AMR Cyber Security

CQUEST

WHITE PAPER

February 2024
VERSION: 1.0

TABLE OF CONTENTS

Introduction

The purpose of this paper is to provide an overview of the CQUEST assessment questionnaire and guidance on managing and demonstrating compliance.

Background

The Bank of England is working to ensure that the financial sector in the UK is resilient to any disruptions to its operations.

The financial sector includes banks, building societies, insurers, and financial market infrastructure providers (FMIs). They carry out this work together with the UK's two other financial authorities: HM Treasury and the Financial Conduct Authority.

Operational disruption to important business services could impact financial stability, threaten the safety and soundness of individual firms and financial market infrastructures (FMIs), and cause harm to consumers and other market participants in the financial system. In this context, firms and FMIs should assess their cyber risk and build adequate resilience capabilities to prepare for, and respond to, cyber events and incidents that could cause operational disruption.

As a result of this mandate the Bank of England has introduced several programs and tools (CBEST and CQUEST) that allow financial organisations to benchmark their cyber technological and security operational resilience.

These tools support regulator supervisory oversight and allow organisations to audit deployed security and quantify their risks with security controls, operations, and processes.

What Is CQUEST?

CQUEST forms part of the Bank of England and the Prudential Regulation Authority (PRA)/FCA's supervisory toolkit to gauge the cyber risk and resilience capabilities of the financial sector. CQUEST can also be used by other firm(s) as a self-assessment tool to consider their own cyber risk and resilience maturity. The CQUEST questionnaire (available online, here) comprises 50 questions with multiple-choice answers across six domains:

1. Governance and Leadership
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover

Using Third Parties To Assess CQUEST Compliance

Engaging third-party experts in the CQUEST process brings several advantages:

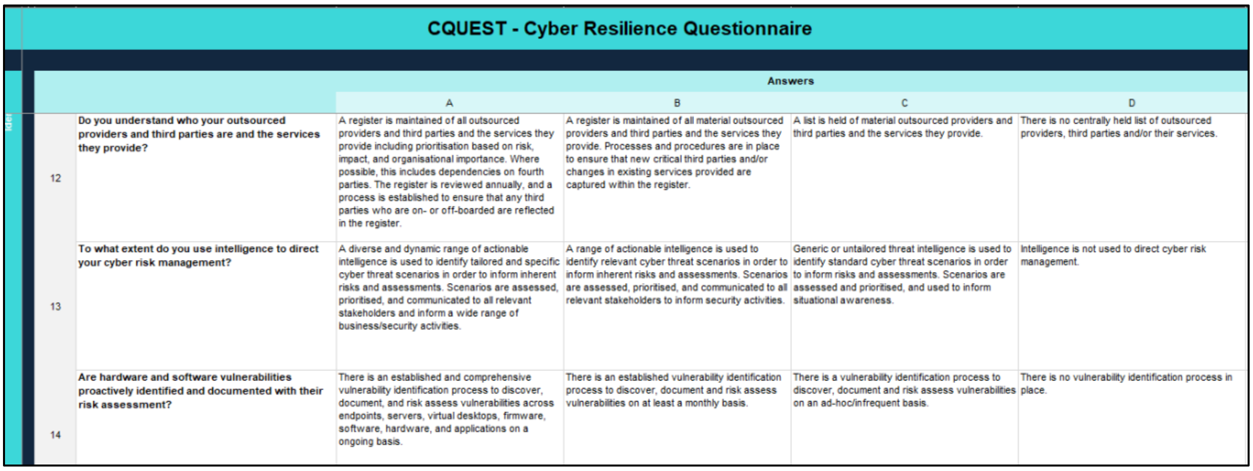
- **Impartial Assessment:** External experts provide unbiased evaluations, offering an objective perspective on cybersecurity measures.
- **Industry Best Practices:** Leveraging third-party expertise allows institutions to tap into industry-leading practices and benchmarks.
- **Fresh Insights:** External perspectives bring new insights, uncovering blind spots that may be overlooked.

Assessing & Reporting Compliance

When assessing compliance you are required to provide a response in accordance with the scale of A-D and the accompanying guidance for each question.

A will typically indicate an organisation complies with the requirement and their capabilities are tested and optimised. D will typically indicate that an organisation does not comply.

The shows the example compliance levels A-D for question 12-14.



CQUEST - Cyber Resilience Questionnaire

		Answers			
		A	B	C	D
12	**Do you understand who your outsourced providers and third parties are and the services they provide?**	A register is maintained of all outsourced providers and third parties and the services they provide including prioritisation based on risk, impact, and organisational importance. Where possible, this includes dependencies on fourth parties. The register is reviewed annually, and a process is established to ensure that any third parties who are on- or off-boarded are reflected in the register.	A register is maintained of all material outsourced providers and third parties and the services they provide. Processes and procedures are in place to ensure that new critical third parties and/or changes in existing services provided are captured within the register.	A list is held of material outsourced providers and third parties and the services they provide.	There is no centrally held list of outsourced providers, third parties and/or their services.
13	**To what extent do you use intelligence to direct your cyber risk management?**	A diverse and dynamic range of actionable intelligence is used to identify tailored and specific cyber threat scenarios in order to inform inherent risks and assessments. Scenarios are assessed, prioritised, and communicated to all relevant stakeholders and inform a wide range of business/security activities.	A range of actionable intelligence is used to identify relevant cyber threat scenarios in order to inform inherent risks and assessments. Scenarios are assessed, prioritised, and communicated to all relevant stakeholders to inform security activities.	Generic or untailored threat intelligence is used to identify standard cyber threat scenarios in order to inform risks and assessments. Scenarios are assessed and prioritised, and used to inform situational awareness.	Intelligence is not used to direct cyber risk management.
14	**Are hardware and software vulnerabilities proactively identified and documented with their risk assessment?**	There is an established and comprehensive vulnerability identification process to discover, document, and risk assess vulnerabilities across endpoints, servers, virtual desktops, firmware, software, hardware, and applications on a ongoing basis.	There is an established vulnerability identification process to discover, document and risk assess vulnerabilities on at least a monthly basis.	There is a vulnerability identification process to discover, document and risk assess vulnerabilities on an ad-hoc/infrequent basis.	There is no vulnerability identification process in place.

When providing a response, it is useful to provide details of exactly how you meet the requirement and reference any supporting documents. By taking this approach organisations can provide clear levels of evidence of how they can comply with each requirement and support any external assessment of their compliance claims.

When assessing compliance organisations can utilise a range of means to assess and validate compliance covering:

- Document based reviews.
- Document based review and audit.
- Desktop based exercises.
- Scenario based testing.

The type of assessment used for each question will vary based on the specific question and evidence required to support the response and the level of maturity of the organisation. For organisations new to the process and known to have a low level of cyber security maturity, then document-based review and supporting audit will provide an effective means of assessing their compliance with the CQUEST assessment.

For organisations with a more mature cyber security posture, it is useful to test the responses with desktop- and scenario-based testing to assess the effectiveness of controls and further identify areas for improvement.

Benefits of CQUEST

Operational resilience is crucial for organisations in the financial sector, due to the complex and dynamic nature of their operations.

CQUEST is a comprehensive approach that goes beyond mere risk management.
It encompasses strategic planning, risk mitigation, and effective response mechanisms, ultimately contributing to the long-term sustainability and success of financial sector organisations. The impact of this framework has direct benefits to any financial organisation.

Below are some of the key benefits of operational resilience and the CQUEST process:

- **Risk Mitigation:** Operational resilience ensures essential services continue even in the face of disruptions, reducing impact of downtime on critical functions. By thoroughly understanding and assessing potential risks, organisations can implement effective risk management strategies to mitigate the impact of disruptions.

- **Regulatory Compliance:** Regulatory bodies often require financial institutions to demonstrate operational resilience. Complying with these regulations not only avoids penalties but also enhances the organisation's reputation.

- **Maintaining Customer Trust:** Operational resilience helps in maintaining customer trust by ensuring that their financial transactions and data are secure and available, even in challenging circumstances.

- **Adaptability & Change:** Operational resilience fosters a culture of adaptability. Organisations can respond more effectively to changes in the business environment, technology, and regulatory landscape.

- **Supply Chain Resilience:** Financial institutions often rely on various third-party vendors. Operational resilience extends to ensuring the entire supply chain is robust, reducing risk of disruptions caused by external partners.

- **Incident Response & Recovery:** Operational resilience frameworks include well-defined incident response plans. A quick and effective response to incidents minimises the impact on operations and reduces recovery time.

Further Support

If you need further support in assessing and testing compliance with the CQUEST questionnaire, or developing prioritised remediation plans and implementing effective controls, then the specialists at AMR CyberSecurity can support you.

Specific areas where we can assist include:

- Maturity assessment, audit, and gap analysis.

- Desktop based exercises.
- Full scenario-based tests.

Please contact enquiries@amrcybersecurity.com to speak to one of our consultants.