be securely protected. It is worth taking a deep-dive into the ways systems communicate with each other, as well as users, machines, assets, and personnel.
Medical systems	Personal records, medical equipment, deployable person records	Multiple systems keep the deployable forces protected and will need to be considered. What data shows the deployability of forces? What would be the impact of an interception of this data?
Cloud-based data	Centralized data available to multiple systems in multiple locations	Major Department of Defense (DoD) initiatives such as Joint All Domain Command and Control (JADC2), Joint Warfighting Cloud Capability (JWCC), etc.

Area	Description	Considerations
Industrial control systems	Power generation, systems critical to maintaining base operations and support	This affects the ability to deploy forces/force generation and maintain home-based operation.

Energy

Area	Description	Considerations
Generation plant control systems	Transfer of data between systems and machines across secure networks	Energy security is of high importance to national infrastructure, and involves a complex network of natural resources, critical data and sensitive material. It is likely that many of the systems involved will already use cryptographic protection, and will require considering in the post-quantum era.
Pumping control systems/Grid control systems	Physical controls, machine identities, user identities across a secure network	Cryptography is likely to be used to authenticate users, as well as the transfer of data between these physical controls.
Energy discovery data collection systems	Storage of sensitive data, connection between machines and networks	Energy security depends on the discovery, analysis, and feasibility of natural resources. It is essential to consider how this data is stored in the long-term and what the impact would be of currently stored and classically encrypted data being harvested for future decryption.
Secure supply chain communica-tions	Ordering, payment, scheduling, involving storage and transfer of PII, sensitive and financial data	How is critically sensitive data stored? What methods of encryption currently prevent a malicious attack as the data is transferred between systems/trading partners, and what would be the impact of a potential breach or theft?

Retail

Quantum cryptography has the potential to dramatically impact the security of data and communications in every industry. Retail forms a large part of national and international economics, relying as it does, on the relationship between consumers, goods, suppliers and services. This makes retailers a lucrative and strategic target for attackers.

By adopting PQC, retailers can help defend against quantum attacks on financial, personal, supply chain, and customer data.

Area	Description	Considerations
Supply chain communica-tions	Transfer of data between systems and machines across secure networks	Which vendors and suppliers are you using? Which companies are you supplying to? Make sure that connections and processes in your supply chain are secure in order to protect your data, equipment, accounting, and IP.
Payment systems	Point of Sale (POS) transfer of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data between remote points and a network, storage of sensitive data	Your organization needs to secure personalized information such as billing details, customer mail addresses and contact details, as well as data relating to transaction records. How is this data stored? How is it managed securely between systems?

Telecommunications

Many telecommunications organizations rely on cryptographic systems to secure their networks, protect customer data, and ensure the integrity of their communications. Migrating to PQC will require updating existing infrastructure, including encryption software, hardware and protocols.

Area	Description	Considerations
Secure user provisioning	User identities, machine identities, for example enabling SIM cards. Connection between networks and remote devices	Cryptography is used to authenticate and protect users and machines logging into systems and using networks. It's essential to consider how these processes might be under threat from a possible quantum attack.
Subscriber identity management	User identity, storage of Personally Identifiable Information (PII), transfer between devices and networks	How is your user identity data stored? What would happen if that encrypted data were extracted and decrypted at a future point in time?
Payment processing	Transfer of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data> between remote points and a network, storage of sensitive data	Your organization needs to secure personalized information such as billing details, customer mail addresses and contact details, as well as data relating to transaction records. How is this data stored? How is it managed securely between systems?

Logistics

Planning, implementing and processing the movement of goods involves a complex network of systems, and many of these systems depend on secure connections between points. As quantum computing becomes increasingly a threat, logistics organizations will need to think carefully about their infrastructure, storage of data, and communications network.

Area	Description	Considerations
Secure vehicle communica-tions	Transfer of data between remote points and between networks	How is data stored and moved between vehicles and networks? Cryptography will be in use to keep those channels safe and your network moving.
Point of delivery tools/Scanning tools	Transfer of sensitive data between remote points and networks	Sensitive data will be transferred from remote points such as handheld devices. What would be the impact of that data being intercepted?

Media

As quantum computers continue to improve, traditional cryptographic methods for keeping files protected will need to be migrated to PQC. Media-based organizations are dependent on digital technology, including cloud-based services and platforms, and streaming services.

Additionally, these companies, many of them high-profile, are often subject to various regulations and compliance requirements. PQC will be necessary to maintain the level of compliance required.

Area	Description	Considerations
Digital Rights Management (DRM)	Secure streaming of files	Streamed content is required to be tightly controlled to protect it from misuse or unauthorised manipulation. The processes involved in DRM include cryptography that could be intercepted by a quantum attack.
User access control	User identity management, device management, transfer of PII	How are your users authenticated? What cryptography is enabling sign-in and is the method secure?

About PQShield

The PQShield team is helping to shape the way our digital world is protected against the threats of tomorrow. At a time when quantum computers will soon be able to break current cryptography methods, we're focused on empowering organizations, industries, and nations, with the ultimate quantum-resistant cryptography solutions.

PQShield began as a spin-out from the University of Oxford, but now with teams in Europe, Japan, the US, and the UK, PQShield has grown into a world-class collaboration of post-quantum cryptographers, engineers, and operators.

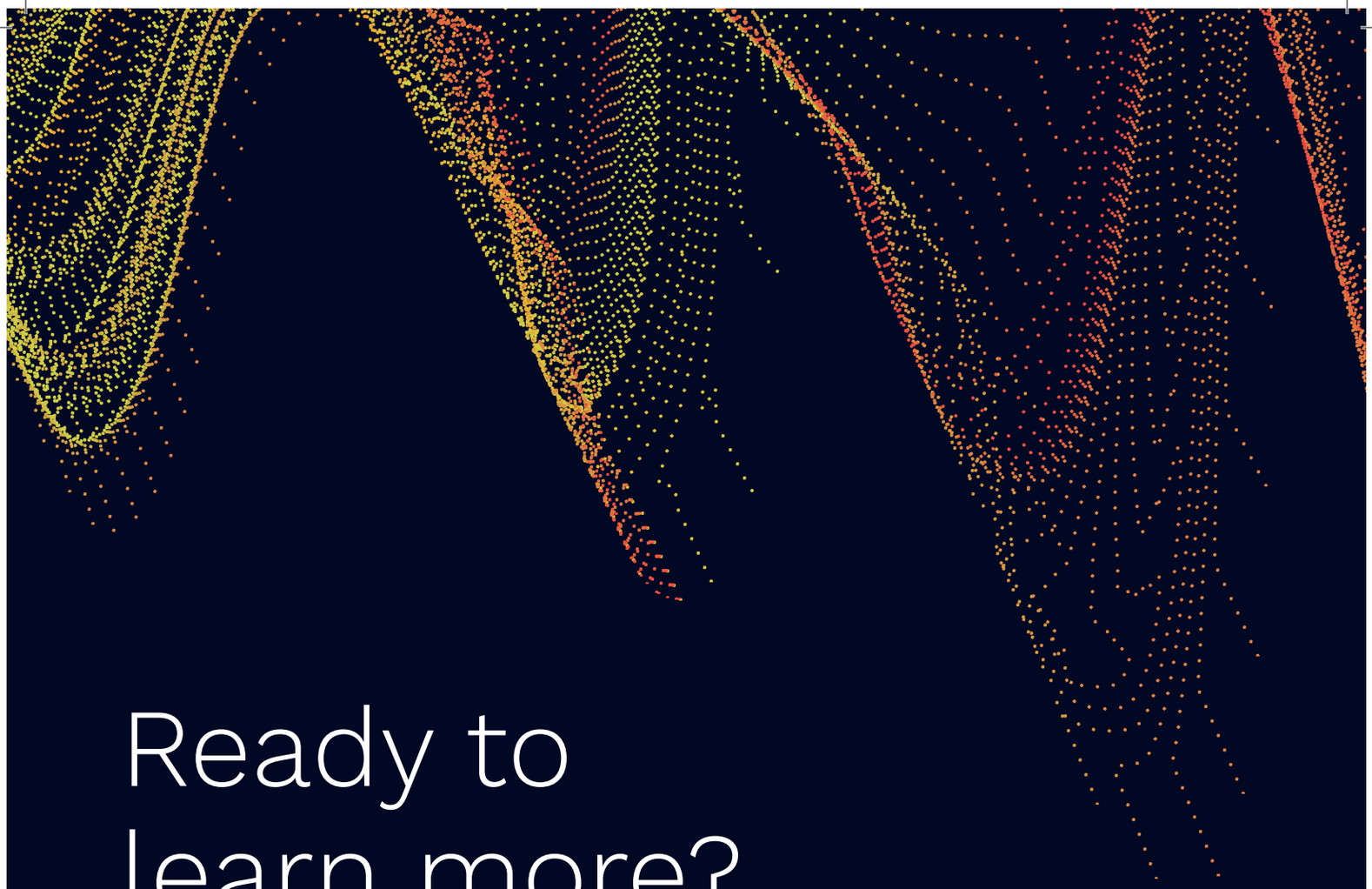
We are a source of truth for stakeholders at every level, and we're seen by both customers and competitors as a leading provider of PQC solutions in hardware and software. Our think openly, build securely ethos has helped us to shape all of the first international PQC NIST standards, and to be the first cybersecurity company to develop quantum-safe cryptography on chips, in applications, and in the cloud.

We've also contributed multiple cryptographic extensions to RISC-V, the open standard instruction set architecture (ISA) that is gaining traction from proprietary competitors such as ARM and Intel, alongside working with many other organisations like the World Economic Forum, IETF, ETSI, GSMA, NCCoE, PQCC and GlobalPlatform, to advise and define their own positions. We're also the experts on PQC side-channel attack resistance, having built a dedicated SCA test lab verified by our industry leading partners.

Our mission is to build products and solutions that help modernize the legacy cryptography in the world's technology supply chain, to deliver new global standards alongside real-world hardware and software upgrades, and to keep the world one step ahead of the attackers. Our mature PQC software and hardware solutions are already in the hands of forward- thinking organizations like Microchip, AMD, Collins Aerospace, MBDA Weapons Systems and many more.

PEERS QUALITY ASSURANCE LTD UKAS MANAGEMENT SYSTEMS
ISO/IEC 27001:2013 9940

PEERS QUALITY ASSURANCE LTD UKAS MANAGEMENT SYSTEMS
ISO 9001:2015 9940



Ready to learn more?

Get in touch

contact@pqshield.com | www.pqshield.com

PQShield Ltd
Oxford
Prama House
267 Banbury Road
Oxford
OX2 7HT

PQShield SAS
Paris
8 Rue des Pirogues de Bercy
Paris
75012

PQShield B.V.
Amsterdam
Keizersgracht 62
1015CS
Amsterdam

PQShield Inc.
New York
228 East 45th Street
Suite 9E
New York
NY 10017

London
City Tower
40 Basinghall Street
London
EC2V 5DE

PQ SHIELD

think openly, build securely

pqshield.com