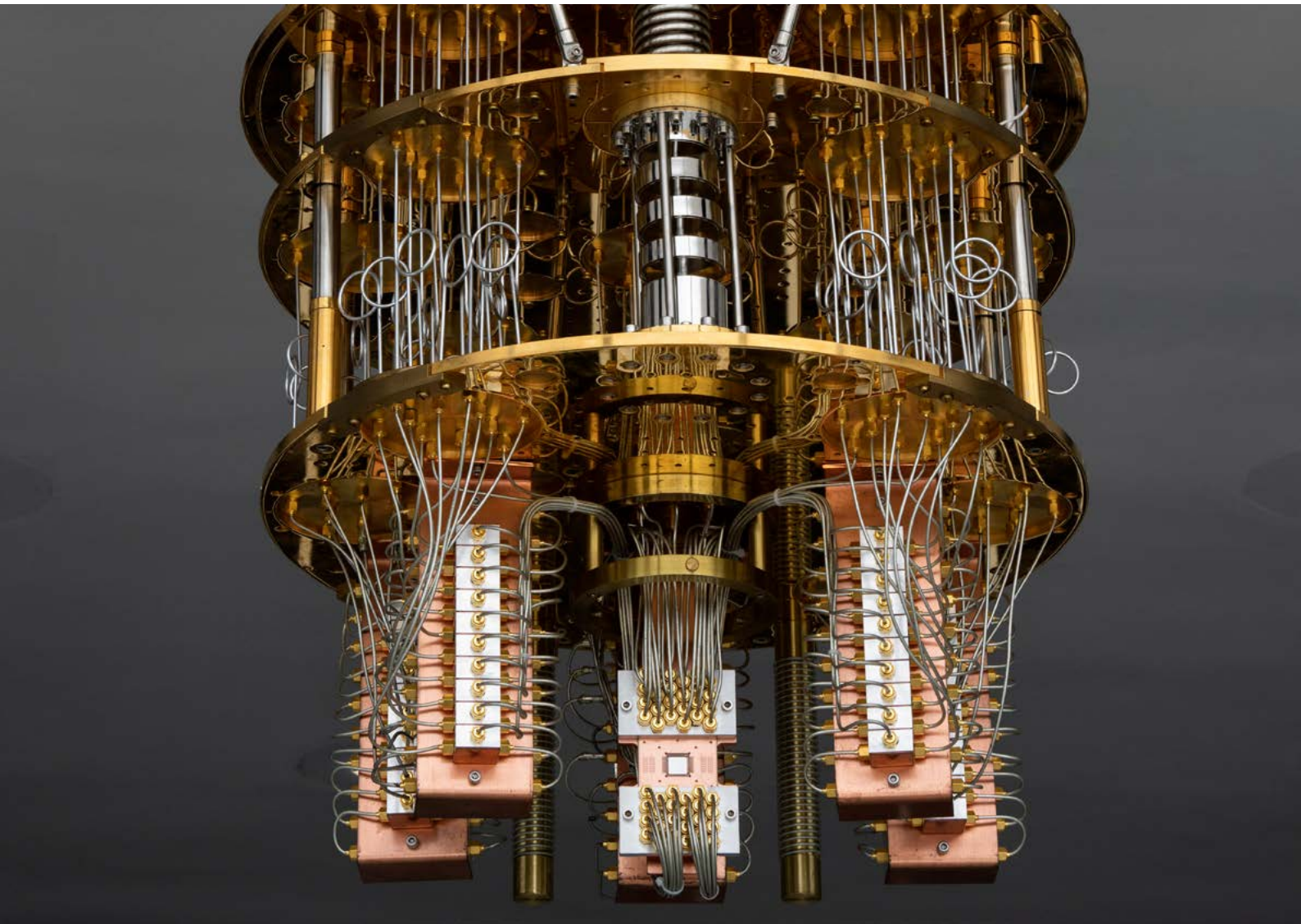
Kicking off your quantum migration program

Guide for conducting a risk analysis and migration planning



AIVD

The General Intelligence and Security Service of the Netherlands (AIVD, Algemene Inlichtingen- en Veiligheidsdienst) focuses on defending democracy against national and international threats so we can live in freedom. The AIVD protects the Netherlands and its population, often invisibly. To this end, the AIVD conducts investigations in the Netherlands and abroad. The AIVD does what is needed to prevent states, organisations or persons from defying, undermining or attacking our rule-of-law. We cannot do this alone. The AIVD has its own role in the network of government bodies that protect the national security of the Netherlands. The AIVD is a department within the Ministry of the Interior and Kingdom Relations.

The National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) is the central information hub and centre of expertise for cybersecurity in the Netherlands. The NCSC's objective is to boost the digital resilience of Dutch society. It is also responsible for protecting the vital infrastructure of the central government of the Netherlands by improving the nation's digital resilience and minimising the consequences of cyber incidents.

Target audience

This guide was written to assist people who play an important part in preparations for the migration to new standards and have responsibilities in defining and implementing a migration plan. In the first place, this includes CIOs, CTOs and CISOs. This guide may also be an interesting read for crypto custodians, and ICT and security architects.

The following parties contributed to this guide:

Anita Wehmann (MinBZK), Oscar Koeroo (department CISO MinVWS), Thomas Attema (CWI/ TNO), Vincent Dunning (TNO), and employees of the Dutch Banking Association and KPN CISO Office.

Introduction

The development of powerful quantum computers has accelerated in the past years. The general view among experts is that quantum computers will probably have sufficient computing power to break many of the most common cryptographic algorithms by 2030 to 2040. Cryptography is an important foundation for information security. As such, the advent of a powerful quantum computer may represent significant risks to organisations that will endanger the confidentiality, integrity and availability of information and processes.

Since 2014, the General Intelligence and Security Service of the Netherlands (AIVD) and National Cyber Security Centre (NCSC) have issued several publications to inform organisations of these risks.[1] Now, it is time for organisations to take action and start preparing for the migration to quantum-safe cryptography. This is why the AIVD and NCSC have created this guide for CIOs, CTOs and CISOs in the government, the business industry, and knowledge institutes.

1 Cf. '*Informatieblad over quantumcomputers* ['Information sheet on quantum computers', in Dutch], AIVD, 2014, https://www.aivd.nl/documenten/publicaties/2014/11/20/informatieblad-over-quantumcomputers; *Factsheet postkwantumcryptografie* ['Factsheet on post-quantum cryptography', in Dutch], NCSC, 2019, https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-postkwantumcryptografie; and *Bereid je voor op de dreiging van quantumcomputers* ['Prepare for the threat of quantum computers', in Dutch], AIVD, 2021, https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.

Getting started with preparing for the migration to quantum-safe cryptography

The migration to quantum-safe cryptography/post-quantum cryptography (PQC)[2] is a complex endeavour and will cost organisations a lot of time and resources. It is therefore important to start preparing for migration now, so your organisation will be shielded from the threat of quantum computing when the time comes. This guide offers some concrete starting points for:

- Mapping your organisation's risks with regard to the quantum computing threat;
- Mapping the crypto assets used by your organisation;
- Risk assessment; and
- Drawing up a migration plan.

The guide also briefly discusses the quantum computing threat and a number of concrete steps that can be taken today. These are the so-called no-regret measures (i.e. measures that will be valuable in all cases). Finally, the guide considers developments relating to the advent of quantum computing for 2023-2024 as shown in Table 1. This guide supplements the PQC Migration Handbook[3] that was published earlier and offers a more elaborate description of the steps that organisations should get started with today (mapping and planning).

The urgency to migrate varies for every organisation. Some organisations cannot wait for post-quantum cryptography standards (which are expected to be available by 2024) because their data needs to be quantum-safe now. Other organisations will benefit from waiting for new quantum-safe cryptographic standards to become available. The urgency and required speed of migration depends on an organisation's risk profile and its risk appetite. For all organisations, it is important to conduct a specific risk analysis for the quantum computing threat and to start preparing for the migration to quantum-safe cryptography.

2 Post-quantum cryptography (PQC) is understood to mean cryptography that is impervious to the threat of quantum computing. However, PQC is defined in different ways by different stakeholders. According to some definitions, for instance, PQC does not include symmetric cryptography such as AES. In this guide, quantum-safe cryptography means both asymmetric and symmetric cryptography that is resistant to the quantum computing threat.

3 See 'The PQC Migration Handbook', TNO, CWI and AIVD, 2023, The PQC Migration Handbook | Publication | AIVD

Table 1: Overview of major threats, the scope for action, and expected developments in the field of quantum-safe cryptography.

	Applicable today (2023-2024)	The future (2025-2035)
Threats	- The 'store now, decrypt later' scenario.	- The integrity of digital signatures is compromised. - The reliability and integrity of data and systems are compromised.
Perspective for action	- Conducting a risk analysis, mapping of cryptographic assets and preparing for migration by creating a migration plan. - Taking no-regret measures.	- Actually conducting migration paths.
External developments	- The new availability of new PQC standards (NIST). - The development of complementary software (e.g. for mapping and asset management).	- Embedding new standards in products. - The development of new guidelines and best practices for migration. - Large-scale migration paths (e.g. internet standards).

The threat explained

It is unlikely that there are quantum computers today that have enough computing power to represent a serious threat to current cryptography. We cannot predict with any certainty at what time it will be possible to use quantum computing to break some of the most common forms of cryptography. A breakthrough may lead to the development of a powerful quantum computer sooner than expected, for instance. Developers may also create new quantum algorithms that will represent a threat to cryptographic algorithms with limited computing power.

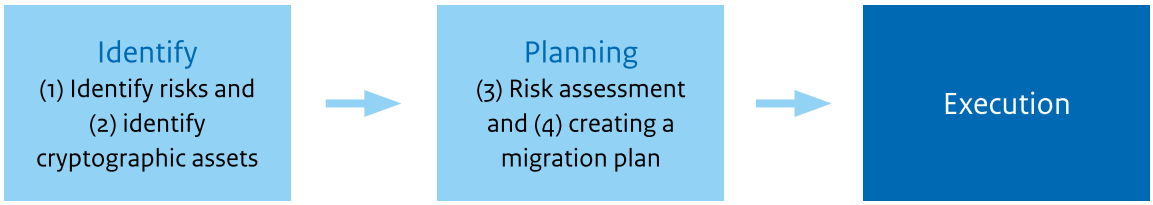
Based on current insights, the 'store now, decrypt later' scenario is the most urgent threat for organisations. Malicious actors could already be collecting encrypted data from their targets so they can decrypt it in the future, once quantum computers have sufficient computing power. Today, it is mainly state actors that represent this threat because they have the intent and required resources to execute such attacks. Organisations that possess sensitive data that must remain confidential after the introduction of quantum computing, must therefore take additional measures today in order to safeguard their data against the actual quantum computing threat.

As Table 1 shows, there are other relevant threats that must be taken into account. Risks also exist with regard to processes that use authentication or authorisation systems or that must register and verify digital signatures, for instance. While these threats might arise at a later point in time, this does not mean that organisations should not start preparing for migration to quantum-safe cryptography already.

Preparing for migration

The migration to quantum-safe cryptography involves complex challenges that will require a lot of time, planning and preparation.[4] Organisations that start preparing for this migration too late, risk not being protected against the quantum-computing threat by the time it materialises. It is therefore important to make time and resources available and deploy them in your organisation in a structured and effective manner.

Figure 1: This guide provides starting points for mapping risks and crypto assets, assessing risks, and creating the migration plan.



Structuring and prioritising next steps can be done through the process of assessing and mitigating any specific risks an organisation faces due to the quantum computing threat. Therefore, make sure that your organisation has an existing and ongoing risk management process in place. [5] Use this process to map the most important business interests that must be protected and outline any existing organisation-wide risks. This will help you better define the risks associated with the quantum computing threat and prioritise actions necessary for preparing (and executing) the migration.

4 Migration can take a long time even with a single encryption standard. For instance, it took more than five years to migrate from SHA-1 to SHA-256 even though the specifications and implementations were already available. The migration to quantum-safe cryptography will be immeasurably more complex and on a much larger scale and is therefore expected to take up a lot of time and effort.

5 Cf. '*Factsheet Risico's beheersen: de waarde van informatie als uitgangspunt* ['Factsheet Risk Management: the value of information as point of departure', in Dutch], NCSC, 2023, https://www.ncsc.nl/documenten/ publicaties/2020/juli/21/factsheet-risicobeheersing.

In the next couple of chapters, we provide starting points and guidelines for incorporating specific risks relating to the quantum computing threat into your existing risk management process. These starting points are:

1. Determine if, and if so, which parts of your organisation are at risk due to the quantum computing threat, and identify your organisation's most important business interests that require protection;
2. Identify your security measures for business interests that use cryptography;
3. Assessing and prioritising risks; and
4. Mitigating and controlling these risks by establishing a migration plan that implements measures to improve your organisation's resilience at this early stage.

1. Gain insight into risks

The risks for your organisation are associated with the interests you are protecting and the intent of an actor who has access to a powerful quantum computer. The first step in establishing your migration plan is gaining insight into potential risks. Based on the current state of knowledge of the quantum computing threat, we recommend taking the following considerations into account in your risk analysis:[6]

- Initially, it is likely that only advanced (state) actors will have access to quantum computers that are powerful enough to break existing cryptographic algorithms. If your organisation or one of your chain partners, customers or suppliers may be a target of state actors, the advent of quantum computing will put your organisation at risk.[7]

- At present, the most realistic and current threat is that data confidentiality will be breached. Other threats, such as authentication and authorisation systems being compromised, will become relevant as soon as powerful quantum computers become available. In this context, it is vital that your risk analysis maps processes, systems and infrastructures that are used to store, process or transfer sensitive or confidential information. In particular, you should look at information that must remain confidential after the advent of quantum computing.

- If, in the near future, you will be replacing or procuring systems with a longer service life, such as ICS/SCADA systems, then you should assume that these systems will have to deal with the advent of powerful quantum computers within the course of their lifetime. This means that such systems will not only have to be resistant to 'store now, decrypt later' threats, but also to such threats as an attack on authentication and authorisation systems. You should therefore also consider the quantum computing threat in your risk analysis with regard to procurement or replacement projects of systems with a longer lifetime.

6 See chapter 2 of the PQC Migration Handbook.

7 Cf: 'Dreigingsbeeld Statelijke Actoren (DBSA 2)' ['Threat Assessment State-sponsored Actors', in Dutch], AIVD, 2022, https://www.aivd.nl/documenten/ publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2.

2. Maintain an overview of cryptographic assets that your organisation uses (crypto asset management)

The importance of maintaining an overview

Cryptographic assets are all (security) measures that use cryptography. An inventory of your crypto assets is indispensable in establishing a structured and effective migration plan. In a broader sense, an accurate and up-to-date list helps monitor possible vulnerabilities in your existing security architecture and solve them quickly should any vulnerabilities be found in algorithms or software libraries. Maintaining a clear asset inventory is therefore not just important with an eye to the migration to quantum-safe cryptography, but it also constitutes a vital part of your asset management in the broadest sense.

The actual risk facing your organisation depends on the security measures that are already in place and how they make use of cryptography. An accurate and up-to-date inventory of cryptographic assets in use will tell you what those are. Making such an inventory can be a challenge. We recommend to start creating an inventory for those business interests that are at risk due to the quantum computing threat based on the analysis performed in the first step.

We recommend appointing someone who will be responsible for managing (and updating) the inventory of crypto assets on behalf of the management or board, for instance your organisation's crypto custodian. In many cases, they will have to create and manage the inventory manually in collaboration with your suppliers and technical experts. At present, software is being developed to create such a list semi-automatically in the future. The CISO is generally the person responsible for ensuring that the inventory is shared and placed in context throughout the organisation on behalf of the management or board.

You can use a Cryptographic Bill of Materials (CBOM) to record crypto assets within your organisation. This is derived from the more familiar Software Bill of Materials (SBOM) that describes crypto assets and their dependencies. You should record at least the following information:

- The forms of cryptographic algorithms and protocols that are in use (type, version);
- The cryptographic materials that are in use (e.g. certificates with associated expiry dates and key lengths);
- The physical systems involved (e.g. servers, information systems, smartcards);
- Dependencies on other systems or data (e.g. open source libraries); and
- Your dependencies on external parties, such as the system vendor, and the associated arrangements, for both closed source and open source hardware or software.

You should also register the purpose of the cryptography used. Does it protect data, for instance, or is it part of an authorisation system? Establish the link between these crypto assets and your business interests that require protection. This will help you determine the extent of the risk to your organisation and which (critical) parts of your organisation are impacted.

See crypto asset management as part of your broader asset management strategy. For instance, you should establish the link between your CBOM and SBOM inventories and incorporate crypto assets in your Configuration Management Database (CMDB). Finally, make sure that you protect your inventories in a suitable manner.

The importance of crypto-agility

Crypto-agility means that cryptographic protocols, products and systems are implemented in such a way that it takes minimal effort to modify the associated cryptographic algorithms. A module system that uses software-based cryptographic algorithms will be more crypto-agile than a specialised hardware system, for instance. Crypto-agility is a configuration and design choice for systems that requires support from people or processes.

We recommend making sure that (new) systems are adequately crypto-agile based on your risk analysis. This means that there should be a reasonable expectation that these systems can be adapted within their service life in the face of developments of the quantum computing threat, such as the discovery of vulnerabilities in cryptographic (quantum-safe) algorithms. The required level of crypto-agility depends on the application. At present, there is no generic set of requirements to which crypto-agile systems must comply. We recommend expressing your need for crypto-agility to your vendors at an early stage.

3. Assess risks

A risk analysis will help you establish to what extent your cryptography-based security measures are at risk due to the advent of quantum computing. Cryptography is generally a component of a larger overall package of security measures. The risks to your organisation therefore depend on the manner in which these security measures are deployed. In some situations, such as information transport, cryptography is the only security measure against man-in-the-middle attacks. If the security of critical processes or infrastructures in your organisation depends heavily on cryptographic algorithms, these require close scrutiny when you establish a migration plan.

Review the outcomes of the risk analysis with an eye to the following factors:

- The threat;
- Business interests to be protected;
- Security measures that are essential to protecting these interests; and
- Cryptographic algorithms that support these security measures.

4. Draw up your migration plan

You can use the outcomes of the risk analysis to draw up a migration plan that aligns with your organisation's needs. It will show the timelines for the required migration, the prioritised actions, and the urgency with which parts of the organisation must be quantum-safe (at this point in time).

There are different mitigation strategies to ensure the quantum security of your organisation. An example is the migration of the cryptography used by your organisation, additional (physical) segmentation, or isolating systems. In most cases, waiting until quantum-safe standards become available for migration is the better option because implementing such new standards will have the smallest possible impact on business operations. We also recommend incorporating a number of concrete no-regret measures into your migration plan. Based on the steps described above, you can then concretise the timelines for executing these migration activities in your organisation.

No-regret measures and early adoption

There are a number of no-regret measures that you can already include in your migration plan and will not represent significant risks to your current operations. This way, you can make sure that your cryptographic protocols (such as TLS) make use of the most recent version (TLS1.3).[8] It is likely that new quantum-safe standards will only be embedded in the most recent version. By taking preparative steps and using the most up-to-date cryptographic protocols at this point in time, you can ensure that your future migration can be performed with less effort.[9]

We also recommend doubling key length when using symmetric cryptography. The current consensus is that this will provide sufficient mitigation against the quantum computing threat. For asymmetric algorithms, we recommend waiting for the NIST standardisation process (refer to the header 'Look ahead').

Does your organisation have a very high urgency to migrate, meaning that it cannot wait for the quantum-safe cryptography standards? In this case, you should consider implementing hybrid solutions today, using a combination of existing cryptographic standards and (candidate) PQC algorithms.[10]

8 Cf: '*NCSC ICT security guidelines for Transport Layer Security* (TLS) NCSC, 2021, https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1.

9 Cf. *Guidelines for quantum-safe transport-layer encryption*, NCSC, 2022, https://www.ncsc.nl/documenten/publicaties/2022/juli/guidelines-for-quantum-safe-transport-layer-encryption/guidelines-for-quantum-safe-transport-layer-encryption.

10 See chapter 4.1 of the PQC Migration Handbook about the migration of symmetric and asymmetric algorithms (including hybrid solutions).

We recommend that the CISO appoints a person within the organisation, department or division to help draw up and implement the migration plan (or having it implemented by a third party). The CISO will retain final responsibility for the definitive migration plan on behalf of the management or board. This individual does not have to be a cryptographic expert, but must understand where and why cryptographic principles are being used, what could go wrong if these protocols are violated, and what important dependencies between systems exist for (critical) business operations. This individual will also communicate with the different stakeholders, involves them in the process at the right times, and reports important findings to the CISO. In addition, they will stay informed of (technological) developments and possibilities in the field of cryptography. Typically, this person fulfils a role as enterprise or security architect or security consultant. It may also be worthwhile to appoint a project leader to coordinate the actual execution and implementation.

Execute the migration in coordination with your stakeholders

You will depend on a range of stakeholders in the migration to quantum-safe cryptography. Communicating with these stakeholders is vital in ensuring the security and interoperability of services. The principal stakeholders are listed below, explaining what you can agree upon with them whilst drawing up (and implementing) your migration plans.

Vendors and internal ICT department

Your (internal or external) hardware and software vendors may already be working on (preparing for) embedding quantum-safe cryptography in their delivered products. Open a dialogue to gain an understanding of what their migration plans look like and determine to what extent these plans will cover your risks. Discuss your needs with your vendors and reach a transparent agreement. Document such an agreement so you can communicate to your own organisation why specific choices are being made. Keep in mind that some market players may state that their products are already quantum-safe or PQC ready. We recommend always investigating and validating such claims thoroughly before making any decisions.

Procurement

Open a dialogue with the procurement department on (establishing) the requirements for buying systems, as well as software and hardware with cryptographic components. For future purchasing, you can reach an agreement on crypto-agility and what this means for migrating such new systems. These processes can be incorporated into the terms of procurement.

Supervisory bodies/inspectorates

Involve supervisory bodies/inspectorates to ensure that your plans comply with the applicable (legal) frameworks and directives.

Customers and other dependencies

Discuss your migration plans with customers, partners and other internal stakeholders and establish agreements where necessary. This communication is important because the migration may, for instance, present interoperability challenges, as a result of which it may be unexpectedly impossible to deliver some services.

Risks in your migration path and plan B

There is still much uncertaint about the timelines of the quantum computing threat. A technological development may occur that increases the urgency of specific threats, or the planned quantum-safe cryptography may contain unintended vulnerabilities. Moreover, the progress of your migration may incur delays for a range of reasons, as may happen in any migration. It is important to be alert to the aforementioned developments and timelines. This will ensure that you keep on top of the risks to your organisation and your migration will be implemented on time. You should also include plans for alternate mitigating measures in your migration plan, such as additional (physical) network segmentation, if your migration path is not expected to be able to mitigate the risks in a timely manner. You should also describe the expected impact on your organisation's objectives and business operations.

Look ahead

At this time, stakeholders are working on guidelines and standards for migrating to quantum-safe solutions in different ways. One example is software that automatically maps crypto assets in existing networks. The American NIST is working to establish standards for quantum-safe cryptography in public key cryptography as part of an open international partnership.[11] These standards are expected to be finalised in 2024 and will be implemented on a large scale. We recommend staying informed of NIST developments relating to PQC algorithms.

The AIVD and NCSC are keeping a close eye on these developments and will include relevant new developments in future versions of this guide or additional knowledge products. Make sure to check out our websites and social media for new publications.

11 Cf. 'Post-Quantum Cryptography', Computer Security Resource Center (NIST), 2023, https://csrc.nist.gov/Projects/post-quantum-cryptography.

Summary scope for action

- Start by conducting a risk analysis to determine which of your business interests that requires protection may be at risk due to the quantum computing threat.
- Using the outcomes of the risk analysis, create an inventory what cryptography your organisation is using and managing, who delivers it, and which existing security measures rely on the cryptography that is in place. Incorporate this into your broader asset management process.
- Assess your risks based on current quantum computing threat insights, your business interests that require protection, and the extent to which your existing security measures depend on cryptography.
- Determine how you want to manage and control your risks. Incorporate crypto-agility into your terms of procurement and draw up a migration plan in consultation with your vendors, chain partners and other stakeholders. Develop an alternate migration strategy as part of your migration plan in case you are unable to execute your migration plan in time.
- Keep up with important developments in quantum computing and review your risk assessment and migration plan in light of these developments on a regular basis. Adjust the migration plan if needed.

As it may be challenging to collect knowledge and keep up with important developments, you can also rely on external resources and partnerships.

Keep a list of people you can turn to within your organisation or determine what external sources will be able to answer your questions. If you are responsible for managing classified state intelligence, contact the NBV at the AIVD.

This brochure is published by:

General Intelligence and Security Service aivd.nl
P.O. Box 20010 | 2500 EA The Hague

National Cyber Security Centre ncsc.nl
P.O. Box 117 | 2501 CC The Hague

January 2024 | Publication no 23405792