Network Security in a Quantum Future

Proof-of-concept development of a Quantum-Aware Risk Manager (Q-ARM) tool for the energy sector

NESO
National Energy
System Operator

Network Security in a Quantum Future Contributing Partners

NESO	National Energy System Operator (Lead)
cambridge consultants Part of Capgemini Invent	Cambridge Consultants
THE UNIVERSITY of EDINBURGH	University of Edinburgh

Executive summary

The field of quantum computing opens up many new opportunities. The topic is technically challenging, and its potential benefits and threats have attracted a great deal of academic research. The quantum threat to cybersecurity is gaining more prominence as a challenge that critical national infrastructure (CNI) providers must begin addressing in the near-term. Notably, the National Cyber Security Centre (NCSC) has just published guidelines for a timeline for CNI providers to migrate their cryptography to be quantum-safe, for example.

Network Security in a Quantum Future (NSiaQF), a Strategic Innovation Fund (SIF) Alpha project, is the next step in providing much-needed visibility for energy network operators. The insight it aims to provide into the scale and timing of the quantum threat for energy systems will enable energy networks to pursue appropriately tailored mitigations.

During the NSiaQF SIF Discovery phase, the project team scoped and designed two interconnected automated tools – the Quantum-Aware Risk Manager (Q-ARM) tool and the Quantum Threat Tracker (QTT). These will assist energy networks to identify and prioritise the systems requiring migration to post-quantum cryptography (PQC).

The objective of the Alpha was to develop proof-of-concept demonstrators of the proposed Q-ARM and QTT tools. This work has been led by the National Energy Systems Operator (NESO) with partners Cambridge Consultants and the University of Edinburgh.

The Q-ARM, which is the subject of this report, is a decision support software tool designed to help operators rapidly model energy sector systems, and systematically identify the risks to those systems posed by quantum computers. It is designed to make post-quantum readiness assessments of energy network assets relatively simple, scalable and reproducible, helping to ensure good value for consumers and support network resilience. It will also help energy networks meet the previously mentioned PQC-readiness timelines.

The QTT is designed to inform and directly feed into the risk assessment delivered by the Q-ARM tool with the latest quantum research. It does this by standardising and formalising the process of estimating when a cryptographically relevant quantum computer will emerge for specific algorithm/key length pairs. See "Proof-of-concept development of Quantum Threat Tracker (QTT) tool for the energy sector" for the Alpha phase report on the QTT.

This report outlines the work that the consortium completed to create an initial proof-of-concept demonstrator for the Q-ARM tool in the Alpha phase. The aim was to demonstrate and illustrate the functionality for potential end users across the energy

sector, and to solicit their feedback. The demonstrator includes an interactive wireframe to demonstrate the user interface for the tool.

The NSiaQF project has delivered several innovations in the Q-ARM Alpha development project, including:

- We developed a clear and innovative approach to characterising the attack types that are enabled by quantum computers and linked those attacks to asset types.
- We developed an innovative quantum risk analysis process for the Q-ARM tool functional prototype. As part of this, we demonstrated that the Q-ARM can successfully process quantum computing threat intelligence from the QTT to inform its evidence-based risk analysis.
- We created a set of unique mapping tables (drawing on a range of previously unconnected research sources) that enable the tool to undertake automated quantum risk discovery. These include: a definitive mapping of mathematical problems (used in quantum-vulnerable cryptographic schemes) to the high-level communications protocols that use them; a unique mapping of mitigation types to quantum attack types that allows the tool to rapidly filter suggested mitigations based on applicability; and a mapping of quantum-enabled attacks to system security properties that allows the effects of attacks to be modelled by the tool.
- We created an architecture that allows the user to create and store energy asset models, for sharing and for use in creating system models.
- We demonstrated the ability of the tool to automatically identify the risks posed to a system by an attacker using a quantum computer for a limited set of pre-identified energy system assets.

It is worth noting that many of these innovations have potential applications outside of the scope of this project; but in the first instance, they will be used to ensure energy sector quantum security.

The value of the Q-ARM tool prototyping activities undertaken in this work package comes from de-risking key aspects of the tool's development. Specifically, the Alpha has delivered value by:

- **Derisking the technical development of the Q-ARM tool**

  Building and testing the Q-ARM proof-of-concept demonstrator has enabled us to demonstrate that it is possible to identify risks from a machine-readable representation of energy systems, to characterise quantum-enabled attacks, and to map these to energy systems in a meaningful and reproducible way. The implementation of these features has provided confidence for proceeding with more rigorous full tool development in Beta.

- **De-risking usability and utility of the user interface through the UX Design**

  The Figma user interface prototyping tool enabled us to rapidly test usability without requiring costly rework. This enabled us to design and test user workflows and interfaces, providing confidence in the starting point for Beta.

- **Testing the utility of various system features through our interactions with energy sector stakeholders**

  Stakeholder feedback has allowed us to identify the most useful features and filter features down: e.g., creation of the user-configurable risk scaling feature in the tool.

- **Maximising the likelihood of stakeholder adoption and buy-in**

  By including key energy network stakeholders in the design process we have maximised the potential for business as usual (BAU) adoption, where value will be realised. We expect to further broaden the range of stakeholders during Beta.

In conclusion, we are confident that the Q-ARM Development Work Package has successfully demonstrated both the technical feasibility of the Q-ARM tool and demonstrated and enhanced the desirability of the tool. We continue to believe that the NSiaQF project delivers meaningful innovation and significant value for the energy sector and for consumers. We look forward to the opportunity to take development to the next stage, building on the Discovery and Alpha Phase, to rapidly develop a tool that can be adopted as part of BAU across the energy sector, enabling a quantum-safe future for the UK's energy users and suppliers.

Contents

1. Introduction

This report forms one of the key deliverables from the Network Security in a Quantum Future (NSiaQF) project. The purpose of this report is to document the research performed in the proof-of-concept demonstrator development in the Strategic Innovation Fund (SIF) Alpha stage. This project follows a successful SIF Discovery phase, completed in 2024.

The Network Security in a Quantum Future (NSiaQF) Project

During the Discovery phase of NSiaQF we scoped and developed an initial design for two interconnected tools. These tools could help energy network operators to prepare for the security threat posed by quantum computing by identifying and prioritising the systems requiring migration to post-quantum cryptography (PQC) in a scalable way.

The first of these tools – the Quantum-Aware Risk Manager (Q-ARM)– is designed to help operators rapidly model energy sector systems and systematically identify the risks to those systems posed by quantum computers.. The other – the Quantum Threat Tracker (QTT) - is designed to inform the risk assessment delivered by the Q-ARM tool with the latest quantum research, by standardising and formalising the process of estimating when a cryptographically relevant quantum computer will emerge for specific algorithm/key length pairs (see "Proof-of-concept development of Quantum Threat Tracker (QTT) tool for the energy sector" for the Alpha phase report on the QTT).

This report outlines the work completed to create a proof-of-concept demonstrator for the Q-ARM tool during the Alpha phase of the NSiaQF project and is one of the key deliverables for the project. To illustrate the functionality, we developed both a functional prototype and a prototype of an interactive 'clickable demonstrator' for the tool, screenshots of which are included in this report.

Structure of this Report

This report discusses the development of the Q-ARM tool during the Alpha phase, and the innovations produced during its development. Key elements are:

- In Section 2 we explain the purpose of the Q-ARM tool, and the goals of the prototype activities.
- Section 3 explains the research and development activities undertaken as part of creating the functional prototype part of the demonstrator, including the incorporation of an energy system test case.
- In Section 4 the design activities for producing a user experience (UX) model of the Q-ARM tool are detailed.

- Section 5 details the next steps required to productionise and release the Q-ARM tool.
- Section 6 details the conclusions from the Alpha phase proof-of-concept demonstrator activities, and the value provided by this program of work .

2. Quantum-Aware Risk Manager (Q-ARM) Tool Overview

The Q-ARM tool is one of the two key innovations being developed under the NSiaQF project (the other being the previously referenced Quantum Threat Tracker, which feeds technical analysis about quantum computing into the Q-ARM tool).

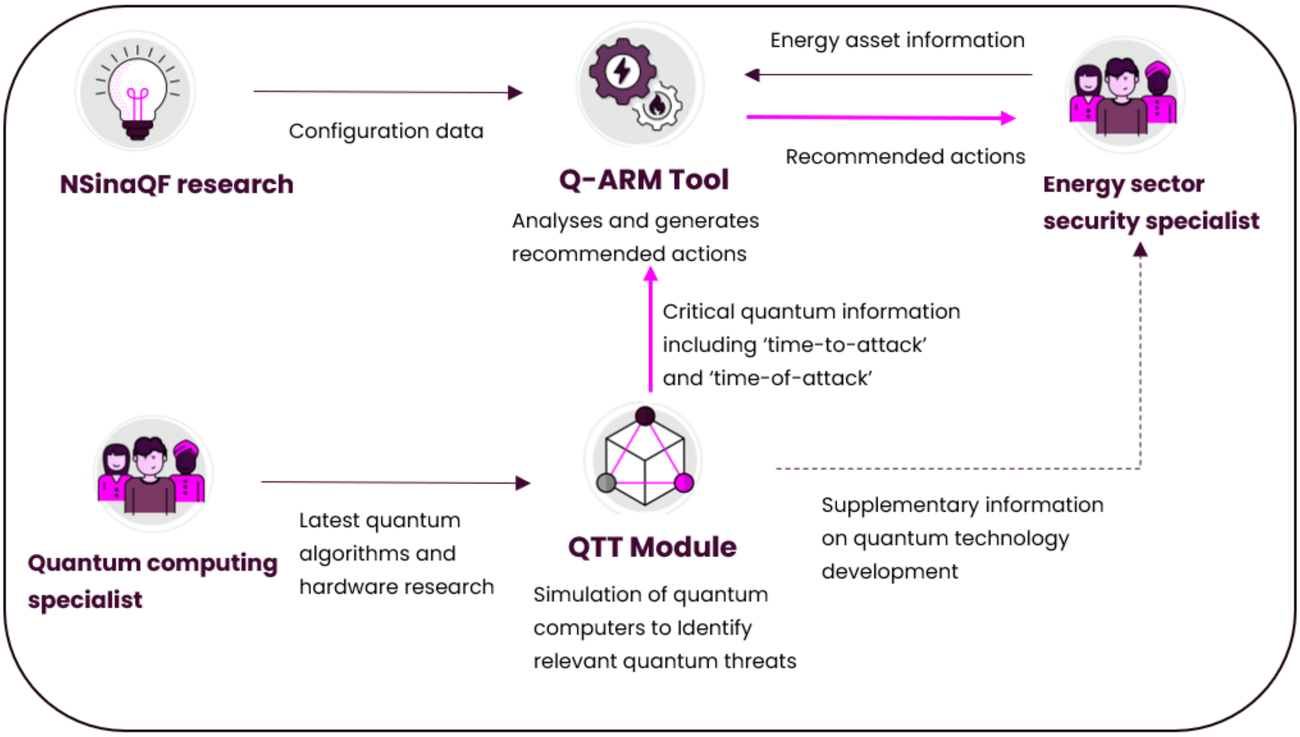

NSinaQF research
Configuration data
Q-ARM Tool
Analyses and generates recommended actions
Energy asset information
Recommended actions
Energy sector security specialist
Critical quantum information including 'time-to-attack' and 'time-of-attack'
Quantum computing specialist
Latest quantum algorithms and hardware research
QTT Module
Simulation of quantum computers to Identify relevant quantum threats
Supplementary information on quantum technology development

Figure 1: Tooling strategy for the NSiaQF project

Purpose of the Q-ARM Tool

The Q-ARM is a decision support software tool that will enable energy network security professionals to generate evidence-driven risk assessments about the quantum threat to the cryptographic security of energy systems. The reports and analysis generated will allow security teams to judge the priority of those risks against the other cyber security risks being managed by their teams.

This will mean that security resources and investment can be allocated strategically, to maximise network security and thereby minimise the risk of disruption for the consumer, at the best value. A clear evaluation of quantum risks ensures that the right mitigations and systems are prioritised to ensure quantum-safe cryptography is being deployed in the most vulnerable parts of the energy network, at the right time. The tool will also support energy network operators in meeting the recently announced NCSC guidelines (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines), which call for CNI providers to ensure that critical assets are quantum safe by 2031.

Functionality of the Q-ARM Tool

The Q-ARM works by interpreting the output from the QTT regarding time-of-attack (year when a quantum-enabled attack could realistically occur) and time-to-attack (amount of time it would take for such an attack to break the specified cryptography, once launched). The Q-ARM and QTT work together to calculate this information for specific cryptographic algorithms and apply it to energy network assets, enabling a security analyst to consider the appropriate mitigation response for their modelled system.

Within Alpha, we wanted to de-risk the most innovative and most time-critical features of the Q-ARM tool, to ensure they were possible before investing in the development of a custom tool set (as envisioned for a future Beta phase).

The Alpha phase objectives for the Q-ARM tool were to:

- Understand the feasibility of capturing expertise about the attacks that quantum computing enables in an automated tool.
- Create a clear and robust procedure for manipulating the underlying quantum and system data to generate a risk profile for energy systems.
- Collate and communicate the most important information about quantum threats (including the feasibility and potential mitigations) in machine-readable form.
- Present energy system specific quantum threat data in an output format that was both understandable and useful to security analysts and to quantum-non-experts.

This was assessed using two interlinked Q-ARM workstreams:

1. Developing a proof-of-concept demonstrator using functional prototyping (effectively the back-end functionality of the tool) to:
   - De-risk the most innovative and technically challenging features required by the tool.
   - Generate and test algorithms and data representations that enable the delivery of those features.
   - Identify the technically challenging design decisions and solutions.
2. Prototyping UX designs and demos (effectively the front-end user interface of the tool) to:
   - Create a user interface design that describes the interaction between the Q-ARM tool and its future users within energy network security teams.
   - Produce a ‘clickable demo’ to allow stakeholders to provide feedback and see how the tool would integrate into their BAU activities.

- Create and test out initial designs for communicating and visualising risks, for users of the tool and its outputs (as part of the clickable demo).
- Gather feedback from core stakeholders to be fed into the requirements for further development of both tool usability and features.

Q-ARM Tool Stakeholder Engagement and Dissemination

A key feature of the Q-ARM tool is that it enables a wide range of energy systems to be modelled by different stakeholders across the sector quickly.

To maximise the likelihood of success in meeting the needs of different types of network operators across the energy sector, the Q-ARM development team has engaged with energy sector stakeholders at multiple points during the Alpha phase. We have used these engagements to explain the project, capture feedback and discuss features with security and innovation teams across the energy sector.

These activities yielded new feature requests and design refinements, that have either been executed already or included in the roadmap for future development in a potential Beta phase of the project (see Development Roadmap section). In general, the feedback received was very positive; stakeholders were excited about the prospect of a tool that could help them to quantify and manage quantum risks appropriately and in a straightforward manner.

Improvements realised in this process include:

- Stakeholders were asked for energy assets that they would like to see prepopulated in the library of assets within the tool. Those that we have already identified have been included and pre-populated with criticality and technical parameters (note that individual organisations can change these defaults if they do not align with their security priorities).
- We have made the tool’s risk scales and matrices configurable by the user (though set at initial default values), to reflect the fact that different organisations within the sector have different risk appetites.

During the Beta phase of the project, we plan to conduct extensive outreach and dissemination within the sector to guide further development.

3. Functional Prototype Workstream: Development and Outputs

This section discusses the development of the Functional Prototype that underpins the Q-ARM tool, and the specific outputs created as part of the Alpha project. The Functional Prototype is the core system component of the proof-of-concept demonstrator; the other component is the UX Interface/clickable demo (discussed below in Section 4).

What is the Q-ARM Functional Prototype?

The Q-ARM Functional Prototype delivers the following functionality:

- Interpreting and using the information on quantum technologies that is generated by the QTT.
- Creating representative models of the energy network assets.
- Interpreting those models and comparing them to information from the QTT, to highlight vulnerabilities.
- Presenting a hierarchy of risks to the modelled assets, from the quantum threat.
- Suggesting appropriate mitigations to lower the presented risk.

The ultimate output from the Q-ARM tool is a risk report that highlights the quantum-enabled risks associated with the energy network system of interest (the latter being an input provided by the user). The Q-ARM Functional Prototype provides the 'back-end' calculations and mapping that enables automation of this risk identification process. This automation will make the exercise of prioritising systems to be upgraded much more scalable.

For the first time, Q-ARM will enable the systematic identification of quantum-enabled risks to the energy network. If the Q-ARM tool is adopted into BAU, the tool will be used to inform decisions that are both economically significant and strategically important for the resilience of energy provision.

In the Alpha phase of this project, the team has therefore sought to de-risk the future development and use of the tool using prototyping to implement and explore the highest risk features first. By generating algorithms and data representations that can be applied to test cases we have validated the effectiveness of these algorithms and data representations. Our definition of 'highest risk' encompassed both significant technical complexity risks, and significant organisational impact risks.

Prototype Development Process

The development of the functional prototype was undertaken using the following product development process, which is discussed in detail in the sections below:

1. Specify requirements and prioritise features.
2. Basic functionality prototype.
3. Test case development and implementation.
4. Stakeholder demonstration and review.
5. Additional feature development and test case update.
6. Stakeholder demonstration and review.
7. Reporting and roadmap assessment.

Specifying Requirements and Prioritising Features

The Q-ARM functional prototype requirements were generated through both workshops and analysis. Key stakeholder groups were identified, and requirements were generated for each of those groups. Note that we may extend the types of stakeholders considered, in the Beta phase of the project. For example, end users of the systems of interest, such as energy network control room staff, could also be important stakeholders whose requirements should be included.

Stakeholder type (or group)	Description
Risk manager	Security personnel with responsibility for assessing and communicating risks, selecting mitigations, and communicating risks to system owners.
Threat analyst	Responsible for modelling the system of interest and ensuring that the model data is correct.
Chief Information Security Officer (CISO)	Has ultimate responsibility for the security of the organisation's assets.
Data, Digital and Technology	The DD&T group within the organisation has the responsibility to ensure that only trusted tools are deployed within the IT estate, and to prevent malicious software being embedded as part of the installation process.
Board	Highest level decision makers within an organisation.
Risk team	The wider risk team (outside of the risk manager); have an interest in the latest information about quantum-safe mitigations and the levels of risk associated with algorithm types.
System owner	Responsible for maintaining the real system of interest.

Stakeholder type (or group)	Description
Head of delivery or budget holder	Has budgetary responsibility for engineering works.
Control owner	Responsible for a specific security control, such as an authentication platform or encryption software.
External stakeholders	Various, including OFGEM and UKRI, electricity and gas Transmission Owners (TO's), Distribution Network operators (DNOs) and Distribution System Operators (DSOs)as well as energy sector special interest groups such as the E3CC.
Third party suppliers	Provide the technologies that form the system of interest.
Consumers	Energy consumers are the ultimate funders for this work.

Table 1: Stakeholder groups that we analysed in order to generate requirements for the prototype

The team evaluated each potential requirement for inclusion within the prototype. "Must have" requirements were those that define a core feature of the tool that is essential for the purpose of identifying quantum risks for energy assets. Requirements that were considered high risk (processes that have not been implemented before) were also considered "must have", to ensure that by including them in the prototype development, we were reducing the development risk for the (eventual) final Q-ARM tool. Requirements that only improved usability or widened the acceptance of the tool were labelled as "nice to have" for the prototype. Features that were deemed to be time-consuming, but not ultimately beneficial to see for the prototype, were deemed "not required for this phase".

At the end of the Alpha phase, all 14 of our identified "must have", three "nice to have", and two "not required for this phase" requirements were implemented (see Appendix D: Details of the Functional Prototype Development, below). We prioritised requirements based on:

- Indicated priority based on interactions with energy sector representatives.
- Discoveries during the implementation process.
- Available resource.
- Estimated effort to implement.

Appendix D provides full details on the requirements capture and implementation. Highlights of de-risked features include:

- The Q-ARM will generate a representation of the quantum-enabled risks that are associated with the assets that are within the System of Interest (SoI).
- The Q-ARM will allow the user to identify the likelihood and impact of the identified risks using a qualitative method that is compatible with NIST SP800-30.
- The Q-ARM will estimate risk likelihood using time-to-attack, and time-of-attack data provided by the QTT and data about the type of attack being assessed.
- The Q-ARM will allow assets and key features (such as data types, cryptographic features, and data property failure impacts) of the SoI to be described and stored within the model.
- The Q-ARM shall allow users to query the level of risk for a quantum-enabled attack at a particular point in time (e.g. in 2034, 2044 etc.).

Prototype Architecture

We generated a prototype architecture for the Q-ARM functional prototype, based on the identified requirements. The architecture highlights the functions that the tool needs to execute; and the data artefacts required by those functions as inputs or generated by those functions as outputs. The architecture was designed to ensure we could deliver all the key requirements identified, and that the tool would be adaptable and scalable for future development.

The architecture is provided in Figure 2 using the following colour-coding:

- Functions (or functional groupings) are in light blue.
- Artefacts generated by the Q-ARM tool are in red.
- Configuration data that can be edited by the user is in orange.
- Configuration data that should only be edited by the tool developer is in light green.
- External data from the QTT is highlighted in purple.

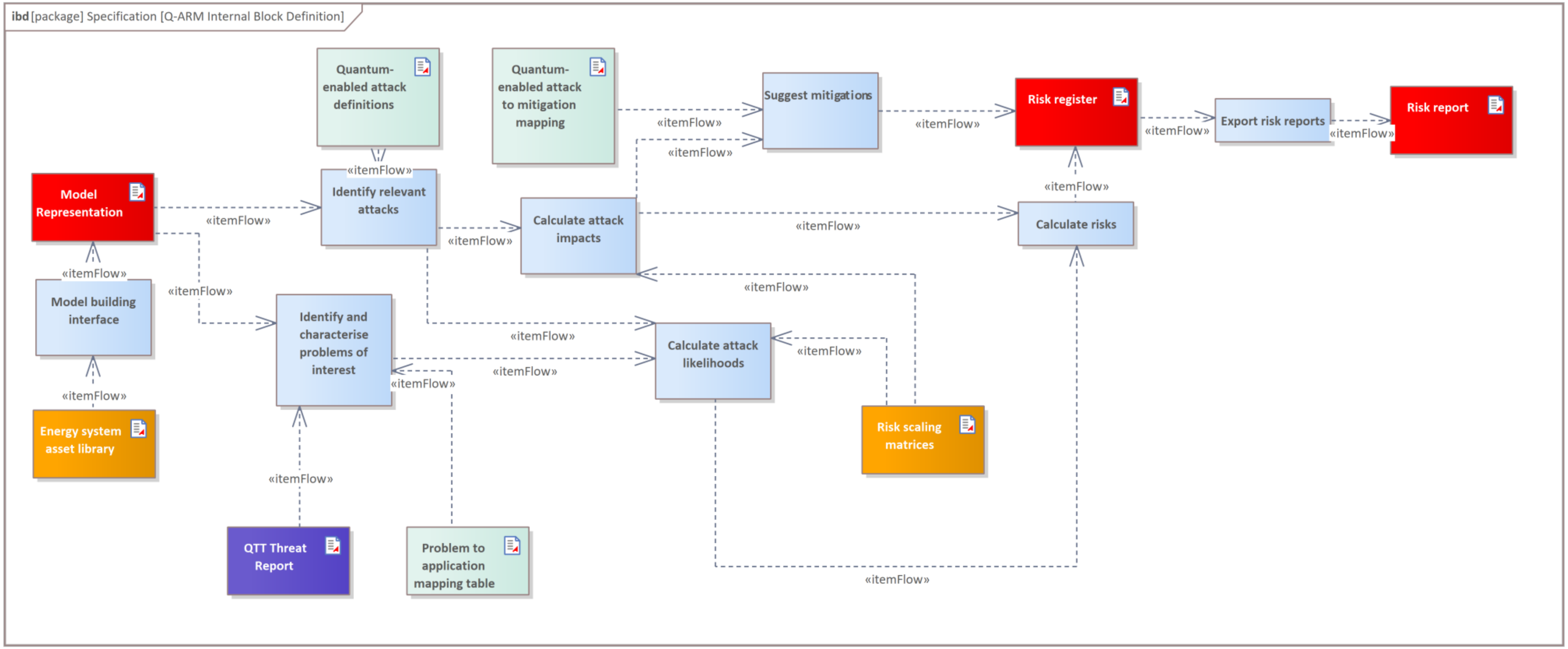

ibd [package] Specification [Q-ARM Internal Block Definition]
Quantum-enabled attack definitions
Quantum-enabled attack to mitigation mapping
Suggest mitigations
Risk register
Export risk reports
Risk report
Model Representation
Identify relevant attacks
Calculate attack impacts
Calculate risks
Model building interface
Identify and characterise problems of interest
Calculate attack likelihoods
Energy system asset library
Risk scaling matrices
QTT Threat Report
Problem to application mapping table
«itemFlow»

Figure 2: Information architecture of the Q-ARM tool (Functional prototype architecture)

Development Environment for the Q-ARM Functional Prototype

Following the development of an outline architecture, the team decided to use Excel/VBA as the development environment for the proof-of-concept tool. The rational was to enable speed of testing and accessibility for end users, and to ensure there was flexibility to integrate easily with third party applications (e.g., the QTT). For more details, please see Appendix D.

In Beta, our plan is that the Q-ARM tool will be developed as a standalone piece of software (not an Excel plugin) using a more rigorous software quality process. This strategy will also allow the UX design to be combined with the required functions.

Characterising Quantum-Enabled Attacks

For the Q-ARM tool to be able to identify quantum-enabled risks to cybersecurity, it must understand clearly how specific cryptographic software can be targeted by quantum computers. To do this in a systematic and future-proof way, the team decided to identify quantum-enabled extensions of the Tactics, Techniques and Procedures (TTPs) used by threat actors.

To do this, we used the TTPs provided in the MITRE ATT&CK Framework. This is a well-established, open knowledge base that was created from analysis of cyber attacks that have previously been launched by adversaries. It is used internationally to create threat models that apply to many sectors, including energy.

The MITRE ATT&CK Framework is used by security teams to:

1. Identify detection strategies for common techniques used by adversaries.
2. Structure threat intelligence using the TTPs as a framework to describe attacks in the wild.
3. Describe the strategies that adversaries use to target systems for testing and security exercises.
4. Compare security defences to TTPs to identify gaps or weaknesses.

Note: More information can be found on the MITRE ATT&CK website's "Getting started" resources: https://attack.mitre.org/resources/ .

The MITRE ATT&CK Framework does not currently specify anything about quantum. To ensure compatibility of the Q-ARM tool outputs with MITRE's ATT&CK Framework, and avoid missing quantum-enabled attack vectors, we reviewed TTPs from the framework that adversaries could enhance using a cryptographically-relevant quantum computer.

We used the following methodology:

1. Identify all mitigations that are associated with classical asymmetric cryptography (highlighted as the cryptography most at risk from quantum-enabled attack during Discovery).
2. Identify all Enterprise and ICS attack techniques from the ATT&CK Framework that are currently countered by the defences from step 1.
3. Evaluate each technique from step 2 and discard techniques that are not enhanced by the adversary having access to a quantum computer.
4. Group all remaining techniques into attack families that can be used for automated risk identification.
5. The Enterprise and ICS frameworks were selected as they represent the vast majority of assets within the energy sector that require active management to migrate to PQC. The mobile device profile was considered out of scope for this phase.

Details from this analysis can be found in Appendix A.

The four types of quantum-enabled attacks we derived from the analysis are as follows:

- **AT1: Decrypt confidential data** – The adversary intercepts the asymmetric key exchange and subsequent data in transit between two legitimate parties. A quantum computer derives the private key from the public key and the adversary uses that private key to identify the session key and subsequently decrypts the data. This includes harvest now, decrypt later attacks.
- **AT2: Content injection** – The adversary intercepts the asymmetric key exchange between two legitimate parties. A quantum computer derives the private key from the public key and the adversary uses that private key to identify the session key. The adversary encrypts their own commands and transmits them to one entity posing as the other.
- **AT3: Forge authentication certificates** – The adversary accesses the published public key of a certificate belonging to an entity that they wish to impersonate. A quantum computer derives the private key of that entity allowing the adversary to forge authentication certificates. This forms the foundation of an attack that allows the entity to gain remote access to protected systems.
- **AT4: Forge code signing** - The adversary accesses the published public key of a trusted software supplier. A quantum computer derives the private key of that supplier allowing the adversary to sign malware and make it look like it comes from the trusted software supplier. This bypasses validation designed to prevent malicious software from running on secure systems.

In the Q-ARM model, the first three attacks target *authenticated connections*. The final attack specifically targets *certified software*. The risk forecast table is generated by identifying vulnerable assets in the inputted model representation, iteratively compiling a list of associated risks.

Every attack was assigned a STRIDE profile based on Microsoft's STRIDE threat model. STRIDE involves assessing if the attack constitutes[1]:

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service (DoS)
- Elevation of privilege.

Each attack we have identified could potentially constitute multiple STRIDE attack profiles (see Glossary for definitions of these attack types).

Additionally, we established a set of potential mitigations, each applicable to multiple attack types. By mapping mitigations to corresponding attack types, the risk forecast provides a tailored list of suggested mitigations for each identified risk.

Dynamic Risk Scaling

A large and varied number of organisations keep the energy sector working. Those organisations are free to pick their own definitions of risk, and their own risk tolerances. For example, the risk scaling for a nuclear reactor is likely to be very different to that of a solar farm. For the Q-ARM tool to be universally applicable to all energy networks, the risk metrics used by the tool need to be parameterisable by the organisation using the tool, in order to best fit their way of working.

For the Q-ARM proof-of-concept, qualitative risk metrics were applied. There is some debate in the cyber security community about the pros and cons of qualitative risk measurements over quantitative risk measurements. While quantitative risk is generally preferable when there is sufficient data, when it is sourced from speculative expert knowledge, applying quantitative metrics can create a false sense that the data is more certain than it is. More advanced techniques to apply metrics to the level of uncertainty exist (also estimated), but these can result in the need for advanced statistical techniques that are outside the scope of this prototyping activity.

Within the Q-ARM functional prototype, all likelihood, impact, risk matrix, and risk acceptability data are configurable by the user (which would normally be done at

[1] Further definitions provided in Section 7. Glossary

organisation level); and these factors then affect the scales used by the tool to identify risk.

For the likelihood definitions, the scale from NIST SP800-30 is suggested by default. The descriptions for the qualitative labels are also taken from NIST SP800-30. They are given in Table 2.

Likelihood label	Label description
Very high	Almost certain
High	Highly likely
Moderate	Somewhat likely
Low	Unlikely
Very low	Highly unlikely

Table 2: Default 'likelihood of risk' scale used by the Q-ARM Functional Prototype tool (Note: this is configurable by end users to fit their organisation's own risk scales)

For the impact definitions, the scale from NIST SP800-30 is suggested by default, though the specific impact descriptions are currently not filled in as they should always be generated by the organisation using the tool. The scale is a simple five-point scale from Very high to Very low, using the same labels as the likelihood scale.

For the risk matrix relationships, the standard values from NIST SP800-30 are provided by default and are given in Table 3.

Likelihood	Impact severity				
	Very low	Low	Moderate	High	Very High
Very high	Very low	Low	Moderate	High	Very High
High	Very low	Low	Moderate	High	Very High
Moderate	Very low	Low	Moderate	Moderate	High
Low	Very low	Low	Low	Low	Moderate
Very Low	Very low	Very low	Very low	Low	Low

Table 3: The default risk matrix used to relate likelihood and severity for risk classification by the Q-ARM functional prototype

A risk acceptability scale is not included within NIST SP800-30, so a provisional scale was developed for this project. This scale is not the risk scale used by any consortium members and is deliberately original to avoid leaking confidential information about risk management. It is found in Table 4.

Risk level	Action statement	Acceptance criteria
Very high	Unacceptable risk. Risk must be managed (ideally mitigated or avoided). May require multiple mitigations to drive down to acceptability.	None
High	Risk unlikely to be tolerated. Risk shall be managed (mitigated, avoided or transferred). May require multiple mitigations to drive down to acceptability.	Only with senior sign off
Moderate	Risk unlikely to be tolerated. Risk shall be managed (mitigated, avoided or transferred).	Only with senior sign off
Low	Tolerable risk. Should be driven down if cost/benefit is favourable.	Acceptable with justification
Very low	Tolerable risk.	Acceptable

Table 4: The default risk acceptance table used by the prototype

Model Representation within the Q-ARM

For the final, fully-developed (Beta/BAU) Q-ARM tool, the energy system modelling interface that users will employ to create models of their own energy network assets will be mostly designed as a drag-and-drop interface. This user interface is described below in Section 4. However, regardless of the user interface, an underlying digital representation of each energy system is needed that can be used for automated machine analysis of the specific risk.

The Q-ARM tool uses the concept of "Generic assets" for high level concepts, and the data required to describe each asset varies by that type. A description is shown in Table 5. The applicable attack labels are aligned with the descriptions provided in previous sections.

Generic asset name	Description	Applicable attacks	Parameters required to define asset
Authenticated connection	A connection between two entities (typically computers) that is both encrypted and uses authentication to verify the	AT1, AT2, AT3	Key rotation/certificate frequency, Key length, Latency requirement, Bandwidth requirement, data transmitted

Generic asset name	Description	Applicable attacks	Parameters required to define asset
	identities of the entities to each other.		
Certified software	Software that is checked using a digital signature to ensure that it comes from a trusted source.	AT4	Confidentiality impact, Duration of confidentiality, Integrity impact, availability impact
Computer	Generic placeholder for assets that can execute software or communicate over networks.	None	Authentication impact
Data	Generic type for describing data that is stored or transmitted by the system.	None	Confidentiality impact, Duration of confidentiality, Integrity impact, availability impact
Unauthenticated connection	A connection between two entities (typically computers) that does not use any form of cryptography.	None	None

Table 5: Generic data types used by the Q-ARM tool. (parameters in bold are mandatory; others are not mandatory but can be used to enhance the analysis)

Note that only quantum attacks are listed; "classical" cyber-attacks are out of scope for this tool, which is why some assets shown have no attack types, despite being vulnerable to classical attacks.

Test Case Performance Testing of the Q-ARM Functional Prototype

The risk forecast output of the Q-ARM functional prototype is dependent on several configurable inputs. These are: the model representation of the target system, the energy network's risk appetite, and the snapshot 'target date' entered by the user which sets the period for the risk analysis.

We created two 'test cases', representing systems within the energy network, for the purpose of development and testing. Each test case consisted of a single energy system. The date (target year to assess quantum vulnerability of the system) of risk evaluation for the Q-ARM analysis was left as a variable, to enable us to explore how the risk profile of the systems changed over time.

This was used to ensure the tool was able to analyse systems that were of genuine interest to the energy network rather than generating a generic tool for all quantum threat assessments.

- Test Case 1 models the relationship between a grid balancing system and an energy generator communicating bids, offers, and acceptance data. The analysis of that system can be found in Appendix B.
- Test Case 2 models the relationship between forecasting data providers (weather, energy consumption prediction etc) and a control centre. The analysis of that system can be found in Appendix C.

Both test cases yielded useful results, that correctly applied the defined attack against the system of interest, and classified the risks according to the selected risk profile. We did not specify a hard time requirement for the Q-ARM functional prototype to execute the analysis of each test case, for this phase. For the more complex test case (Test Case 2) the execution time was consistently approximately 0.2s. This is an acceptable performance from a usability perspective and is likely to improve when the analysis algorithm is implemented in a different programming language.

4. UX Design Prototype Workstream: Development and Outputs

Early within the Alpha phase, it became clear that a functional prototype of the Q-ARM tool could be technically effective, but did not capture the imaginations of users, nor did it inspire detailed discussions about how the Q-ARM could be embedded into the day-to-day activities of its intended users.

The project team therefore decided that a user interface for the demonstrator was required, to act as an interactive clickable demo to illustrate how target users might interact with the Q-ARM tool. This is referred to as the Q-ARM UX Design prototype, or the 'clickable demo' below.

The clickable demo enabled us to:

1. Collect feedback from users and other stakeholders to learn what tools and features are most beneficial to them.
2. Assess how the tool might be integrated into their workflows.
3. Optimise system usability to ensure the quantum risk forecasting process is quick and easy to operate by the target user groups.

The UX Design Prototype can be shared with potential users as a cloud-hosted link, to demonstrate intended functionality and collect user feedback.

Development approach

Working closely with the partners, the team built the clickable demonstrator using rapid iterative development cycles across the following process:

1. **Workshop to capture user needs** – An interactive session where NESO worked alongside team members from CC and the University of Edinburgh to outline stakeholder needs and user requirements.
2. **Mapping of the user workflow** – A talk flow analysis of desired user steps, simplified to reduce number and complexity of steps to achieve the simplest and most intuitive workflow for users.
3. **Building a clickable wireframe demo** - An early clickable prototype without final colour materials and finish (CMF), created to collect feedback from NESO stakeholders.
4. **Building a clickable mock-up demo** - Developed a higher fidelity clickable prototype for user feedback. This was an interactive visual mock-up of how the Beta system might work to help us assess usability, what users find most useful and communicate the future vision to stakeholders.
5. **Gathering user feedback** - Created an accompanying questionnaire to collect user feedback during testing of the interactive visual mock-up. This document was

supplied with a link to the interactive visual mock-up to help guide users through a quantum risk forecasting workflow from setting up a model to outputting data and a report.

This approach has confirmed that stakeholders, especially potential users, are bought into the value of the Q-ARM tool, while providing additional feedback and inputs to support continued refinement of the user experience in a future phase.

Clickable Demonstrator Design and Development

The clickable demo demonstrated a subset of the overall tool features representing the core user workflow. This allowed us to visualise and test a large proportion of the user experience for the Q-ARM while other pages and features were deprioritised.

By the end of the Alpha phase, the mock-up included the following high fidelity exemplar pages:

- Dashboard.
- System modelling.
- Quantum risk forecast.
- Reporting.

The interface itself enables users to leverage the insight generated by the QTT to quickly and easily evaluate quantum threats and output reporting to review with stakeholders and ultimately take action to secure the system.

The prototype is not a fully functional system; rather, it is a representation of the user interface, therefore not all features are fully operational.

Quantum computing is a complex and highly technical subject; our team wanted to counteract this technical barrier by making the tool accessible and frictionless for energy sector end users.

The development of the clickable demonstrator revealed several usability challenges that the Q-ARM must overcome to effectively deliver value to users. These challenges included:

1. **Accurate and intuitive communication of quantum risk forecast confidence levels.**

   Needed in order to support users with decision making and mitigation selection.

   Addressed by the QTT Update workflow (a button that lets the user instantly pull in the latest updated tech information from the QTT, to inform the analysis), and the creation of a ‘confidence graph’ to help aid trust and explainability.

2. **Accurate and easy to understand representation of impact of proposed quantum mitigations.**

   We developed the idea of plotting risk on a histogram and updating this graphic with 'risk after proposed mitigation' as a 1:1 comparison of risk before and after mitigation. This approach seemed to be clear and familiar to users and received good feedback from stakeholders.

3. **Clear naming conventions for each step of the user journey, for easier usability.**

   The tasks performed by the user within the tool can be found on different tabs; we have called these 'Models, Quantum Risk Forecast and Reporting' as an intuitive and easy to understand series of steps to help users progress from building a system model to generating the risk forecast and generating a report.

We also defined the risk assessment as a 'forecast' to indicate it is a future prediction.

Below is an example of the developed demonstrator, followed by a summary of key development aspects and example snapshots from the clickable demo. Further detail on the full demonstrator can be found in Appendix E.

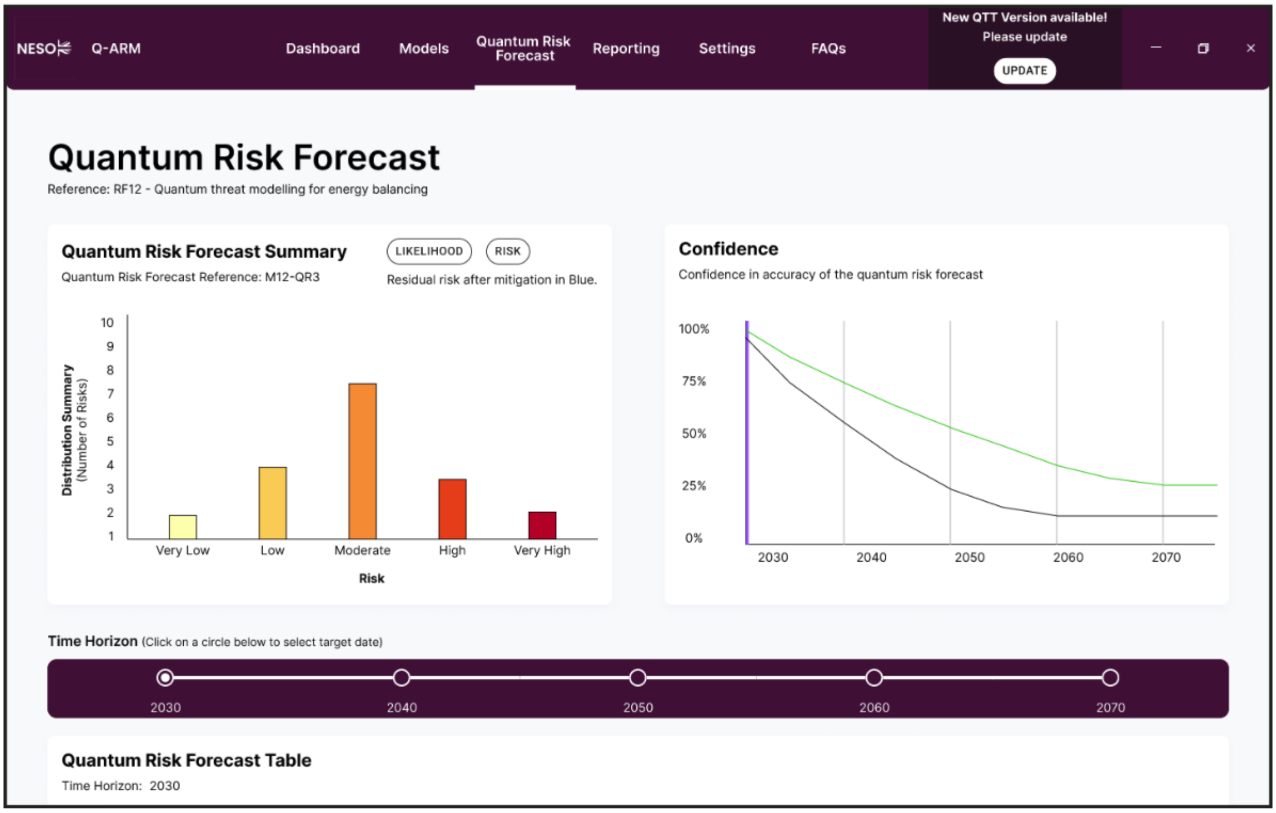
Quantum Risk Forecast Page

This page summarises the quantum risk forecast for the chosen model, allowing users to evaluate the data.

On the top left we have a histogram plotting number of risks against severity. In its current state, this tells you what would happen if no action was taken.

On the top right we have a confidence graph, which shows how confidence in the accuracy of the quantum risk forecast changes as we look further into the future.

The time horizon selector allows you to explore how the risk profile changes over time.



New QTT Version available!
Please update

Quantum Risk Forecast

Reference: RF12 - Quantum threat modelling for energy balancing

Quantum Risk Forecast Summary

Quantum Risk Forecast Reference: M12-QR3

Residual risk after mitigation in Blue.

Confidence

Confidence in accuracy of the quantum risk forecast

Time Horizon (Click on a circle below to select target date)

Quantum Risk Forecast Table

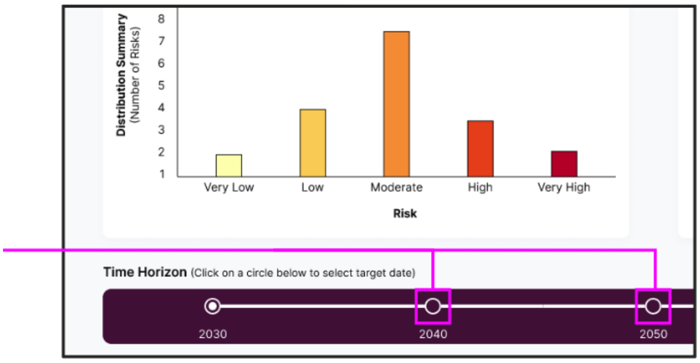
Time Horizon: 2030

On the top left we have a histogram plotting the number of risks against severity. In its current state, this tells you what would happen if no action was taken.

On the top right we have a confidence graph, which shows how confidence in the accuracy of the quantum risk forecast changes as we look further into the future.

The time horizon selector allows you to explore how the risk profile changes over time.

Clicking the small white circles on the time horizon scale lets the user move through different time horizons, with risks or likelihood values changing accordingly. In future versions of the tool, the risk forecast table and confidence graph will also update as the user navigates through different time horizons.



Time Horizon (Click on a circle below to select target date)

Key Learnings:

- We identified the importance of clearly communicating when the QTT database is out of date and requires an update. This action is central to ensuring quantum risk forecasts are as accurate as possible by using the latest estimates of quantum computing developments. In the current update workflow, a large white button appears on the navigation bar, encouraging users press this before progressing any further. In the fully functional version, we could use a warning pop-up to check if a user wishes to proceed if a new QTT update is available.

- The software interface must provide a simple, intuitive interface to model a wide variety of complex systems. This is specifically challenging for modelling the energy network due to the different fidelities of systems and wide range of energy sector-specific default assets that need to be modelled. Furthermore, we need to provide flexibility for users to create their own custom assets as this information is considered sensitive and not easily sharable for security reasons.
- A histogram plot combined with confidence graphs seems to be the most appropriate approach to communicate the quantum risk forecast summary.
- The tool needs to allow for multiple methods of extracting information based on the target audience, and must fit with existing reporting styles or templates so it does not create a hurdle for their use in BAU.

Feedback from Users

By testing prototypes with users, we identified several improvements to features that improved usability and how the workflow could be further optimised. These have all since been implemented in the clickable demo, but not implemented in conjunction with the functional prototype.

Details of these feedback points and how we addressed them in the clickable demo can be found in Appendix E.

5. Future Work

Key Discoveries from Alpha

In the Alpha phase, through developing the Q-ARM demonstrator, we have increased our confidence that the Q-ARM can become a powerful tool to support energy network risk analysts and threat managers in the mitigation of quantum threats to the energy sector. We have also demonstrated that the Q-ARM tool can integrate with - and draw the relevant quantum technology information from – the QTT (see "Proof-of-concept development of Quantum Threat Tracker (QTT) tool for the energy sector" for the Alpha phase report on the QTT for more details).

This work has led to the following key discoveries:

Workstream	Description	Impact
Functional prototype	We have templated a methodology for describing an abstract energy system into a machine-readable format (using an adjacency matrix).	We have a scalable template for translating the modelling of systems into an operational tool.
	We have automated the process for calculating and presenting risk based on a combination of information provided by the QTT and the modelled energy system, and presented this in a risk register familiar to target users.	We have created an algorithm that can be translated from the functional prototype to a deployable software package, addressing one of the highest risks identified at the start of Alpha.
	We have automated the recommendation of appropriate mitigations, evaluating the corresponding impact on risk, and presented it in a risk register familiar to target users.	
UX design prototype (clickable demo)	We have identified a logical workflow that allows users to build a system model, generate and analyse a quantum risk forecast and output data and a report.	We have collected positive feedback from NESO stakeholders. We have an easy to understand and compelling demo that can be shared with other entities in the energy sector.

Workstream	Description	Impact
	We have received some initial feedback on the value of features and system usability.	Builds confidence in the value and usefulness of the tool to target users.
	We have started validating some of the novel user interactions on the Q-ARM such as the Quantum Risk Forecast and applying mitigations.	This adds confidence in the value of the tool and starts to de-risk some of the most novel and therefore challenging barriers to user adoption.
	We have identified many open questions and next steps to help us build a plan for further development.	We have developed our understanding of UX challenges, enabling greater visibility of the path to pilot and launch.

Table 6: Key discoveries through Alpha

Backlog of Features for Future Development

Some features and requirements that we identified in the workshop, analysis, and user feedback sessions have not yet been implemented in the Alpha prototype. We propose to develop these during the Beta phase. A summary of those features is provided in Appendix F.

Development Roadmap for Beta

The proof-of-concept demonstrator has provided confidence that the technical challenges identified within Discovery can be addressed. Alpha phase work has also provided additional steer for the development of an effective user interface.

As this tool will inform security decisions, the full development of the tool in Beta must be planned with quality assurance in mind, including a plan for structured testing. The software quality plan for this phase was adequate for proof-of-concept prototyping, but will need enhancing to deliver a trustworthy tool.

The high-level next steps are to bring the learnings into a deployable Q-ARM tool, alongside the development of the QTT and then to integrate this into BAU for energy network operators.

Our initial view on a proposed development roadmap is proposed in Table 7:

Stage	Task	Description
1 – Full Tool Requirements Capture	Requirements Workshop	Creation of drafted requirements specification (including both functionality and deployment) and review with stakeholders from energy networks. Categorising of common / unique requirements across stakeholders and feature prioritisation.
	Requirements Issue	Issue of prioritised requirements document for stakeholder review and acceptance.
	UX Development	The existing interface has been primarily developed with feedback from NESO stakeholders. Hold an interface development workshop to assess existing usability features with a wider set of stakeholders and identification of new user requirements / functionality not already explored for stakeholders within different energy networks.
	Long Term Support Requirements	Selection of long-term support strategy (determination of who is responsible for bug fixes, feature requests, maintenance, etc., across the product lifetime).
2 – Q-ARM and QTT Deployable Tool Development	Agile Software Tool Development	Series of sprints to develop features from requirements capture. Includes implementing user stories, refining backlog and sprint retrospectives.
	Stakeholder Feature Review	Periodic feature review with stakeholders including demonstrations. Includes requirements review.
	System Demonstration and Documentation	Demonstration of developed system in development environment with stakeholders and users. Complete user guide documentation.
	Generic Tool User Acceptance Testing	Final review of generic tool with users ahead of phased deployment to energy networks. Option to proceed with generic tool or to complete unique feature requirements.
	Unique Feature Development	Additional sprints to develop unique features / customisations for energy networks.

Stage	Task	Description
	Customised Tool User Acceptance	Final review of customised tool with users ahead of phased deployment to energy networks.
3 – Pre-Deployment Testing	Staging Environment Setup	Setup of pre-deployment environment at energy networks. This may be completed in parallel with Stage 2.
	Install Q-ARM	Install of the Q-ARM tool in the non-production space, connecting to the QTT tool.
	Training and User Testing	Initial training of users and free testing window to report bugs.
	Support Sprints	Sprints targeted around bug fixes / capturing larger feature requests.
4 – Tool Deployment	Deploy to Business as Usual	Install Q-Arm on energy networks' production space and begin live operation.
	User Training Sessions	Additional user training sessions at energy networks as required.
5 – Deployed Tool Support	Setup Ongoing Support	Collect user feedback, address bugs and feature requests, essential maintenance, etc., through business as usual.
	Customisation to new users	Development of custom instances of the tool for new members of the energy network (and perhaps beyond).

Table 7: Provisional development roadmap

Frequent user engagement will be required throughout to ensure that the user interface is as easy to use as possible for the security teams wishing to apply it.

Additional energy sector assets to embed into the tool as default options will also be created.

6. Conclusion

Alpha Phase Delivery

NSiaQF Alpha Phase has delivered several innovations in the Q-ARM tool development:

- **We have developed an innovative quantum risk analysis process.**

  As outlined in Discovery, most quantum risk assessment techniques assume that the time until a cryptographically relevant quantum computer is built is the only factor that needs to be considered when assessing attack risk. In fact, this time is variable for different algorithms and key sizes, and the amount of time it takes a quantum computer to launch an attack has a large effect on the types of attack that can be launched.

  Our innovative approach, developed and demonstrated in Alpha, also takes into account the amount of time that data needs to remain confidential, and the lifetimes of certificates and keys. This lets the tool build a more detailed picture of quantum risk and will enable energy networks using the tool to more effectively prioritise which systems require migration.

- **We have developed a clear and innovative approach to characterising quantum-enabled attack types.**

  To the best of our knowledge, this project is the first time that TTPs have been extended to include a complete definition of the attacks that quantum computers can enhance in a format that is widely used by the security community. This is important because it will enable both the functionality of the Q-ARM tool, and the ability of energy network security teams to incorporate this information into their BAU risk analysis (since TTPs are widely used for this).

- **We have integrated several different areas of expert knowledge to feed into the Q-ARM tool by mapping key links between cyber security and quantum computing domains.**

  The Q-ARM tool brings together a unique combination of functionalities that have not previously been integrated into a single tool. One key innovation was that we created three significant mapping tables that enable the automation of quantum risk identification within the tool:

  - Mapping connections between mathematical problems that quantum computers can solve and software libraries that security professionals are familiar with.
  - Mapping quantum attacks to the mitigations that protect against them.

- Mapping between quantum attacks and the security properties that they undermine.

The functional prototype for the Q-ARM tool is the first time that these disparate areas of key quantum and cybersecurity information have been explicitly brought together. Doing this is important to inform the tool's analysis process, as these links are key to prioritising which software is the most pressing to upgrade to be quantum-safe. This is highly valuable and has applications outside of the energy sector.

However, to remain valid going forward, these mappings will need to be validated, kept up to date, and expanded with more information for security teams.

- **We have created an architecture that allows the creation and storage of energy asset models for sharing (and for use in creating system models).**

  The value that this provides is a common view of such assets for all tool users, and the ability to enable rapid model building through reuse.

- **We have developed and demonstrated an approach to automatically identify the risks posed to an energy system by an attacker using a quantum computer**.

  Once fully developed as part of the tool in the Beta phase, this will enable users to work at scale/significantly more quickly than they would be able to using manual analysis.

- **We have developed and demonstrated an approach to process quantum computing threat intelligence (from the QTT) to perform evidence-based risk analysis based on the latest research into quantum computers**.

  When fully developed (in Beta), this will enable security teams to manage the risks posed to their systems in an informed way.

Work Package Benefits

The specific value of the Q-ARM tool, within the context of the NSiaQF project, is:

- It is designed to make post-quantum readiness assessments of energy network assets relatively simple, scalable and reproducible. This will help to ensure good value for consumers and support network resilience. This will also be particularly important for energy networks, as they work to meet the PQC-readiness timelines for CNI providers that have recently been set out in NCSC's guidelines (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines).
- It will output reports and information that integrate easily with current BAU for energy networks; and provides clear and easy-to-understand outputs that can be shared

with both technical and senior stakeholders. This will support effective decision-making about strategies and investment for quantum readiness.

- It will enable common understandings of energy network asset value (defined as the criticality of the asset to the continuing and resilient delivery of energy services), to be shared across the whole sector. This avoids the cost and effort of duplicated work by individual energy networks, which can keep costs down and improve resilience.
- It will ensure detailed knowledge sharing regarding the quantum threat and associated timelines across the whole sector. This is valuable because, fundamentally, PQC-readiness is not a problem that a single organisation can solve on its own. It requires coordination and a shared understanding of what assets are at risk, when, and what mitigations are appropriate. Also, the field of quantum computing is moving extremely quickly as new discoveries are announced that make the realisation of cryptographically relevant quantum computers more feasible. This methodology allows security professionals to make evidence-based judgements about the risks and to compare them with other cyber security risks and each other.

The Q-ARM tool prototyping activities in this work package have focused on de-risking key aspects of the tool's development and proving the viability of the overall tool both from a technical standpoint (functional prototype development workstream) and a user interface standpoint (UX design workstream).

Specific value points are:

- We have derisked the highest-risk parts of the technical development of the Q-ARM tool, demonstrating that:
  - It is possible to identify risks from a machine-readable representation of energy systems.
  - It is possible to characterise quantum-enabled attacks and map these to energy systems in a meaningful and reproducible way.
  - The Q-ARM tool is technically feasible.
- We have de-risked the usability and utility of the user interface by:
  - Creating user workflows and interfaces using a light-touch wireframe approach, incorporating key learnings on user interactions and effective communication.
  - Creating new features to enhance the utility of the user interface based on stakeholder feedback; such as the creation of the user-controlled risk scaling feature.

- We have maximised the likelihood of stakeholder adoption and buy-in by including key energy network stakeholders in the process of designing the tool; this:
    - Has enabled opportunities (which are ongoing) to provide feedback on features and usability to shape the tool.
    - Maximises the potential for the tool to eventually be adopted as part of BAU for energy networks, ensuring its value is realised.

7. Glossary of Terms

Term	Meaning
Architecture	Outline software design detailing high level input and outputs, including artefacts and configuration data.
ATT&CK Framework	Knowledge base of adversarial techniques created by MITRE based on real-world observations, focussing on how adversaries interact with systems during an operation, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.
Denial of Service (DoS)	Disrupting service availability.
Elevation of privilege	Gaining unauthorized access to higher-level permissions.
Information disclosure	Unauthorized access to information.
NCSC	National Cyber Security Centre
NIST SP800-30	A guide for conducting risk assessments of federal information systems and organizations, providing a structured approach to identify, evaluate, and mitigate risks
Post-quantum cryptography (PQC)	Cryptographic algorithms designed to be secure against the potential threats posed by quantum computers.
Repudiation	Denying actions or transactions.
Spoofing	Impersonating another user or system.
Tactics, Techniques and Procedures (TTPs)	The specific methods and strategies used by adversaries to achieve their objectives in cybersecurity, encompassing the overall approach (tactics), the specific methods employed (techniques), and the detailed processes followed (procedures).
Tampering	Unauthorized modification of data.
Time-of-attack	The estimated year that a quantum enabled attack could realistically occur.
Time-to-attack	The estimated time elapsed for a quantum-enabled attack to break a specific cryptography (from start of

	attack to successful breaking of the cryptographic scheme).
User experience (UX)	The overall experience a person has when interacting with a product, system, or service, encompassing aspects like usability, accessibility, and pleasure derived from the interaction.
VBA	Visual Basic for Applications, a programming language developed by Microsoft that is primarily used for automating tasks in Microsoft Office applications like Excel, Word, and Access

Appendix A – Quantum-enabled MITRE ATT&CK TTPs

MITRE ATT&CK contains 203 Enterprise techniques (with 453 sub techniques) and 83 Industrial Control System (ICS) techniques. Rather than analyse each technique, we identified the five mitigations (out of 44 Enterprise mitigations and 52 ICS mitigations) that related to asymmetric cryptography, and then only addressed the techniques that those mitigations were a defence against:

1. M1041: Encrypt sensitive information (Enterprise)
2. M1045: Code signing (Enterprise)
3. M0808: Encrypt network traffic (ICS)
4. M0941: Encrypt sensitive information (ICS)
5. M0945: Code Signing (ICS)

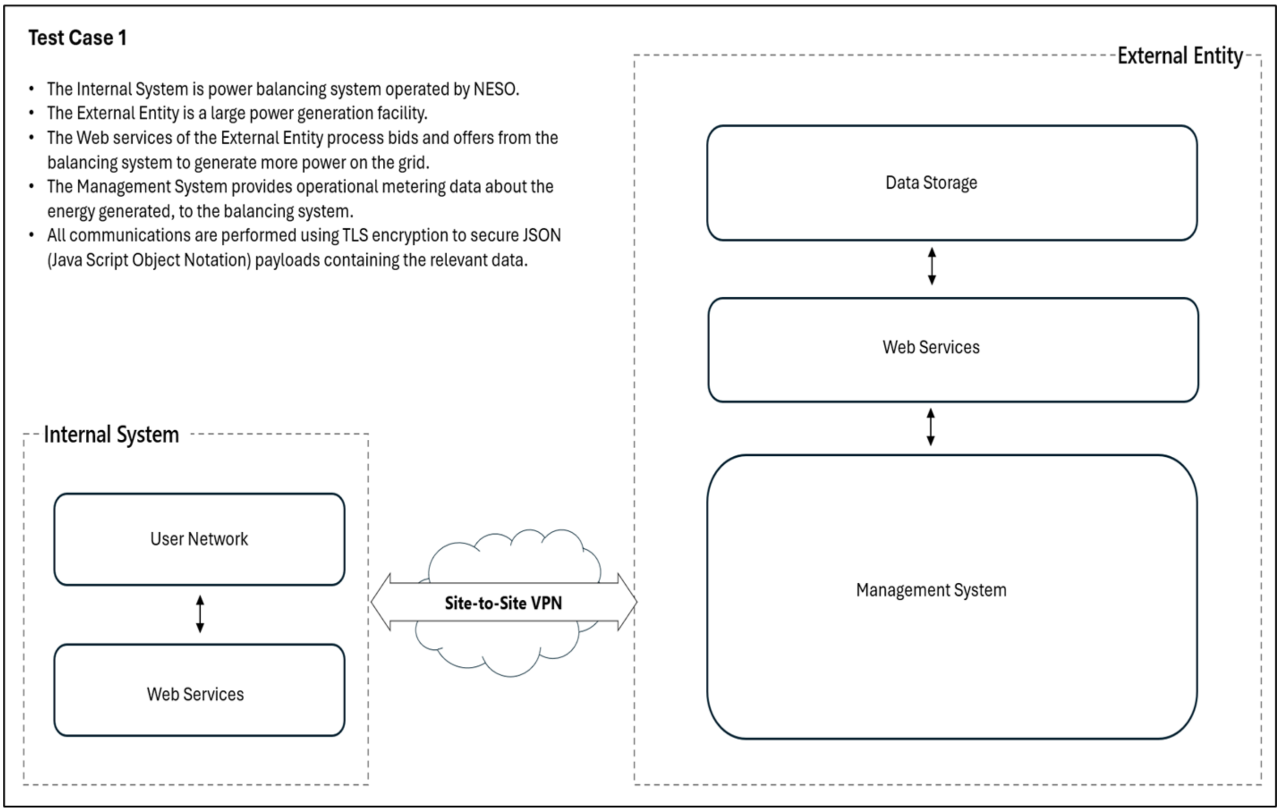
By grouping the affected techniques, we produced just four quantum-enabled attack types that cover a total of 26 techniques that were found to be able to benefit from quantum computers. The resulting attacks (and associated techniques) are as follows:

- AT1 - Decrypt confidential data
  - Covering techniques T1557, T1040, T0842
- AT2 – Content injection
  - Covering technique T1659
- AT3 – Forge authentication certificates
  - Covering technique T1649
- AT4 – Forge code signing
  - Covering techniques T1059, T1554, T1543, T1546, T1525, T1036, T1601, T1505, T1127, T1204, T0857, T0849, T0821, T0889, T0839, T0843, T0873, T0851, T0862, T0857, T0863

Appendix B – Test Case 1

Test case 1 represents the relationship between an energy generator and a control room with responsibility for balancing the grid. Note that all example systems had the constraint of being detailed enough to be usable for validation of the Q-ARM functional prototype, but not so specific as to accurately describe actual operations within NESO (in order to preserve confidentiality and security).

The structure of the test case is given in Figure 3.



Test Case 1

- The Internal System is power balancing system operated by NESO.
- The External Entity is a large power generation facility.
- The Web services of the External Entity process bids and offers from the balancing system to generate more power on the grid.
- The Management System provides operational metering data about the energy generated, to the balancing system.
- All communications are performed using TLS encryption to secure JSON (Java Script Object Notation) payloads containing the relevant data.

Figure 3: Test architecture illustrating a grid balancing system used to demonstrate the prototype

Node definitions					Relevant impacts				
Name	Type	Connection type / Certificate technology	Hosted on (certified software only)	Data transmitted (connection only)	Confidentiality	Duration (hours)	Integrity	Availability	Authentication
Internal system: web server	Computer	-	-	-	-	-	-	-	High
External entity: web server	Computer	-	-	-	-	-	-	-	High
Internal system: web services	Certified software	X.509 Certificates	Internal system: web server	-	Low	Indefinite	Very High	Very High	-
External entity: web services	Certified software	X.509 Certificates	External entity: web server	-	Low	Indefinite	Very High	Very High	-
External entity: management system	Certified software	X.509 Certificates	External entity: web server	-	Moderate	Indefinite	Very High	Very High	-
Bid-Offer-Acceptance (BOA)	Data	-	-	-	High	0.5	High	High	-
Link between internal and external web servers	Authenticated connection*	https (TLS 1.3)	-	BOA	-	-	-	-	-

*The impact is inherited from the data transmitted (i.e. from *BOA* for Link between internal and external web servers).

Table 8: Test Case 1 model representation (node definitions)

For the purposes of the prototype, we used a standard risk scaling matrix from NIST SP800-30. This is used to determine the initial magnitude of each risk based on the calculated likelihoods and severities.

Test Case Results

Below are examples of generated risk forecast tables using the NESO test model and the standard risk scaling matrix for Test Case 1. To determine the performance of the tool, the year 2025 (Table 9) and 2070 (Table 10) are used to see the differing risk profiles for these two years that are generated within the report. The corresponding risk histograms show outputs from the test case risk report in graphical form (Figure 4 for 2025 and Figure 5 for 2070).

These outputs describe the specific quantum-enabled risks that the system is deemed to be susceptible to by the tool and the histograms show the risk profile of the entire system by summarising the number of risks of each level that the tool has generated.

Six quantum-enabled risks were identified for the energy network balancing test case. For both, the “Property Impact(s)” column uses the following abbreviations:

- Auth = Authentication
- C = Confidentiality
- I = Integrity

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
1	Link between internal webserver and external webserver is intercepted and BOA is read as plaintext	• Link between internal webserver and external webserver • Internal system: web server • External entity: web server • BOA	AT1	C	Attacker has access to BOA	High	Very Low	Low
2	Link between internal webserver and external webserver key exchange is intercepted and attacker spoofs either Internal system: web server or External entity: web server	• Link between internal webserver and external webserver • Internal system: web server • External entity: web server	AT2	Auth	Attacker sends malicious messages spoofing either Internal system: web server or External entity: web server	High	Very Low	Low
3	Attacker steals public key used to produce authentication certificate used to authenticate Internal system: web server to External entity: web server or vice-versa.	• Link between internal webserver and external webserver • Internal system: web server • External entity: web server	AT3	Auth	Attacker sends malicious messages spoofing either Internal system: web server or External entity: web server	High	Very Low	Low
4	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Internal system: web services	• Internal system: web services	AT4	I, Auth	Attacker executes arbitrary code in place of Internal system: web services	Very High	Very Low	Low
5	Attacker steals public key for trusted software supplier and digitally signs a malicious patch	• External entity: web services	AT4	I, Auth	Attacker executes arbitrary code in place of External entity: web services	Very High	Very Low	Low

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
	to External entity: web services							
6	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to External entity: management system	• External entity: management system	AT4	I, Auth	Attacker executes arbitrary code in place of External entity: management system	Very High	Very Low	Low

Table 9: Risks automatically identified by the prototype tool for test case 1 (Energy Balancing System), for the year 2025

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
1	Link between internal webserver and external webserver is intercepted and BOA is read as plaintext	• Link between internal webserver and external webserver • Internal system: web server • External entity: web server • BOA	AT1	C	Attacker has access to BOA	High	High	High
2	Link between internal webserver and external webserver key exchange is intercepted and attacker spoofs either Internal system: web server or External entity: web server	• Link between internal webserver and external webserver • Internal system: web server • External entity: web server	AT2	Auth	Attacker sends malicious messages spoofing either Internal system: web server or External entity: web server	High	Moderate	Moderate
3	Attacker steals public key used to produce authentication certificate used to authenticate Internal system: web server to External entity: web server or vice-versa.	• Link between internal webserver and external webserver • Internal system: web server • External entity: web server	AT3	Auth	Attacker sends malicious messages spoofing either Internal system: web server or External entity: web server	High	High	High
4	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Internal system: web services	• Internal system: web services	AT4	I, Auth	Attacker executes arbitrary code in place of Internal system: web services	Very High	High	Very High
5	Attacker steals public key for trusted software supplier and digitally signs a malicious patch	• External entity: web services	AT4	I, Auth	Attacker executes arbitrary code in place of External entity: web services	Very High	High	Very High

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
	to External entity: web services							
6	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to External entity: management system	• External entity: management system	AT4	I, Auth	Attacker executes arbitrary code in place of External entity: management system	Very High	High	Very High

Table 10: Risks, automatically identified by the prototype tool for test case 1 (Energy Balancing System), for the year 2070

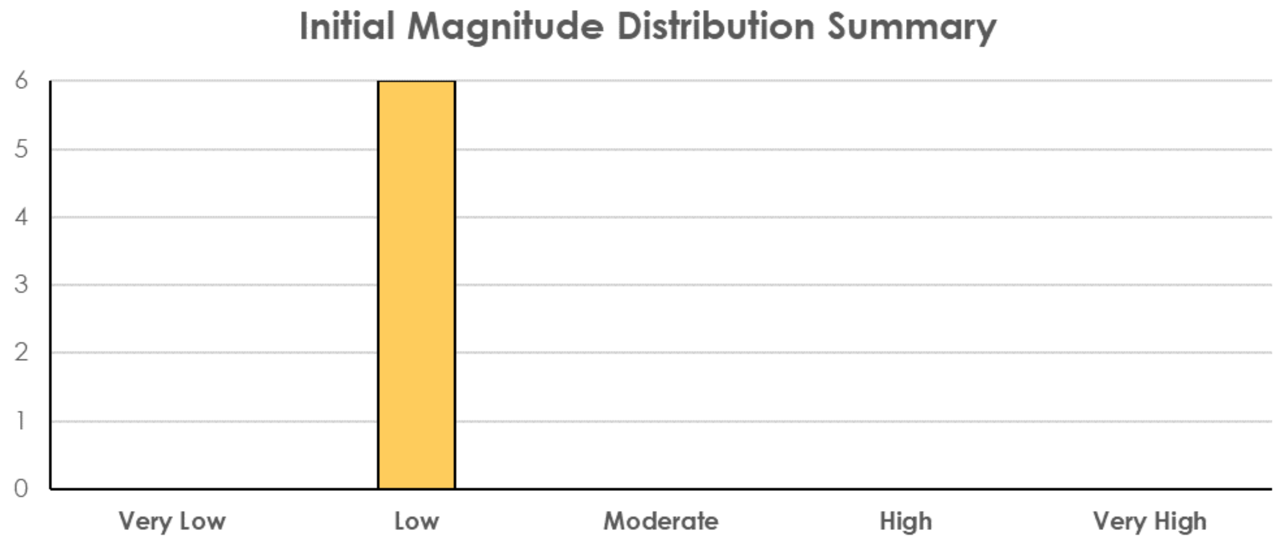


Figure 4: Generated risk histogram for test case 1, 2025

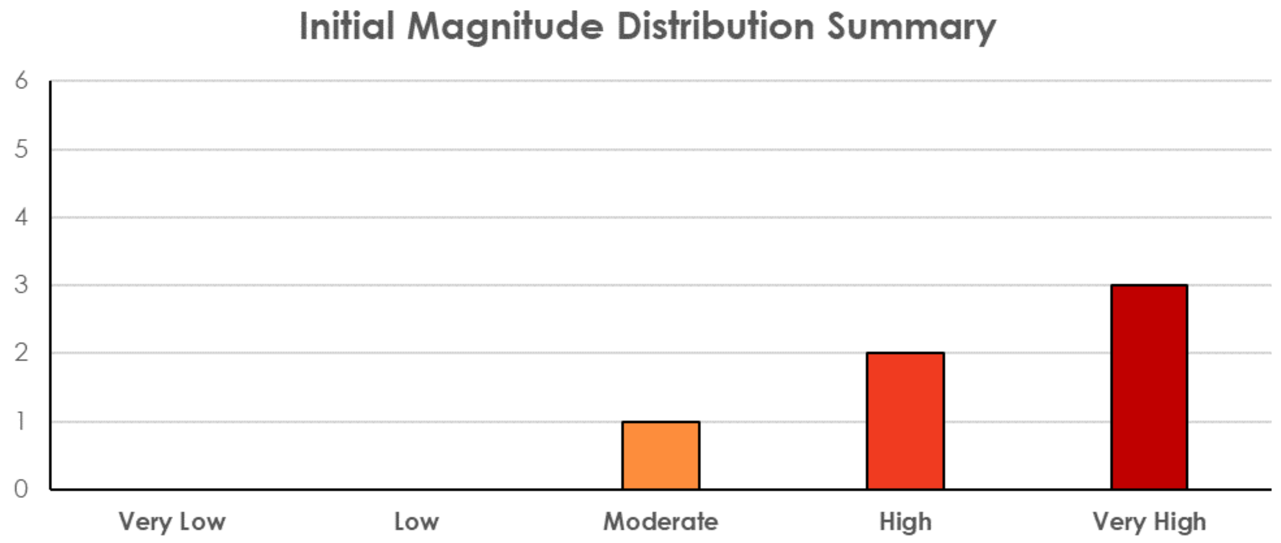


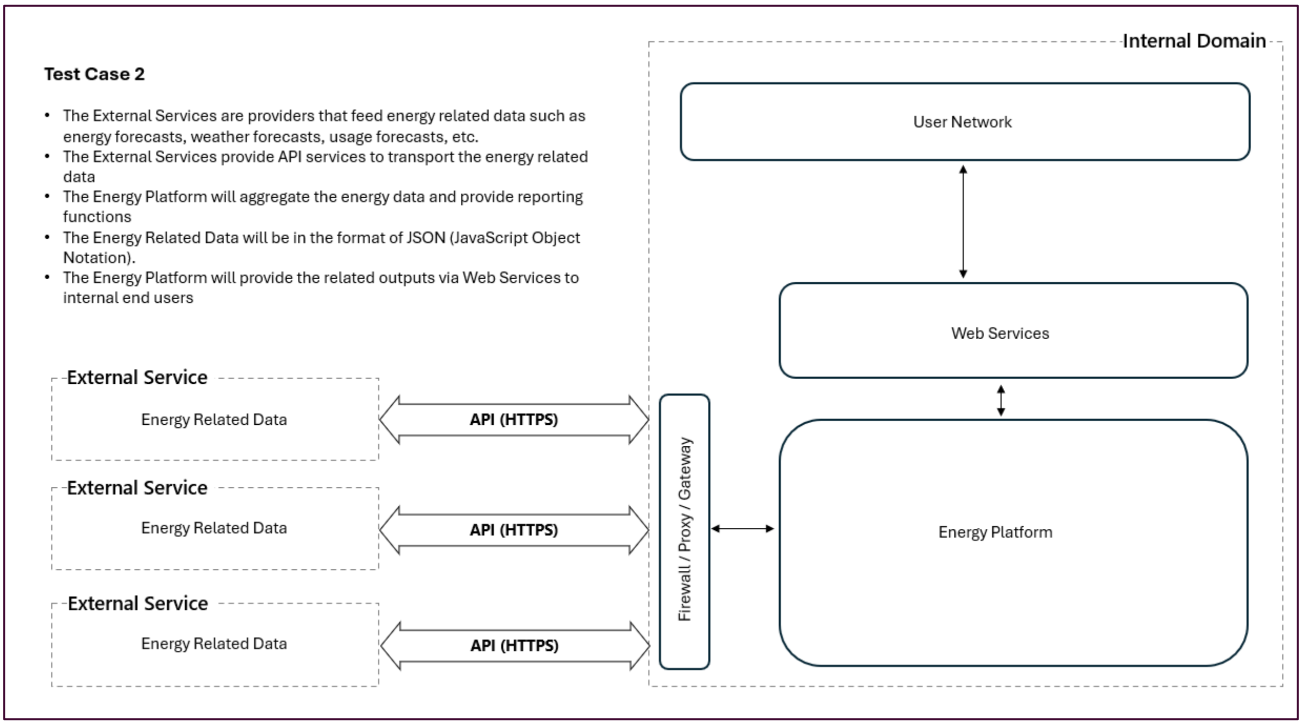
Figure 5: Generated risk histogram summary for test case 1 –2070

Appendix C – Test Case 2

Test case 2 represents the relationship between several services that offer predictive data about the weather, the energy available on the grid, and future energy consumption, that is used to perform pre-emptive control actions to stabilise the grid.

Note that all example systems had the constraint of being detailed enough to be usable for validation of the Q-ARM functional prototype, but not so specific as to accurately describe actual operations within NESO (in order to preserve confidentiality and security).

The structure of the test case is given in Figure 6.



Test Case 2

- The External Services are providers that feed energy related data such as energy forecasts, weather forecasts, usage forecasts, etc.
- The External Services provide API services to transport the energy related data
- The Energy Platform will aggregate the energy data and provide reporting functions
- The Energy Related Data will be in the format of JSON (JavaScript Object Notation).
- The Energy Platform will provide the related outputs via Web Services to internal end users

Figure 6: Test architecture illustrating a grid balancing system used to demonstrate the prototype

Node definitions					Relevant impacts				
Name	Type	Connection type/certificate technology	Hosted on (certified software only)	Data transmitted (connection only)	Confidentiality	Duration (hours)	Integrity	Availability	Authentication
Internal energy platform	Computer	-	-	-	-	-	-	-	High
Internal web services server	Computer	-	-	-	-	-	-	-	High
Internal user computer	Computer	-	-	-	-	-	-	-	Very high
Weather service computer	Computer	-	-	-	-	-	-	-	High
Energy consumption service computer	Computer	-	-	-	-	-	-	-	High
Energy usage service computer	Computer	-	-	-	-	-	-	-	High
Internal energy platform software	Certified software	X.509 Certificates	Internal energy platform	-	Very low	Indefinite	High	Moderate	-
Internal web services software	Certified software	X.509 Certificates	Internal web services server	-	Very low	Indefinite	High	Moderate	-

Node definitions					Relevant impacts				
Name	Type	Connection type/certificate technology	Hosted on (certified software only)	Data transmitted (connection only)	Confidentiality	Duration (hours)	Integrity	Availability	Authentication
Software running on user machines	Certified software	X.509 Certificates	Internal user computer	-	Low	Indefinite	Very High	High	-
Weather service platform software	Certified software	X.509 Certificates	Weather service computer	-	Very low	Indefinite	High	Moderate	-
Energy consumption service platform software	Certified software	X.509 Certificates	Energy consumption service computer	-	Very low	Indefinite	High	Moderate	-
Energy usage service platform software	Certified software	X.509 Certificates	Energy usage service computer	-	Very low	Indefinite	High	Moderate	-
Weather predictions	Data	-	-	-	Very low	Indefinite	Moderate	Moderate	-
Energy predictions	Data	-	-	-	Low	Indefinite	Moderate	Moderate	-
Usage predictions	Data	-	-	-	Low	Indefinite	Moderate	Moderate	-
Link between weather service and the energy platform	Authenticated connection*	https (TLS 1.2)	-	Weather predictions	-	-	-	-	-

Node definitions					Relevant impacts				
Name	Type	Connection type/certificate technology	Hosted on (certified software only)	Data transmitted (connection only)	Confidentiality	Duration (hours)	Integrity	Availability	Authentication
Link between the energy service and the energy platform	Authenticated connection*	https (TLS 1.2)	-	Energy predictions	-	-	-	-	-
Link between the usage service and the energy platform	Authenticated connection*	https (TLS 1.2)	-	Usage predictions	-	-	-	-	-

*The impact is inherited from the data transmitted (i.e. from *Weather predictions* for *Link between weather service and the energy platform*).

Table 11: Test case 2 model representation (node definitions)

For the purposes of the prototype, we used a standard risk scaling matrix from NIST SP800-30. This is used to determine the initial magnitude of each risk based on the calculated likelihoods and severities.

Test Case Results

Below are examples of generated risk forecast tables using the NESO test model and the standard risk scaling matrix for test case 2. To determine the performance of the tool, the year 2025 (Table 12) and 2070 (Table 13) are used to see the differing risk profiles for these two years that are generated within the report. The corresponding risk histograms show outputs from the test case risk report in graphical form (Figure 7 for 2025 and Figure 8 for 2070).

These outputs describe the specific quantum-enabled risks that the system is deemed to be susceptible to by the tool and the histograms show the risk profile of the entire system by summarising the number of risks of each level that the tool has generated.

Fifteen quantum-enabled risks were identified for the forecasting test case. For both, the “Property Impact(s)” column uses the following abbreviations:

- Auth = Authentication
- C = Confidentiality
- I = Integrity

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
1	Link between weather service and the energy platform is intercepted and Weather predictions is read as plaintext	• Link between weather service and the energy platform • Internal energy platform • Weather service computer • Weather predictions	AT1	C	Attacker has access to Weather predictions	Very Low	Very Low	Very Low
2	Link between the energy service and the energy platform is intercepted and Energy predictions is read as plaintext	• Link between the energy service and the energy platform • Internal energy platform • Energy consumption service computer • Energy predictions	AT1	C	Attacker has access to Energy predictions	Low	Very Low	Very Low
3	Link between the usage service and the energy platform is intercepted and Usage predictions is read as plaintext	• Link between the usage service and the energy platform • Internal energy platform • Energy usage service computer • Usage predictions	AT1	C	Attacker has access to Usage predictions	Low	Very Low	Very Low
4	Link between weather service and the energy platform key exchange is intercepted and attacker spoofs either Internal energy platform or Weather service computer	• Link between weather service and the energy platform • Internal energy platform • Weather service computer	AT2	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Weather service computer	High	Very Low	Low
5	Link between the energy service and the energy platform key exchange is intercepted and attacker spoofs either Internal energy platform or Energy consumption service computer	• Link between the energy service and the energy platform • Internal energy platform • Energy consumption service computer	AT2	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy consumption service computer	High	Very Low	Low

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
6	Link between the usage service and the energy platform key exchange is intercepted and attacker spoofs either Internal energy platform or Energy usage service computer	• Link between the usage service and the energy platform • Internal energy platform • Energy usage service computer	AT2	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy usage service computer	High	Very Low	Low
7	Attacker steals public key used to produce authentication certificate used to authenticate Internal energy platform to Weather service computer or vice-versa.	• Link between weather service and the energy platform • Internal energy platform • Weather service computer	AT3	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Weather service computer	High	Very Low	Low
8	Attacker steals public key used to produce authentication certificate used to authenticate Internal energy platform to Energy consumption service computer or vice-versa.	• Link between the energy service and the energy platform • Internal energy platform • Energy consumption service computer	AT3	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy consumption service computer	High	Very Low	Low
9	Attacker steals public key used to produce authentication certificate used to authenticate Internal energy platform to Energy usage service computer or vice-versa.	• Link between the usage service and the energy platform • Internal energy platform • Energy usage service computer	AT3	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy usage service computer	High	Very Low	Low
10	Attacker steals public key for trusted software supplier and digitally signs a malicious patch	• Internal energy platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Internal energy platform software	High	Very Low	Low

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
	to Internal energy platform software							
11	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Internal web services software	• Internal web services software	AT4	I, Auth	Attacker executes arbitrary code in place of Internal web services software	High	Very Low	Low
12	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Software running on user machines	• Software running on user machines	AT4	I, Auth	Attacker executes arbitrary code in place of Software running on user machines	Very High	Very Low	Low
13	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Weather service platform software	• Weather service platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Weather service platform software	High	Very Low	Low
14	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Energy consumption service platform software	• Energy consumption service platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Energy consumption service platform software	High	Very Low	Low
15	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Energy usage service platform software	• Energy usage service platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Energy usage service platform software	High	Very Low	Low

Table 12: Risks automatically identified by the prototype tool for test case 2 (Energy Balancing System), for the year 2025

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
1	Link between weather service and the energy platform is intercepted and Weather predictions is read as plaintext	• Link between weather service and the energy platform • Internal energy platform • Weather service computer • Weather predictions	AT1	C	Attacker has access to Weather predictions	Very Low	Very High	Very Low
2	Link between the energy service and the energy platform is intercepted and Energy predictions is read as plaintext	• Link between the energy service and the energy platform • Internal energy platform • Energy consumption service computer • Energy predictions	AT1	C	Attacker has access to Energy predictions	Low	Very High	Low
3	Link between the usage service and the energy platform is intercepted and Usage predictions is read as plaintext	• Link between the usage service and the energy platform • Internal energy platform • Energy usage service computer • Usage predictions	AT1	C	Attacker has access to Usage predictions	Low	Very High	Low

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
4	Link between weather service and the energy platform key exchange is intercepted and attacker spoofs either Internal energy platform or Weather service computer	• Link between weather service and the energy platform • Internal energy platform • Weather service computer	AT2	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Weather service computer	High	Moderate	Moderate
5	Link between the energy service and the energy platform key exchange is intercepted and attacker spoofs either Internal energy platform or Energy consumption service computer	• Link between the energy service and the energy platform • Internal energy platform • Energy consumption service computer	AT2	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy consumption service computer	High	Moderate	Moderate
6	Link between the usage service and the energy platform key exchange is intercepted and attacker spoofs either Internal energy platform or Energy usage service computer	• Link between the usage service and the energy platform • Internal energy platform • Energy usage service computer	AT2	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy usage service computer	High	Moderate	Moderate

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
7	Attacker steals public key used to produce authentication certificate used to authenticate Internal energy platform to Weather service computer or vice-versa.	• Link between weather service and the energy platform • Internal energy platform • Weather service computer	AT3	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Weather service computer	High	High	High
8	Attacker steals public key used to produce authentication certificate used to authenticate Internal energy platform to Energy consumption service computer or vice-versa.	• Link between the energy service and the energy platform • Internal energy platform • Energy consumption service computer	AT3	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy consumption service computer	High	High	High
9	Attacker steals public key used to produce authentication certificate used to authenticate Internal energy platform to Energy usage service computer or vice-versa.	• Link between the usage service and the energy platform • Internal energy platform • Energy usage service computer	AT3	Auth	Attacker sends malicious messages spoofing either Internal energy platform or Energy usage service computer	High	High	High
10	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Internal energy platform software	• Internal energy platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Internal energy platform software	High	High	High

ID	Caused by (Risk Scenario)	Affected Asset(s)	Attack Type	Property Impact(s)	Outcome Description	Severity	Likelihood	Initial Magnitude
11	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Internal web services software	• Internal web services software	AT4	I, Auth	Attacker executes arbitrary code in place of Internal web services software	High	High	High
12	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Software running on user machines	• Software running on user machines	AT4	I, Auth	Attacker executes arbitrary code in place of Software running on user machines	Very High	High	Very High
13	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Weather service platform software	• Weather service platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Weather service platform software	High	High	High
14	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Energy consumption service platform software	• Energy consumption service platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Energy consumption service platform software	High	High	High
15	Attacker steals public key for trusted software supplier and digitally signs a malicious patch to Energy usage service platform software	• Energy usage service platform software	AT4	I, Auth	Attacker executes arbitrary code in place of Energy usage service platform software	High	High	High

Table 13: Risks, automatically identified by the prototype tool for test case 2 (Energy Balancing System), for 2070

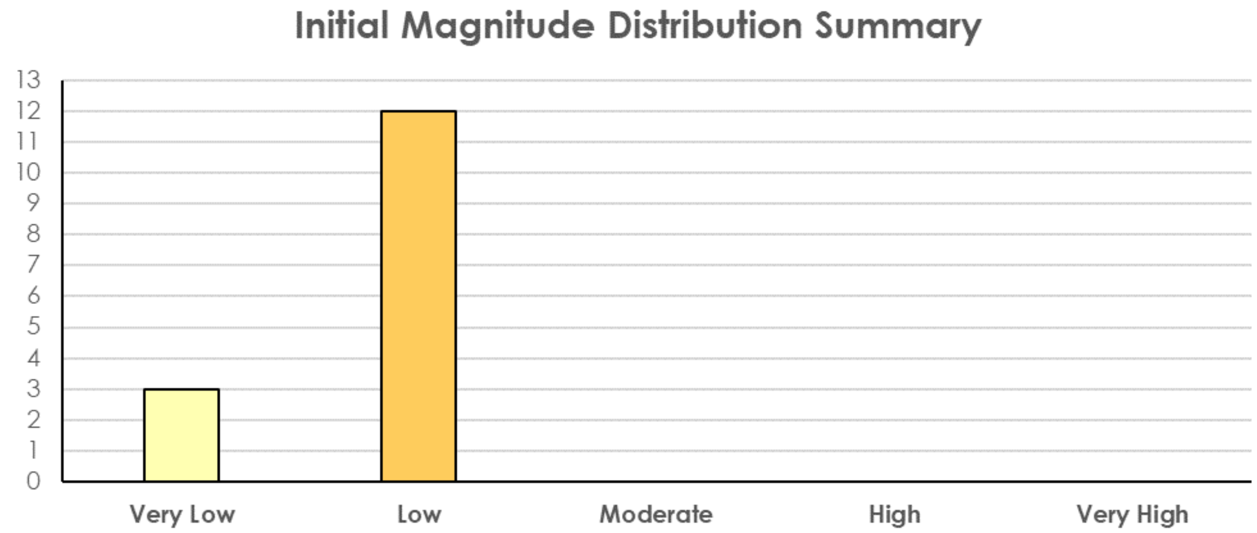


Figure 7: Generated risk histogram for test case 2, 2025

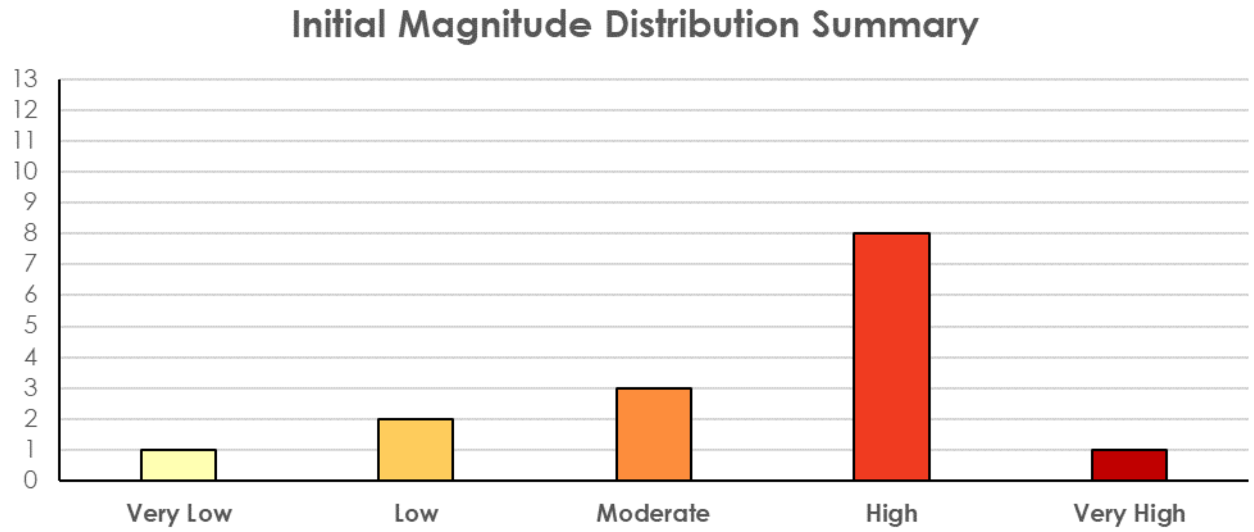


Figure 8: Generated risk histogram summary for test case 2, 2070

Appendix D: Details of the Functional Prototype Development

Requirements Capture and Prioritisation

Error! Reference source not found. shows the current status of all requirements identified during the workshop and analysis phase of the project.

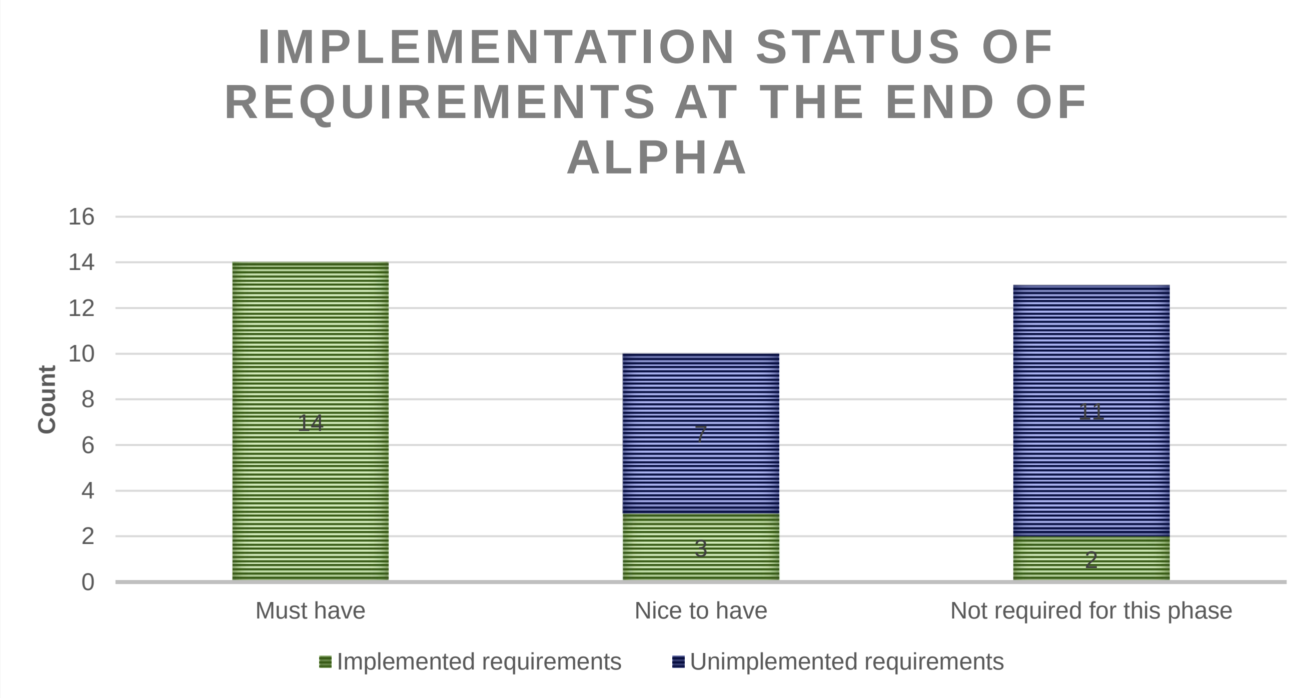


Figure 9: Requirement status at end of Alpha phase Q-ARM functional prototype development.

Table 14**Error! Reference source not found.** shows all of the requirements that were identified and were subsequently fully or partially implemented within the prototype. They have been ordered by assigned priority.

✓ - Must have ≈ - Nice to have ✕ - Not required for this phase

Requirement Description	Alpha Priority	Implementation Status
The Q-ARM will generate a representation of the quantum-enabled risks that are associated with the assets that are within the System of Interest (SoI).	✓	Complete - Implemented as described.
The Q-ARM will allow the user to identify the likelihood and impact of the identified risks using a qualitative method that is compatible with NIST SP800-30.	✓	Complete - Implemented as described.

✓ - Must have ≈ - Nice to have ✕ - Not required for this phase

Requirement Description	Alpha Priority	Implementation Status
The Q-ARM will allow the user to set the time period (in years) that the likelihood assessment will be performed over. E.g. "This risk has a high likelihood of occurring between now and 2035."	✓	Estimates run from now till the target date selected by the user.
The Q-ARM will allow the user to export a report outlining the SoI model and the risks associated with the model assets.	✓	Model is not graphical. Report is in the form of a table and histograms.
The Q-ARM will estimate risk likelihood using time-to-attack, and time-of-attack data provided by the QTT and data about the type of attack being assessed.	✓	Complete - Implemented as described.
The Q-ARM will allow assets and key features (such as data types, cryptographic features, and data property failure impacts) of the SoI to be described and stored within the model.	✓	Complete - Implemented as described.
The Q-ARM will allow the linkages between assets to be captured as data flows.	✓	Complete - Implemented as described.
The Q-ARM will allow cryptographic material, such as certificates and key parameters to be recorded as part of the model	✓	Complete - Implemented as described.
The Q-ARM shall support the modelling of critical energy assets	✓	Complete - Validated by test cases provided.
The Q-ARM will not require any administrative permissions for users to operate it.	✓	Complete - Macros do need to be enabled for the prototype Excel to work.
The output from the QTT will be importable into the Q-ARM without using protected file types such as .exe.	✓	Complete - Though currently this is manual.
The Q-ARM shall allow users to query the level of risk for a quantum-enabled attack at a particular point in time (e.g. in 2034, 2044 etc.).	✓	Complete - Implemented as described.

✓ - Must have ≈ - Nice to have ✕ - Not required for this phase

Requirement Description	Alpha Priority	Implementation Status
The Q-ARM will have a sample SoI and demonstration that allows the features of the Q-ARM to be understood.	✓	Complete - Implemented as described.
The Q-ARM tool will produce reports that are compatible (in terms of likelihood levels, impact levels and risk levels) with NESO risk reports through configuration of the scales used.	≈	Complete - Implemented as described.
The Q-ARM tool will produce reports and forecasts which can be classified (e.g. "Confidential")	≈	Complete - Implemented as described.
The Q-ARM shall allow the creation of reusable assets	≈	Complete - Asset library is used and can be imported into the model.
The Q-ARM will allow the user to explore how risk likelihood changes over the predicted lifetime of the assets.	≈	Complete - Implemented as described.
The Q-ARM report will list the top 5 risks and their mitigations and displays distribution summary histograms for both likelihood and initial magnitude	≈	Complete - Implemented as described.
The Q-ARM tool will reduce the likelihood of an attack by one level if the window of opportunity for an attack is too small for the attack to be feasible.	≈	Complete - Implemented as described.
The Q-ARM tool will allow risk managers to enter a risk matrix that defines risk levels.	✕	Complete - Implemented as described.
Users shall be able to create assets that have not been added by default.	✕	Complete - Yes, simply a new line in the table.
The Q-ARM will allow users to export the risk representation as a graphic	≈	Partially complete - Currently an Excel histogram is created.
The Q-ARM will create a table of suggested mitigations that could be used to control the quantum-enabled risk.	≈	Partially complete - High-level mitigations are provided based on attack type and nothing else.

Table 14: Requirements implemented for the Q-ARM functional prototype

Development Environment for the Q-ARM Functional Prototype

Following the development of an outline architecture, the first development choice our team needed to make was the selection of prototype format. After assessing existing off-the-shelf threat modelling tools, most notably ThreateDragon and Microsoft Threat Modeller, we decided to develop the initial Q-ARM functional prototype using Microsoft Excel Visual Basic for Applications (VBA). This had the following key advantages:

- Allowed rapid development across multi-skilled teams using a common and familiar development environment.
- No restriction with integration with third party applications (required for integrating the Q-ARM with the QTT).
- Utilises native table functionalities to store information (relevant to both databases for further system development and presentation of output reports in risk registers).
- Flexibility to allow additional functionality (for example using VBA / Python macros).
- The above aspects of Microsoft Excel VBA allowed us to focus development on the manipulation of the data to prove core functionality, rather than needing to spend time developing or interacting with graphical modelling functions that already exist in other threat modelling software.
- The final Alpha prototype utilised a combination of native Excel features, and customised VBA macros which allow automation of information across the work sheet.

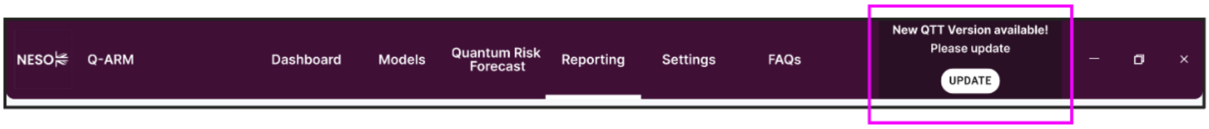
In Beta, the tool will be a standalone piece of software (not an Excel plugin) developed following a more rigorous software quality process. This strategy will also allow the UX design to be combined with the required functions.

Appendix E: Details of UX Interface Design Activities

Page Navigation: Further Details on Design and Functions

The page navigation is common across the top of all pages within the clickable demo tool, allowing a user to access key functionality to navigate across the tool, and to review and update the QTT data that the system is basing the risk assessment on.

The following images highlight the QTT update workflow.

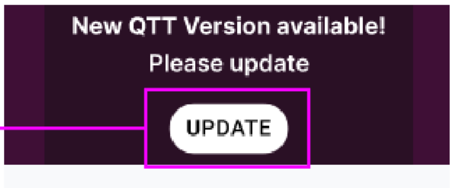


On the menu bar at the top, you can see a button labelled 'UPDATE' with text above explaining 'New QTT version available! Please update'.

This button helps the user ensure that the QTT database referenced by the Q-ARM is always up-to-date. This ensures quantum risk forecasts are performed based on the latest understanding of quantum computing developments.

By hovering over the text with a mouse cursor, a window appears that explains the purpose of the QTT.

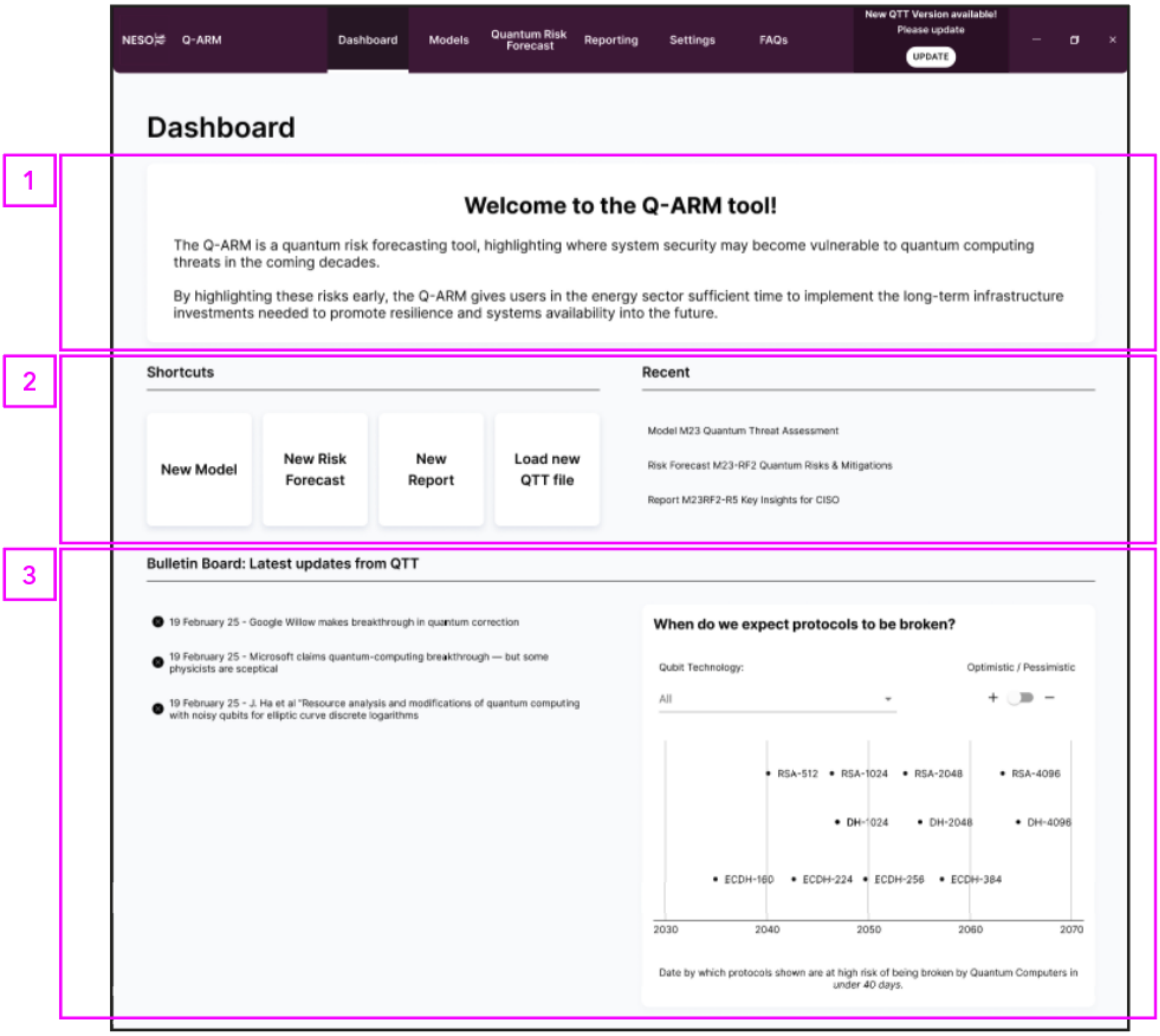
Click on the 'Update' button and watch the short animation as the system updates.



Dashboard Page: Design and Functions

On opening the Q-ARM tool, the dashboard is the first page users will see. At the top of the page, we added some welcome text with a brief text summary highlighting the purpose and value of the tool. To optimise efficient use of the tool we also included a collection of common shortcuts and recently edited files to streamline the process of starting work.

The below image shows a screenshot of the developed dashboard, featuring exemplar data for illustration purposes.



Dashboard

Welcome to the Q-ARM tool!

The Q-ARM is a quantum risk forecasting tool, highlighting where system security may become vulnerable to quantum computing threats in the coming decades.

By highlighting these risks early, the Q-ARM gives users in the energy sector sufficient time to implement the long-term infrastructure investments needed to promote resilience and systems availability into the future.

Model M23 Quantum Threat Assessment

Risk Forecast M23-RF2 Quantum Risks & Mitigations

Report M23RF2-R5 Key Insights for CISO

Bulletin Board: Latest updates from QTT

- 19 February 25 - Google Willow makes breakthrough in quantum correction
- 19 February 25 - Microsoft claims quantum-computing breakthrough — but some physicists are sceptical
- 19 February 25 - J. Ha et al "Resource analysis and modifications of quantum computing with noisy qubits for elliptic curve discrete logarithms

When do we expect protocols to be broken?

Date by which protocols shown are at high risk of being broken by Quantum Computers in under 40 days.

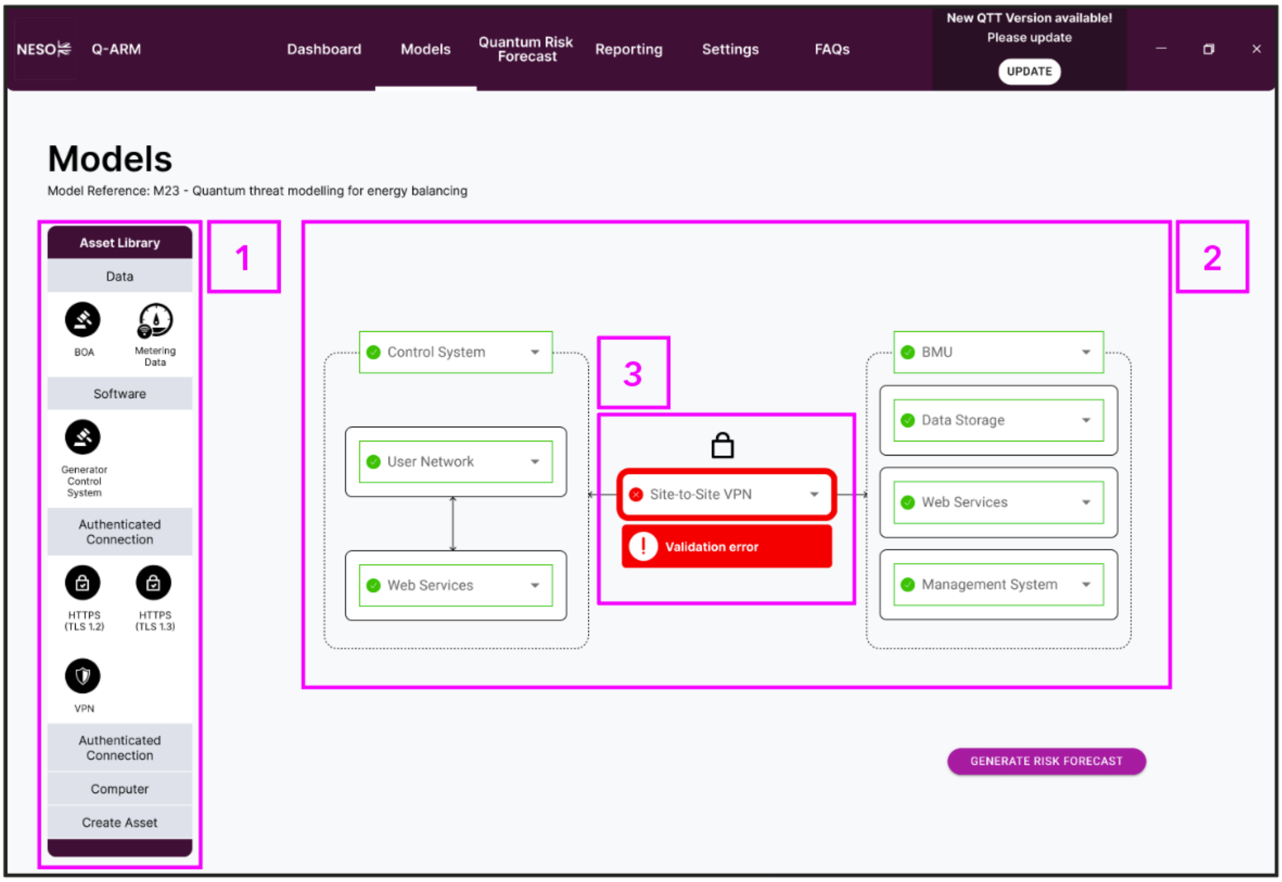
The demo starts on the dashboard screen, this is the home page. It includes the following:

1. Welcome text.
2. Shortcuts to recently used files.
3. Bulletin board - Helps educate users on the latest and most relevant breakthroughs in quantum computing, via news headlines and a map of protocol resilience.

Modelling Page: Design and Functions

The modelling page is used to allow a user to build or import a representation of the target system within the tool. This graphical drag-and-drop interface has been developed to facilitate the population and visualisation of the network, represented in the node definitions and adjacency matrix of the functional prototype.

Other generic system modelling software exists; however, due to the specific detail needed to support a quantum risk forecast we felt it necessary to include this functionality in the Q-ARM. This approach enables us to improve usability by automatically validating the data and giving the user some guidance where more detailed technical information is needed. This detailed information is critical to perform an accurate quantum risk forecast.



The 'Models' page consists of three parts:

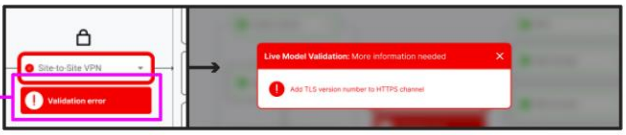
1. Asset library featuring generic and energy specific assets.
2. Model building area.
3. Live model validation – to ensure that all required information is completed within the model to allow for automatic risk forecast assessment.

Users will ultimately be able to add or remove assets in the model by dragging elements from the asset library into the modelling area (this action is not yet functional in the current demo).

At the centre of the modelling area, there is an element highlighted in red, with a label underneath that says, 'validation error'. This is a demonstration of how our live validation tool will work in the final product. The live validation tool tells users when a model doesn't have enough data about the system to generate an accurate risk forecast. Where key information is missing, a red pop-up and bounding box appear, drawing the user's attention to the problem.

The pop-up then provides further guidance to help a non-technical user add detailed encryption data to the asset. Once the data has been added, the asset turns green to indicate a quantum risk forecast can now be performed. If the user isn't able to update the information for whatever reason, it may still be possible to run a quantum risk forecast if the asset is highlighted yellow. In this case the missing data is not considered critical enough to significantly affect the performance of the forecast.

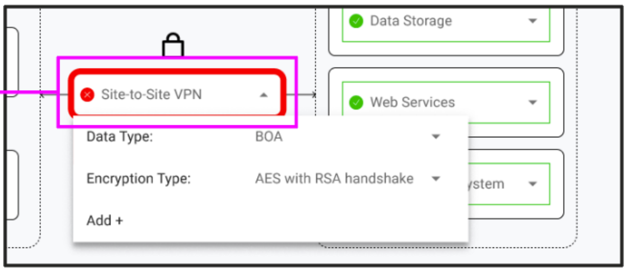
Clicking on the Validation error label opens a pop-up window providing more information about what data is missing.



Live Model Validation: More information needed ✕

Add TLS version number to HTTPS channel

To update an asset's data, click the down arrow on the text box. This reveals a drop-down menu where the user can select the relevant options.



Data Type: BOA

Encryption Type: AES with RSA handshake

Add +

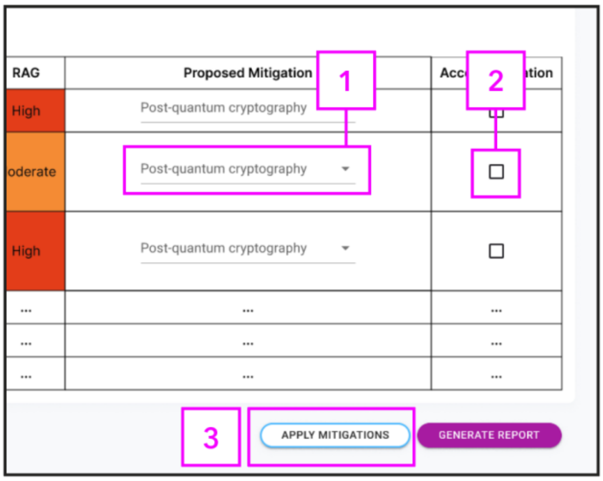
(Note: in this demo, data about the model can't be updated.)

Quantum Risk Forecast Page: Further Details on Design and Functions

Key to the tool's use is the ability to evaluate the effect of mitigations on the risk profile. The quantum risk forecast allows users to explore the effects of recommended mitigations on the risk profile:

1. To see how different mitigations effect risk, you will be able to select a proposed mitigation from the drop-down.
2. Check the accept mitigation box to apply this mitigation to the quantum risk forecast.

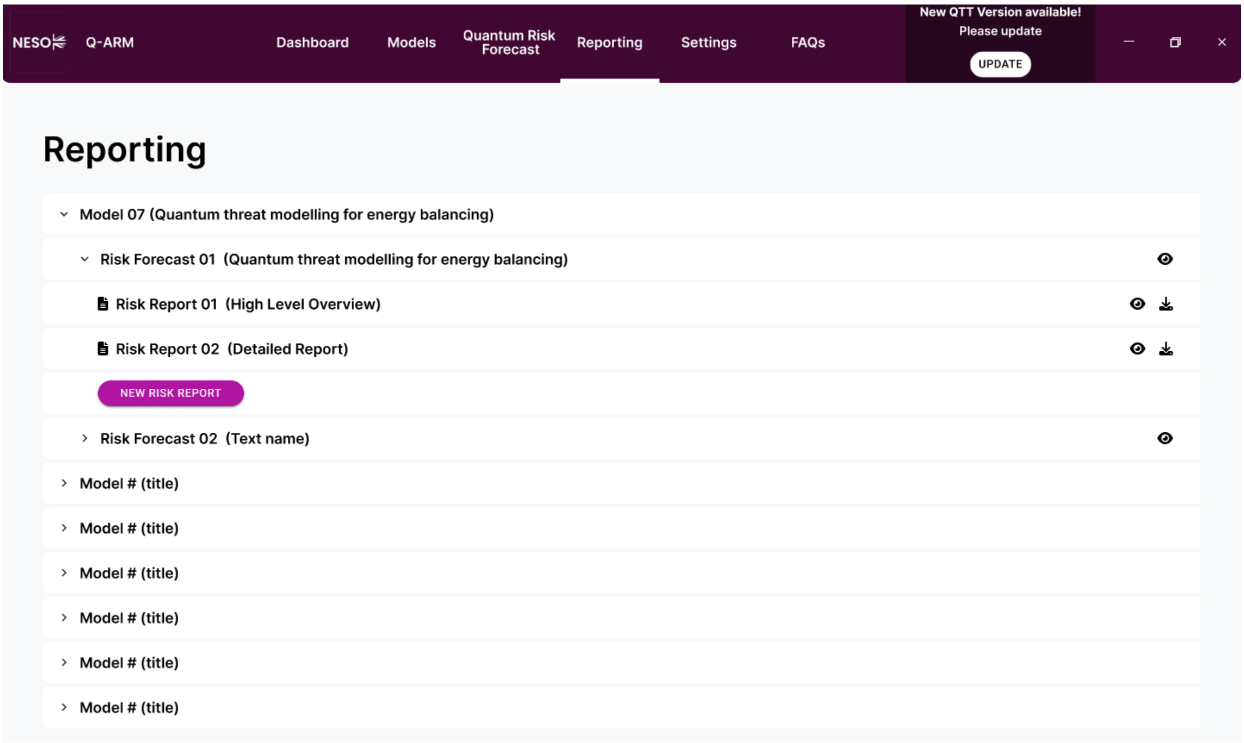
Press the 'apply mitigations' button. This updates the quantum risk forecast histogram showing residual risk after mitigations as a series of blue bars.



RAG	Proposed Mitigation	Acc tion
High	Post-quantum cryptography	☐
oderate	Post-quantum cryptography	☐
High	Post-quantum cryptography	☐
...	...	...
...	...	...
...	...	...

Reporting

This page shows a list of all risk forecasts generated in this software tool. Where multiple risk forecasts are available, there will be a drop down to navigate between versions.



Reporting

- Model 07 (Quantum threat modelling for energy balancing)
  - Risk Forecast 01 (Quantum threat modelling for energy balancing)
    - Risk Report 01 (High Level Overview)
    - Risk Report 02 (Detailed Report)
  - Risk Forecast 02 (Text name)
- Model # (title)
- Model # (title)
- Model # (title)
- Model # (title)
- Model # (title)
- Model # (title)

Feedback from Users and How we Addressed This

By testing prototypes with users, we identified several improvements to features that improved usability and how the workflow could be further optimised. These have all since been implemented in the clickable demo but not implemented in conjunction with the functional prototype.

Page	Feedback
Dashboard and Ribbon	• We re-arranged the order and prominence of features on the dashboard based on feedback from NESO stakeholders. • We re-designed the Bulletin Board section to show QTT updates that were less technical and more useful to NESO users. • Feedback from stakeholders was that the QTT update button wasn’t clear enough, so we’re tried to further emphasis this feature. In the future we could go further to really highlight and flag this function if needed.
Models	• We simplified the process of understanding a validation error and the method used to add data to resolve the issue.

Page	Feedback
Quantum Risk Forecast	• We added additional guidance text to help make the graphs easier to understand without a voice over. • We updated the time-horizon selector to make it clear this related to everything on the page, not just the graphs above. • We updated the process of applying mitigations to remove a user step and allow a more experimental approach to applying different proposed mitigations and seeing the effect this has on the risk distribution.
Reporting	• We initially trialled a different way of presenting documentation but found this led to an overwhelming amount of information being presented. We then switched to an accordion style expanding menu which was familiar to stakeholders and went down well.

Table 15: Key stakeholder feedback on the Clickable demonstrator

Appendix F: Development Backlog

The following features identified during Alpha will be picked up in Beta:

- The tool shall produce multiple risk registers simultaneously for several time periods so the user can see how risk changes over time.
- Risk reports shall embed the version of the QTT software used and the version of the QTT data used, to allow traceability.
- The tool shall support custom risk reports to be generated for different stakeholder needs. These may include system diagrams, top N risks, risk histograms, likelihood histograms, and suggested mitigations.
- The tool shall support mixed classical, hybrid, and pure PQC algorithms in a single system.
- The tool shall automatically check for updates of the QTT output to support the use of the latest threat intelligence.
- The tool shall allow users to revert to old versions of the QTT output to validate risk reports generated on old information.
- The tool shall contain a knowledge base about quantum safe mitigation options that can be read in pdf format.
- The tool shall support time estimates from other sources than the QTT to allow for a comparison between the QTT estimates and those from other organisations.
- The user interface shall support the creation and sharing of new energy system assets.
- A standardised installation and deployment process shall be generated so that IT teams can validate that the tool is safe and not at risk of leaking confidential data.