CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

CROSS MARKET OPERATIONAL RESILIENCE GROUP HANDBOOK

VERSION 1 | SEPTEMBER 2025 | TLP CLEAR

CONTENTS

CMORG-endorsed capabilities (including good practice guidance, response frameworks and contingency tools) have been developed collectively by industry to support the operational resilience of the UK financial sector. The financial authorities support the development of these capabilities and collective efforts to improve sector resilience. However, their use is voluntary, and they do not constitute regulatory rules or supervisory expectations; as such, they may not necessarily represent formal endorsement by the authorities.

1 Introduction

1.1 About CMORG

The Cross Market Operational Resilience Group (CMORG) was established to improve the operational resilience of the sector e.g. public private management of collective action strategies. The group forms the strategic focal point for sector-wide operational resilience discussions and meets at least four times a year. CMORG is supported by a number of technical and industry subgroups. These groups design, manage, and deliver operational resilience improvement projects on a voluntary and collaborative basis.

CMORG operates on the principle that its outputs and interventions should benefit all in the sector, and any of its contingencies or interventions should be accessible beyond its core membership. Those firms directly participating on or within the CMORG structure are expected to act for the benefit of the sector without attribution to their firms. These outputs, or capabilities, are detailed within this document.

1.2 CMORG Membership

CMORG is co-chaired by the Executive Director for Supervisory Risk of the Bank of England and the CEO of UK Finance. CMORG membership requires individuals at CRO, COO or SMF24 Chief Operations function level. To ensure the group has a relevant and balanced view from across the sector, CMORG membership will aim to consist of a minimum:

- wholesale banks
- retail banks
- FMIs
- 2 Insurers
- Authorities (Bank of England, HM Treasury, FCA)
- National Cyber Security Centre (NCSC)

1.3 CMORG Project Management Office (PMO)

CMORG is supported by the PMO, jointly resourced by UK Finance and the Bank of England. The PMO supports the industry's design and delivery of sector resilience enhancements. This includes secretariat resources for its governance, project management and advisory support, and providing the operations that underpin CMORG.

1.4 How to Access Capabilities

The majority of CMORG capabilities can be accessed through the CMORG website.

Please note that a CMORG account will be required to access materials classified at TLP GREEN and above. If you are having trouble accessing the CMORG website, please contact us through the following webpage: https://www.cmorg.org.uk/contact-us

1.5 How to Get in Touch

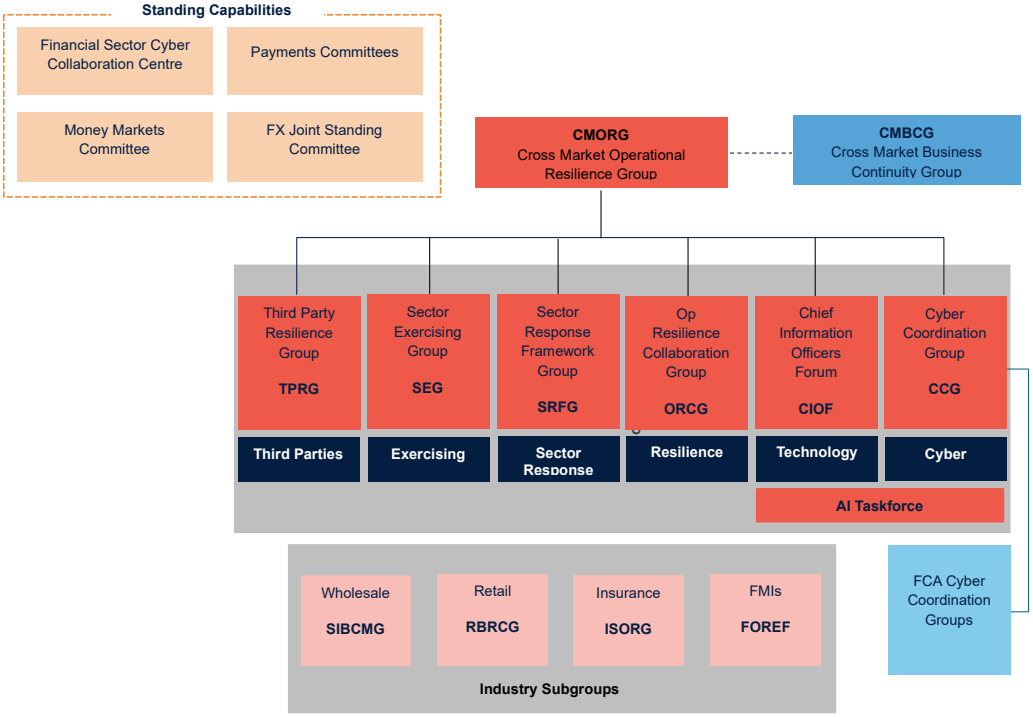
You can contact the PMO via email on enquiries@cmorg.org.uk or CMORG@bankofengland.co.uk

2 Governance Structure

2.1 Governance chart

The CMORG subgroup structure allows for the design and delivery of capabilities. Each subgroup covers a specific area of operational resilience and is made up of relevant expertise from across the sector.

- **Chief Information Officers Forum (CIOF):** tracks technology developments and assesses their impact on the UK financial system.
- **Cyber Coordination Group (CCG):** monitors the cyber landscape, security and resilience developments, and builds capabilities to support the resilience of the UK financial system.
- **Operational Resilience Collaboration Group (ORCG):** provides cross-sectoral thought leadership on operational resilience and delivers operational resilience improvement projects.
- **Sector Exercising Group (SEG):** develops and maintains a forward-looking, medium-term, exercising strategy and associated execution programme.
- **Sector Response Framework Group (SRFG):** owns and maintains the Sector Response Framework and ensures that it is continually improved and embedded across the sector.
- **Third Party Resilience Group (TPRG):** accountable for all third-party resilience-related activity under CMORG, in support of improved resilience across critical third parties and the wider ecosystem.



3 How CMORG Delivers Capabilities

1. Initiating a workstream

CMORG workstreams are delivered through its subgroups and are aligned to CMORG's workplan and strategic priorities. The subgroup members and chairs will discuss initiating a new workstream and when agreed, a business case is drafted.

2. Drafting a business case

The workstream lead will draft a business case, including a description of the project, its alignment to the CMORG strategy, key milestones, prioritisation scoring and potential resource requirements. This is then shared with the PMO to finalise before being presented to CMORG members.

3. Endorsement

Proposed new business cases are brought to CMORG's meetings, where they are discussed by members. If members endorse the business case and agree executive sponsorship, the workstream will be initiated, added to the portfolio and prioritised. Time-sensitive business cases can also be agreed by written procedure outside the CMORG meeting cycle.

4. Delivery Focus

Following endorsement, the workstream becomes delivery focused and the work is progressed by the working group with direction from the relevant subgroup(s).

5. Publication

The output(s) of the workstream is taken back to CMORG members at their meeting(s). The deliverable is then scheduled for publication if members endorse and circulated on the CMORG website at the relevant classification. TLP Clear capabilities are publicly available.

4 Sector Response Capabilities

This section outlines the key sector response capabilities developed by CMORG.

Sector response capabilities enable firms to respond swiftly and cohesively to severe disruptions, mitigating the risk to the sector as a whole. CMORG has a number of capabilities that support a collective sector response to incidents. These capabilities foster shared situational awareness, structured decision-making, and consistent communication across firms and authorities. This collective approach helps maintain market stability, protect consumer confidence, and ensure continuity of important business services during crises.

4.1 Sector Response Framework (inc. Incident Lexicon)

About the capabilities

The Sector Response Framework (SRF) provides a structured mechanism for the UK financial sector to coordinate and respond collectively to systemic incidents. It describes the operational, tactical, and strategic levels of response, supported by Sector Response Groups, FMI Crisis Committees, and the Cross Market Business Continuity Group (CMBCG). The framework includes escalation triggers, roles and responsibilities, and integrates with the Authorities' Response Framework (ARF). The SRF capability also includes the Firm Mapping Template, which firms can use to map their memberships to relevant groups, to integrate the SRF within their own crisis plans and processes. The SRF Response Groups document provides detailed descriptions of the response groups and committees that form the operational structure of the SRF. The SRF references supporting tools such as the Incident Lexicon, which provides a standardised lexicon and reporting principles to support consistent communication across the UK financial sector. It aims to reduce confusion and improve clarity when firms report incidents externally, particularly during sector-wide events.

Owner

This is a CMORG-owned capability, developed by the Sector Response Framework Group (SRFG). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Dates

This capability is regularly reviewed, but original publication dates for the documents described above range between May 2021 and December 2024.

TLP rating and sharing

Documents range between TLP: Green and TLP: Amber. Please refer to the artefact library or the CMORG Website for the Sector Response Framework; Sector Response Framework Summary Document; Sector Response Framework Mapping Template; Sector Response Framework – Response Groups documents for further information.

4.2 Reconnection Framework v3

About the capability

The third iteration of the Reconnection Framework provides guidance for restoring connectivity between a compromised organisation and its clients following a malicious cyber incident. It outlines a phased approach to ensure systems are returned to a trusted state before resuming operations. It emphasises transparency, collaboration, and technical assurance, including attestation and forensic reporting. The framework supports pre-planning, governance, and communication, and is designed to reduce recovery time while maintaining security and trust across the financial sector.

Owner

This is a CMORG-owned document, developed by the Cyber Coordination Group (CCG). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

July 2025

TLP rating and sharing

This document is classified as TLP: Clear.

4.3 Operationally Paralysed Global Systemically Important Bank (GSIB) – Sector Response Principles

About the capability
This document sets out sector-wide principles to guide the UK financial system's collective response to a scenario in which a Global Systemically Important Bank (GSIB) becomes operationally paralysed. Developed by CMORG following SIMEX18, it outlines immediate, behavioural, and planning principles for firms, FMIs, and authorities to coordinate effectively during the first 24–48 hours of such an incident. It includes a GSIB Heat Map to assess systemic impact and substitutability, and highlights the importance of strategic coordination, communication, and pre-agreed contingency planning to maintain market confidence and stability.

Owner
This is a CMORG-owned document. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date
May 2021

TLP rating and sharing
This document is classified as TLP: Amber.

4.4 Firm Shutdown/Sector Restart Playbook

About the capabilities
The CMORG Collective Action Firm Shutdown/Sector Restart Playbook enables the sector to shut down and restart on a coordinated basis in the event of a major operational disruption. The playbook was developed in support of SIMEX24, which explored the impact of a national power outage (NPO) on the UK financial sector. The playbook could be relevant in other extreme scenarios, for instance a major cyber-attack. Developed under CMORG governance and aligned with the UK Financial Authorities' strategic planning, it outlines the procedures for alert and notification, firm/FMI level response during and immediately following an outage, resumption of services, sector restart, communications, and remediation and restoration.

Owner
These documents are CMORG-owned. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date
September 2024, June 2025

TLP rating and sharing
This document is classified as TLP: Amber+Strict.

5 Cyber and Technology

This section outlines the key cyber and technology capabilities developed by CMORG.

Robust cyber and technology capabilities support the operational resilience of the UK financial sector by enabling rapid detection, containment, and recovery from cyber threats. CMORG has developed several capabilities in this area, with a focus on mitigating those risks that might be broader than a single firm. Sector-wide exercises, sharing threat intelligence, and promoting consistent use of frameworks can help firms to address vulnerabilities, manage third party risks, and maintain trust and stability during cyber incidents.

5.1 Data Vaulting Reference Architecture and Cloud-Hosted Data Vaulting Good Practice

About the capability

The Data Vaulting Reference Architecture is intended to help firms implement data vault solutions in a consistent and secure way, and to reduce the barriers to entry for firms in safeguarding their data. It defines a cloud-hosted capability that can be leveraged by firms across the sector and deployed flexibly in terms of scale, coverage and location. This includes a generic design blueprint that can be implemented including firm-specific security policies, infrastructure and operating models.

The Cloud-Hosted Data Vaulting Good Practice provides practical guidance for implementing cloud-hosted data vaulting to enhance operational resilience in the UK financial sector. It outlines best practices for securely storing critical data in isolated, immutable cloud environments to support recovery from cyber incidents such as ransomware or data corruption.

Major cloud service providers were engaged to confirm the viability of the both the reference architecture and the good practice guidance.

Owner

This is a CMORG-owned document, produced by the CIO Forum. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

April 2022, February 2025

TLP rating and sharing

The Reference Architecture is classified as TLP: Amber.

The Cloud-Hosted Data Vaulting Good Practice is classified as TLP: Clear.

5.2 Cloud Control Framework

About the capability

The Cloud Control Framework establishes a baseline set of control standards for financial services firms and cloud service providers (CSPs), operating across the shared responsibility model. The standards are intended to drive improved capability and consistency across the sector, whilst helping firms to clarify key requirements during cloud adoption. The Cloud Control Framework recognises that implementation of controls is likely to vary across the sector, and leverages work already undertaken by firms and CSPs and aims to create a trusted industry standard to support a sector-wide approach to cloud control standards. The Framework is endorsed by major CSPs and aligned to more detailed controls specifications documented in the Cyber Risk Institute's (CRI) Cloud Profile.

Owner

This is a CMORG-owned document, produced by the CIO Forum. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

December 2021

TLP rating and sharing

This document is classified as TLP: Amber.

5.3 Guidance for Post-Quantum Cryptography

About the capability

This capability provides strategic guidance for UK financial institutions to prepare for the cryptographic risks posed by quantum computing. The guidance outlines the urgency of transitioning to post-quantum cryptography (PQC) and aligns with NCSC and NIST recommendations. It includes background on quantum computing and the impact to cryptography, as well as a review of PQC algorithms, a roadmap to PQC and vendor readiness. Firms are encouraged to use the guidance to enhance cryptographic inventory capabilities and develop a structured migration roadmap in order to build resilience against the impact of quantum computing.

Owner

This is a CMORG-owned document, developed by the Cyber Coordination Group (CCG). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

April 2025

TLP rating and sharing

This document is classified as TLP: Clear.

5.4 AI Baseline Guidance Review

About the capability

This capability provides a comprehensive overview of good practice for managing risks associated with Generative AI (Gen AI) adoption in the UK financial sector. The guidance consolidates insights from government, industry, and regulatory sources into five thematic areas: government and regulatory approaches, risk management frameworks, technical implementation, third party and legal considerations, and education and awareness. The document also highlights essential reading and toolkits to support firms in navigating the fast-evolving GenAI landscape.

Owner

This is a CMORG-owned document, developed by the AI Taskforce. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

April 2025

TLP rating and sharing

This document is classified as TLP Clear.

6 Operational Resilience

This section outlines CMORG's key operational resilience capabilities.

Building operational resilience capabilities can enhance the financial sector's ability to withstand, adapt to, and recover from severe disruptions. CMORG aims to play a central role by coordinating sector-wide exercises, sharing lessons learned, and promoting consistent approaches to identifying and protecting Important Business Services. This collective effort strengthens firms' ability to maintain continuity, manage interdependencies, and safeguard financial stability during crises.

6.1 Strategic Risk Register v3

About the capability

The Strategic Risk Register (SRR) captures the most relevant risks facing the financial sector. Refreshed in 2025, the register reflects the Operational Resilience Collaboration Group (ORCG)'s Threat Monitoring Framework, the Dynamic Scenario Library, the National Risk Register and the Authorities' recommendations to provide a composite view of the strategic risk landscape. Risks are listed with a theme, domain, risk and scenario and categorised as short, medium and long term.

Owner

This is a CMORG-owned document. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

April 2025

TLP rating and sharing

This document is classified as TLP: Amber+Strict.

6.2 Guidance For Firm Operational Resilience v3

About the capability

This third edition of the guidance provides updated principles and practical direction for UK financial firms implementing operational resilience frameworks. It supports compliance with PRA SS1/21 and FCA PS21/3, covering the identification of Important Business Services (IBSs), setting and testing Impact Tolerances (ITOLs), mapping critical resources, managing vulnerabilities, and embedding resilience into governance and culture. The guidance also includes a structured approach to scenario testing and self-assessment, with emphasis on continuous improvement, third party dependencies, and lessons learned from sector-wide incidents such as the 2024 CrowdStrike outage.

Owner

This is a CMORG-owned document, developed by the Operational Resilience Collaboration Group (ORCG). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

April 2025

TLP rating and sharing

This document is classified as TLP: Clear.

6.3 Dynamic Scenario Library

About the capability

The Dynamic Scenario Library (DSL) provides a structured, sector-wide catalogue of severe but plausible scenarios to support operational resilience planning and testing across the UK financial sector. It is designed to be a shared, customisable resource for firms to test their ability to remain within impact tolerances under stress. Scenario development is informed by the CMORG Strategic Risk Register (SRR) and sectoral threat monitoring.

Owner

This is a CMORG-owned document, developed and maintained by the Operational Resilience Collaboration Group (ORCG). Please direct any enquiries to CMORG@bankofengland.co.uk.

Publication Date

First published March 2025 (to be updated regularly).

TLP rating and sharing

This document is classified as TLP: Clear.

6.4 Sectoral Threats to the UK Financial Sector

About the capability

This capability is the inaugural edition of the CMORG-endorsed Threat Monitoring Sector Trend Report, developed by the Operational Resilience Collaboration Group (ORCG). It provides a collective, cross-sectoral view of the most significant threats to the operational resilience of the UK financial sector, based on submissions from 26 member firms. The report complements the CMORG Strategic Risk Register (SRR) and is designed to support strategic risk management, scenario planning, and resilience development.

Owner

This is a CMORG-owned document, developed and maintained by the Operational Resilience Collaboration Group (ORCG). Please direct any enquiries to CMORG@bankofengland.co.uk.

Publication Date

First published March 2025 (to be updated regularly).

TLP rating and sharing

This document is classified as TLP: Amber+Strict.

7 Third Parties

This section outlines the key third party capabilities developed by CMORG.

With the financial services sector more interconnected than ever, third party risk management goes beyond firm-level assurance. CMORG's third party focused capabilities can help firms to identify, assess, and mitigate vulnerabilities in their supply chains. This is supported by promoting sector-wide coordination, sharing lessons from incidents like Log4j, and encouraging consistent practices in supplier assurance, dependency mapping, and incident response. This collective approach strengthens the sector's ability to withstand disruptions originating from third party failures.

7.1 Supplier Risk Assurance Framework

About the capability

This capability provides practical guidance and tools to help organisations assess the risk of third party suppliers and ensure appropriate levels of risk-based control. The framework includes a third party assurance risk scale comprising three elements: an example of risk factors and weightings that can help an organisation identify the drivers of the risk of their third party providers; a calculator that interprets those risk factors to group third parties by different risk levels; and an escalating control scale that can be deployed to manage the risk of third party providers at the different risk levels.

Owner

This is a CMORG-owned document, developed by the Operational Resilience Collaboration Group (ORCG). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

July 2023

TLP rating and sharing

This document is classified as TLP: Green.

7.2 Collaborative Scenario Testing of Critical Third Parties

About the capability

This report outlines a methodology and approach for collaboratively testing the resilience of critical third parties (CTPs) that support multiple firms. The approach aims to reduce duplicated assurance efforts, improve visibility into third party recovery capabilities, and support regulatory expectations for operational resilience. The document is a sanitised version of a report covering a pilot of collaborative scenario testing with two third party payment providers to assess the viability of the methodology. This has been published at TLP: Clear to encourage sharing and awareness among the financial sector and. A full report at TLP: Amber is available on request to firms who are members of the Operational Resilience Collaboration Group (ORCG).

Owner

This is a CMORG-owned document, developed by the Operational Resilience Collaboration Group (ORCG). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

July 2023

TLP rating and sharing

This document is classified as TLP: Clear.

7.3 Collaborative Scenario Testing of Third Parties – Effective Practices

About the capability

The capability provides a set of principles and broad expectations of the industry on how scenario testing with third parties should be conducted. The guidance is intended to be used by financial firms of all maturities either as a guidance for building a framework for scenario testing with third parties, or to act as a check point for established programs. Third parties to the financial sector can also benefit from the expectations, standards and reporting requirements laid out in the capability. It outlines good practice on scenario testing including with regards to selection of scenarios, expectations around evidencing resilience during scenario testing, coverage of scenario test reports and incorporation of third party scenario test obligations into contracts.

Owner

This is a CMORG-owned document, produced by the Operational Resilience Collaboration Group (ORCG). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

September 2024

TLP rating and sharing

This document is classified as TLP: Clear.

7.4 Third Party Exit Plan Template

About the capability

This capability provides a standardised template and guidance for managing the exit of material and high-impact third party suppliers. It supports firms in meeting regulatory expectations under UK and EU frameworks, including PRA SS2/21 and DORA. The template covers supplier information, exit strategies, roles and responsibilities, risk and impact assessments, data management, communications, and testing. It is designed to ensure operational resilience and continuity during both planned and stressed exits.

Owner

This is a CMORG-owned document, produced jointly by the Third Party Resilience Group (TPRG) and the Third Party & Outsourcing Committee (TPOC). Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date

February 2025

TLP rating and sharing

This document is classified as TLP: Clear.

8 Payments

This section outlines the key payments-related capabilities developed by CMORG.

CMORG's payment capabilities are designed to enhance resilience and transparency across the financial sector by strengthening operational continuity and reducing exposure to systemic vulnerabilities. This includes promoting sector-wide collaboration on payment assurance, sharing insights from disruptions such as real-time payment outages, and encouraging consistent practices in payment dependency mapping and incident response. Through this coordinated approach, CMORG contributes to a more robust and secure payments ecosystem.

8.1 GBP Payments Prioritisation Framework (Phase One and Two)

About the capability
The Payments Prioritisation Framework outlines a principles-based framework for identifying and prioritising payments (both wholesale and retail) during severe operational disruption. Developed in two phases, the first focuses on a prioritisation and contingency framework for high-value CHAPS payments and FMI settlements that support the stability and the integrity of the UK financial markets. The second phase identifies critical interbank retail payments for prioritisation, looking at FPS and Bacs and retail payments in CHAPS.

Owner
These are CMORG-owned documents. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date
August 2022, April 2023

TLP rating and sharing
These documents are classified as TLP: Green.

8.2 Voluntary Sterling Settlement (VSSP) Playbook

About the capability
The VSSP playbook outlines the operational framework for invoking a Voluntary Sterling Settlement Postponement (VSSP), a contingency measure delivered through the Cross Market Business Continuity Group (CMBCG) to suspend sterling settlement in extreme disruption scenarios. It provides guidance for horizon scanning, alert and notification procedures, decision-making, communication, remediation and restoration. It builds on lessons from SIMEX16, COVID-19 contingency planning and the 1987 Storm from which the concept of a Voluntary Sterling Settlement Postponement originated.

Owner
These documents are CMORG-owned. Please direct any queries to CMORG@bankofengland.co.uk.

Publication Date
September 2024, June 2025

TLP rating and sharing
This document is classified as TLP: Amber+Strict.

9 Further Capabilities

Sector Response

Cash-Related Incident Playbook

This capability aims to establish a high-level coordinated collective response in the event of a major incident affecting the provision and circulation of cash and consumers.

Custody Contingency Sector Response Principles

This document sets out sector-wide principles for responding to custody service disruptions, guiding coordinated action and strategic response planning across firms and UK Financial Authorities.

FSCCC Incident Management Playbook/Finance Emergency Call Cyber

This capability provides guidance for engaging with the FSCCC, including the invocation and management of a Finance Emergency Call Cyber (FinECC) during significant cyber events affecting the UK financial sector.

UK Finance Incident Management Communications Playbook

To set out the approach and procedures by which the UK Finance media team will lead a single, unified voice to an incident specific to the banking and finance sector and UK Finance members.

Cyber and Technology

Cyber Incident Reporting Framework (Ghostbusters Guide)

The framework acts as a consolidated set of advice, guidance and best practice to support cyber incident reporting requirements and processes within the UK.

Log4j Lessons Learned

This document shares sector-wide lessons and recommendations from the Log4Shell vulnerability, aiming to improve cyber preparedness, response coordination, and resilience across the UK financial sector.

Security in the Cloud

Best practice guidance on how to plan and implement security in the cloud.

Operational Resilience

SIMEX22 Single Company Exercise

This document is a combined exercise and injects pack for SIMEX22, helping financial firms test crisis response to a simulated G-SIB disruption scenario.

SIMEX24 Post Exercise Report

This report documents the findings and strategic recommendations from SIMEX24, a full-day operational resilience exercise led by CMORG and the UK financial authorities.

Covid-19 Lessons Learned

This document summarises operational resilience lessons from COVID-19 for the UK financial sector, offering 17 firm-level recommendations and 4 sector-wide actions coordinated by CMORG.

Settlement Contingencies (Operations)

Contingency documentation explaining how Voluntary Sterling Settlement Postponement (VSSP) and Amended Settlement Hours (ASH) would be invoked and helping firms prepare their own contingency capabilities in support of these tools.

Stocktake of Firm-Level Resilience Metrics

A summary of key findings from a cross-sector survey on how UK financial firms measure resilience.

Third Parties

Critical Sectors Risk Review

A review of the risk posed by the financial services sector dependencies on Critical National Infrastructure sectors.

Third Party Information Security Management

Guidance for UK financial firms on managing third party cyber risks, with NIST-aligned recommendations, a SolarWinds case study, and procurement security best practices.

Payments

Mortgages Advances and Property Completions Industry Playbook

Principles-based guidance for UK retail firms to support consistent customer outcomes during operational disruptions affecting mortgage advances and property completions.

FX Settlement Crisis Management Playbook

Sets out strategies, trigger points, operating principles and common/unilateral options for recovery and re-start of FX settlements in the event of unavailability of a critical third party or CLS.

Non-Standard Closure of Crest (NSCC) White Book

Outlines contingency procedures that explain how to cope with the impact of a major operational disruption in the CREST system or the wider market.

10 Annex: TLP Rating Definitions

Rating	Purpose	Sharing
TLP: RED, Not for disclosure, limited to participants only	Sources may use TLP: Red when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.
TLP: AMBER, Limited disclosure, restricted to participants' organisations	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved.	Recipients may only use TLP: AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
TLP: GREEN, Limited disclosure, restricted to the community	Sources may use TLP: GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released out of the community.
TLP: CLEAR, Disclosure is not limited	Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction