Bank of England | FCA FINANCIAL CONDUCT AUTHORITY | Bank of England PRA

Cyber risk and resilience management

FCA GC26/9 I PRA CP17/26

19 November 2026

1 Executive summary

1.1 Cyber threats continue to grow in frequency, sophistication and potential impact, as firms become increasingly reliant on technology and interconnected services. Greater digitalisation, complex third-party and supply-chain dependencies, geopolitical tensions, and the emergence of technologies such as artificial intelligence (AI) and quantum computing are also changing the threat landscape and increasing the potential for cyber incidents to cause significant disruption. Firms need strong basic cyber controls and the ability to detect, contain and recover quickly from incidents. This is vital to ensure their safety and soundness, maintain the orderly functioning of markets and protect consumers.

1.2 We, the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA) and the Bank of England (together 'the regulators'), have been pursuing a broad programme of work aimed at strengthening cyber resilience across the financial sector, including work to address cyber risks from emerging technologies such as AI and quantum computing. As part of this programme, we are now seeking views on a set of principles-based, outcomes-focused expectations on how firms should manage their cyber risk and resilience. These expectations would provide a foundational framework for effective cyber risk and resilience management, setting out clear outcomes firms should achieve.

1.3 Our proposals would not introduce new rules. Instead, they clarify how firms should meet current regulatory requirements on governance, operational resilience, operational risk and third-party risk in a cyber context. We anticipate that firms will welcome this additional clarity given the growing and rapidly changing nature of the cyber threat landscape. We will publish the finalised expectations (reflecting

feedback to this consultation) as a joint PRA/Bank supervisory statement (SS) and FCA Finalised Guidance (FG).

1.4 The proposed SS/FG reflects the progress firms have made in strengthening their operational resilience and supervisory insights and experience since we introduced the framework in 2021. Firms that have invested in operational resilience as a key strategic consideration should find it easier to meet our expectations without significant extra burden or costs.

1.5 Given the importance of effective cyber risk and resilience management to our objectives, and the rapidly evolving technology and threat landscape, we are likely to make additional regulatory and supervisory interventions in this area in the future.

1.6 The proposed SS/FG would apply to banks, insurers, financial market infrastructures (FMIs) and FCA-regulated firms that are subject to SYSC 15A operational resilience requirements. We recommend that other firms consider aligning to the National Cyber Security Centre (NCSC) Cyber Essentials: a government-backed, industry-supported scheme to help organisations identify how to protect themselves against common online threats. We also encourage these firms to consider other relevant NCSC guidance and tools, such as the Early Warning Service and Board Cyber Toolkit. These firms may also benefit from having cyber insurance cover in anticipation of potential cyber incidents, in the same manner as firms in scope of the guidance.

1.7 Proportionality and cross-sectoral and international interoperability are central themes throughout this consultation. A key proposal is for all in scope firms to refer to the NCSC Cyber Assessment Framework (CAF) as they develop and assess the maturity of their own cyber risk and resilience measures. Firms could also draw on their compliance with relevant international standards and regulation on cyber risk and resilience from non-UK financial authorities as evidence that they are meeting our expectations.

1.8 Alongside the proposed SS/FG, we have published two documents setting out current effective practices in relation to developments in AI and quantum computing. These are intended to help support firms in managing cyber risks related to these specific technologies. Given the rapidly-evolving nature of these technologies, these documents do not set supervisory expectations and are outside the scope of this consultation. However, we welcome comments on how they can be improved.

1.9 You can find the **draft proposed SS/FG in Annex 1**.

1.10 Please respond to this consultation by **26 February 2027**.

2 Overview

2.1 Cyber threats are evolving rapidly, and AI is increasing the speed, scale and sophistication of attacks, with the AI Security Institute and the NCSC reporting that AI is advancing more quickly than expected. AI-powered cyber defence may improve resilience over time, but there is an urgent need for firms to strengthen security now.

2.2 Good basic cyber hygiene remains fundamental to reducing risk, alongside robust plans to respond to and recover from cyber incidents. Boards and senior management should:

- recognise that resilience depends not only on preventing attacks, but also on ensuring organisations can detect, contain and recover from them quickly
- prioritise the outcomes we have set out in the draft SS/FG by giving cyber resilience leaders the authority and resources they need to strengthen their defences

2.3 Our proposed expectations for how firms should manage their cyber risk and resilience have been informed by lessons from:

- cyber incidents affecting the financial sector
- the regulators' supervision of cyber risk and resilience across firms, including thematic findings from threat intelligence-led penetration tests (CBEST and STAR-FS), supervisory questionnaires, and operational resilience self-assessments
- relevant information requests, multi-firm reviews and firm surveys
- technology developments, notably in AI and quantum computing

2.4 The expectations seek to clarify how firms should comply with existing regulatory requirements in the context of managing cyber risks. This approach seeks to:

- give firms clear technical guidance without imposing unduly prescriptive requirements
- enable firms to meet our expectations proportionately
- support effective and transparent engagement between firms and the regulators

2.5 While we are not proposing new rules, we do intend to use the expectations in the draft SS/FG when we supervise and enforce firms' compliance with our existing rules including those referred to in Annex 2 of the draft SS/FG.

2.6 The proposals complement existing rules, supervisory expectations, and guidance in relevant areas including:

- corporate governance
- operational resilience
- operational risk
- third-party risk management

2.7 They are designed to be interoperable with:

- cross-sectoral guidance, notably the NCSC's CAF
- relevant regulation and guidance for the financial sector by non-UK financial regulators and global standard-setting bodies (SSBs)

Scope

2.8 The expectations in the draft SS/FG would apply to:

- UK banks, building societies and designated investment firms
- Insurance and reinsurance firms and groups in scope of Solvency II, including the Society of Lloyd's and managing agents
- UK central counterparties, UK central securities depositaries, UK recognised payment system operators and UK specified service providers supervised by the Bank (collectively financial market infrastructure ('FMIs'))
- FCA solo-regulated firms subject to operational resilience requirements in SYSC 15A of the FCA Handbook. In addition to the dual-regulated firms referred to above, this includes:
  - enhanced scope Senior Managers & Certification Regime (SM&CR) firms
  - UK recognised investment exchanges
  - electronic money institutions
  - payment institutions
  - registered account information service providers
  - consolidated tape providers
  - qualifying cryptoasset firms (from 25 October 2027)

2.9 We refer to in-scope firms and FMIs collectively as 'firms' throughout the draft SS/FG and in this consultation (CP/GC).

2.10 The draft SS/FG would not apply to:

- credit unions
- non-directive insurance firms
- FCA solo-regulated firms that are not subject to operational resilience requirements in SYSC 15A
- UK branches of non-UK firms (third-country branches)
- non-UK FMIs

2.11 However, firms outside of scope of the proposed SS/FG would still be encouraged to refer to it in their cyber risk and resilience management.

2.12 The proposed exclusion of third-country branches and non-UK FMIs aligns to the scope of our requirements and expectations on operational resilience. However, we may still refer to the intended outcomes of the draft SS/FG when we assess a third-country branch's or non-UK FMI's implementation of cyber risk and resilience frameworks developed at parent or group level.

Interoperability with cross-sectoral and international standards

NCSC Cyber Assessment Framework (CAF)

2.13 The NCSC CAF is a key tool to help UK organisations assess and improve their cyber security and resilience, manage cyber risks and protect essential services. It supports both internal assessments and external oversight.

2.14 A key proposal in this CP/GC is for all in-scope firms to use the CAF's outcomes, objectives, and indicators to develop and assess their own cyber risk and resilience measures. The draft SS/FG sets out the **outcomes** that firms should achieve, with the CAF providing a way of **benchmarking** how they are achieving them. The draft SS/FG signposts the sections of the CAF which we would expect firms to refer to. We propose to use the CAF as a key benchmark in our supervisory engagement with firms.

2.15 As well as the CAF, we would expect firms to consider relevant guidance from the NCSC (as the UK's technical authority for cyber security), and the National Protective Security Authority (as the UK's technical authority for personnel and physical security).

Interoperability with global and international standards

2.16 Internationally active firms are subject to legislation, regulation and guidance on cyber risk and resilience management in their home jurisdictions and other jurisdictions where they operate. These often pursue similar outcomes to those in our draft SS/FG.

2.17 There is also a growing body of standards and guidance issued by the G7 Cyber Expert Group (CEG) and global SSBs including: the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Markets Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO), the Financial Stability Board (FSB), and the International Association of Insurance Supervisors (IAIS). These provide a global common foundation for cyber risk and resilience management in the financial sector. As far as possible, we have designed our expectations to be interoperable with these global standards, and legislation, regulation and guidance in other jurisdictions.

2.18 Interoperability does not mean duplication, equivalence or homogeneity. Firms would remain responsible for demonstrating to us that they are meeting our expectations. However, internationally active firms would be able to draw on their compliance with non-UK legislation, regulation, standards and guidance as supporting evidence of them meeting our expectations. They would also be able to consider relevant cross-sectoral guidance in the jurisdictions where they operate, including (but not limited to) the:

- US National Institute of Standards and Technology (NIST) Cyber Security Framework
- Cyber Risk Institute (CRI) Profile
- International Organization for Standardization (ISO) standards

The evolving technology landscape: artificial intelligence and quantum computing

2.19 The expectations in the draft SS/FG are technology-agnostic. They would apply to any technology that firms use. This is key to ensuring that our expectations remain adaptable and effective over time.

2.20 At the same time, we are keen that firms strengthen their ability to prepare for and respond to developments in certain technologies that could pose significant risks (notably AI and quantum computing).

2.21 Alongside the draft SS/FG, we have published two effective practices documents setting out how firms can manage cyber risks relating to AI and quantum computing respectively. These documents are complementary to, but separate from, the proposed SS/FG and highlight current effective practices. Given the fast-evolving landscape in these areas, they are not set as supervisory expectations. This approach will allow us to update these practices periodically to reflect changes in these technologies and the cyber threat landscape. While the documents are not formally part of this consultation, we intend for these documents to be useful for firms in practice and would welcome comments on how we can improve them.

Collective action

2.22 The financial services sector is highly interconnected. An issue that initially affects one firm or third party can go on to affect other firms or the wider sector. Collaboration is vital to address these issues. While our expectations are addressed to individual firms, we strongly encourage firms to engage with collective action and incident response frameworks to enhance both individual and collective cyber risk and resilience management. These include, but are not limited to, the Cross-Market Operational Resilience Group (CMORG) and the Financial Services Cyber Collaboration Centre (FSCCC).

Implementation

2.23 After the consultation process, we expect to publish a Policy/Feedback Statement including a final version of the SS/FG. Given the evolving threat landscape, cyber risk and resilience management is likely to remain a supervisory priority and key area of focus in the foreseeable future, with continued supervisory attention to firms' ability to anticipate risks and manage the impact of disruptions.

Responses

2.24 We invite responses to our proposals set out in this consultation by Friday 26 February 2027. See 'Responding to the Consultation' below for details on how to respond and for information on how we will handle your personal data.

3 Our proposals

Structure of the draft SS/FG

3.1 The draft SS/FG covers the following areas:

- **Governance:** How a firm should embed cyber risk and resilience management in its corporate governance and risk management frameworks.
- **Identification and assessment:** How a firm should identify, assess, and understand its assets and the cyber risks it faces, including the implications for its resilience.
- **Protection:** How a firm should implement capabilities and controls to protect against cyber risk and enhance its cyber resilience.
- **Detection:** How a firm should implement capabilities and controls to detect cyber events and incidents.
- **Response and recovery:** How a firm should respond to and recover from cyber incidents.
- **Assurance and continuous improvement:** How a firm should gain assurance on the continued effectiveness of its cyber risk and resilience management capabilities and controls.

3.2 Our expectations in different chapters of the draft SS/FG are complementary and mutually reinforcing. We would expect firms to consider how their cyber capabilities and controls work on their own and in coordination with other areas – for example, how detection capabilities and controls support incident response and recovery.

Overarching principles (Chapter 2)

3.3 This chapter covers principles which underpin our expectations such as alignment to cross-sectoral and international standards and the importance of collective action. It also sets out that in line with the principle of proportionality, and to avoid unnecessary burden, firms should implement the expectations in the SS/FG in a way that reflects their size, complexity and risk profile.

Governance (Chapter 3)

3.4 We already hold boards and senior management responsible for their firms' operational resilience, operational risk management and third-party risk management, among other areas. Given the evolving cyber threat landscape, we think it is essential that cyber risk and resilience are treated with the same importance and rigour as other key risks facing firms. Cyber risk is not just a technology issue; it is a business and strategic risk that could adversely impact firms, counterparties and customers – and, in some cases, the financial system.

3.5 The draft SS/FG therefore includes expectations which set out and underscore the role of the board and senior management in establishing and owning clear and effective governance arrangements for cyber risk and resilience management (cyber

governance). The proposed expectations cover five areas which should collectively help firms to:

- establish clear accountability for cyber risk
- improve oversight and challenge
- support informed decision-making
- identify, escalate and manage cyber risks and incidents in a timely way

Board oversight and accountability

3.6 The draft SS/FG clarifies the board and senior management's responsibility for a firm's cyber governance, which should be consistent with and form part of its overall risk management framework. It sets out expectations for the board and senior management to be clearly accountable and own a firm's cyber governance.

Experience, knowledge and skills of the board

3.7 The draft SS/FG includes expectations for the board to maintain sufficient collective knowledge, skills and experience to appropriately understand the cyber threat landscape and the main cyber risks facing the firm. We consider that this helps them deliver effective and informed oversight of firms and challenge senior management, where appropriate. We do not expect every board member to become a cyber expert, but they should all attain and maintain a sufficient understanding of cyber issues.

Risk culture

3.8 People are a critical, but often underemphasised, component of cyber risk and resilience management. The draft SS/FG includes expectations for firms to promote a strong cyber risk culture, recognising the role of all staff in managing cyber risks and resilience (including employees, contractors and secondees).

Documentation and Management Information (MI)

3.9 Firms should adequately document their cyber risk and resilience strategy, policies, procedures and measures. The draft SS/FG proposes that the board makes sure it receives MI relating to cyber risk and resilience management. MI should provide clear, useful and timely information on the firms' cyber risk and resilience so that the board can oversee, challenge and make decisions effectively.

Senior management responsibilities

3.10 Senior managers play a critical role in translating board-approved strategies into actions to strengthen firms' cyber risk and resilience. The draft SS/FG sets out that firms should assign ownership for cyber risk and resilience to a senior manager with appropriate authority, experience and functional independence. For firms subject to the Senior Managers Regime, this would include an appropriate Senior Management Function (SMF) holder, such as the Chief Operations Function (SMF24).

3.11 All senior managers should actively manage risks within their areas of responsibility. The draft SS/FG sets out how this applies in the context of cyber risk and resilience, for example, by ensuring appropriate cyber hygiene and managing risks from the use of unauthorised information and communications technology including AI-based applications.

Identification and Assessment (Chapter 4)

3.12 The draft SS/FG sets out that firms should appropriately document and understand their technology estate and the key cyber risks they face. They need this foundation to identify their most critical assets, how those assets connect to and depend on each other, any weaknesses and how cyber disruption could spread across the firm.

3.13 The proposed expectations aim to help firms make informed decisions and prevent, detect, respond to and recover from cyber incidents.

Identification of assets

3.14 We propose that firms maintain a comprehensive, documented and up-to-date inventory of assets relevant to their cyber risk and resilience. These assets include data, hardware, software and third-party and key supply chain dependencies. Firms could use data from existing documents, such as bills of materials, operational resilience maps, self-assessments, and third-party registers. We also propose that firms identify and prioritise key assets and manage them effectively across their lifecycle. Firms should regularly update their asset inventories, particularly in response to events such as major cyber incidents or material changes in their information and communications technology infrastructure.

Identification of cyber risks

3.15 We also propose that firms identify, assess, understand and document the cyber risks they are exposed to. They should monitor for new cyber risks including, but not limited to, those arising from geopolitical events or rapid changes in technology.

3.16 Given the rapidly evolving cyber threat landscape, it is important for firms to use threat intelligence. They should be able to demonstrate to supervisors how they have used this to identify and assess risks, and make decisions about capabilities, controls, priorities and resources.

3.17 To help identify risks, firms should identify, assess and understand their vulnerabilities. Boards and senior managers should set a risk appetite on key control indicators for vulnerability management.

Protection (Chapter 5)

3.18 Appropriate and proportionate protective capabilities and controls are key to reducing the likelihood of cyber risks crystallising and pre-emptively limiting their impact when they do.

3.19 We assess firms' protective capabilities through supervisory activities such as CBEST, STAR-FS, SIMEX, and the Cyber and Operational Resilience Stress Test. These activities have highlighted the importance of certain principles that should inform firms' protective capabilities, including:

- defence-in-depth, with layers of interlocking controls (people, processes, and technology)
- infrastructure, network, and data security including:
  - secure network configuration
  - embedding controls from inception (secure-by-design)
  - providing read-only access to sensitive data if broader access is unnecessary

- applying the strictest controls as a baseline (secure-by-default)
- identity and access management controls including restricting access to the minimum necessary to accomplish tasks (least privilege)

Identity and access control

3.20 The draft SS/FG proposes that firms have robust identity and access controls in line with the principle of least privilege to ensure that only authorised users can access their critical assets. 'Users' include people as well as services and technology such as AI agents and automated processes.

3.21 We also propose that firms verify, authenticate, and authorise identities before granting access. They should use stronger authentication, such as multi-factor authentication, where there is a potential risk to the delivery of important business services or critical operations.

3.22 Firms should maintain effective, timely processes for creating, changing, reviewing and removing access rights. These should align with 'zero trust' principles where access is not assumed but is verified and restricted to the minimum level necessary.

Data security

3.23 Data is a vital asset for firms, making data security a pivotal component of effective cyber defence. The draft SS/FG proposes that firms identify and classify data according to criticality, sensitivity and risk and protect it throughout its lifecycle. Other proposals for firm's data security include applying appropriate access and cryptographic controls (guided by relevant post-quantum cryptographic (PQC) standards), managing risks from external processing, maintaining data integrity and recoverability, and securely disposing of data when no longer required.

System security

3.24 The draft SS/FG sets out that firms should reduce the risk of cyber incidents through effective system security. This includes controlled, consistently applied and well-governed configuration and systems management, and patching and vulnerability management practices.

Physical security

3.25 Firms' cyber security and resilience depend on physical assets that are often overlooked. These range from business premises to data centres, telecommunications infrastructure and undersea cables. Some of these assets may be owned and managed by third parties.

3.26 Consequently, we propose that firms have robust physical security controls which should be designed to prevent, detect, and respond to attempts to gain unauthorised access to physical assets, networks, data, or operational technology whether by insiders, contractors or hostile actors.

People security

3.27 Many cyber incidents originate from compromised or malicious individuals with privileged access to a firm's assets, or simple human error.

3.28 The draft SS/FG therefore proposes that firms have appropriate, preventative controls for insider-risks, and that they review them regularly as part of a secure-by-

design approach. These should include acceptable use policies for relevant situations such as staff using their own devices for work and accessing social media.

Digital customer journeys

3.29 We propose that firms consider the cyber security and resilience of their end-to-end digital customer journeys. Firms should consider controls to address risks such as abnormal transactions, compromised credentials or unauthorised access.

Detection (Chapter 6)

3.30 To respond to cyber incidents effectively, firms need to be able to detect them quickly in the first place. The 2025 CBEST thematic review highlighted insufficient detection as a common weakness among firms, which can hamper their incident management and exacerbate operational disruption. The draft SS/FG proposes that firms should monitor all their key risk areas appropriately and review and update their methods and technology to progressively strengthen their detection capabilities. Firms should detect, log and analyse cyber events and incidents to support robust incident management and continuous improvement.

Response and recovery (Chapter 7)

3.31 Firms should assume there will be some operational disruption from cyber incidents and maintain effective response and recovery arrangements to limit their impact.

3.32 We propose that firms have arrangements to promptly and effectively contain and eradicate cyber incidents, restore services and minimise the impact of disruption on firms and the wider financial system (see sub-sections below).

3.33 We expect firms should prepare for a range of incidents, including severe but plausible cyber incidents, and adapt their response and recovery arrangements as threats, technologies and business models evolve.

Governance

3.34 The draft SS/FG proposes that firms have clear governance and accountability arrangements for cyber incident response and recovery to support a timely and coordinated response. These may only be activated during incidents, so may need different decision-making structures from business-as-usual arrangements.

Cyber incident response and recovery (CR&R) plan

3.35 To support timely and effective response to and recovery from cyber incidents we propose that firms have a documented and proportionate CR&R plan. A CR&R plan is an umbrella term covering any documents relevant to cyber response and recovery arrangements. There is no specific format or template for the firm's CR&R plan. The plan should set out key response and recovery actions, decision points and escalation arrangements, and be kept up to date to reflect evolving threats and lessons learned.

Coordination and collective incident response

3.36 There should be a coordinated response across the financial sector (and other sectors) where there is a sector-wide or systemic cyber incident. We therefore

propose that a firm's CR&R plan include measures for coordinating with Collective Incident Response Frameworks including the Sector Response Framework (SRF), which is owned and maintained by CMORG. Firms should test their ability to coordinate and communicate with key external stakeholders during a cyber disruption, including through joint exercises.

Response

3.37 The draft SS/FG proposes expectations to strengthen firms' ability to respond to cyber incidents which aim to limit the impact of disruption for firms, support the continued delivery of important business services within impact tolerances and restore a secure operating environment.

3.38 To support these outcomes, we expect firms to analyse, contain, mitigate, remediate and eradicate cyber incidents in a timely manner.

Recovery

3.39 The draft SS/FG also proposes that firms have cyber recovery arrangements that should be distinct from, but complementary to, their response arrangements. They should focus on the firms' ability to restore important business services within impact tolerances and return affected systems, infrastructure and data to a trusted operational state.

3.40 Firms should test the on-going effectiveness of their recovery arrangements especially where external or internal dependencies are compromised, degraded or unavailable. We also expect that they develop appropriate capabilities (such as bare metal recovery) to deal with high severity cyber incidents affecting important business services.

Assurance and continuous improvement (Chapter 8)

3.41 The draft SS/FG sets expectations for firms to assess the effectiveness of their arrangements across the cyber resilience lifecycle, through a risk-based cyber assurance programme. They should use a range of testing, exercising, and assurance activities, including threat intelligence-led assessments where appropriate. This should help firms identify weaknesses and enable them to continuously improve their cyber risk and resilience management.

4 The regulators' objectives, cost benefit and 'have regards' analysis

The FCA's strategic and operational objective: integrity

4.1 Cyber is regularly cited by the industry as one of the top sources of risk to the UK financial system. The proposed SS/FG aims to strengthen the resilience of individual firms, and in turn the sector. The proposals do not introduce new rules but clarify existing expectations to support firms to meet an appropriate standard.

4.2 The FCA considers that the proposed SS/FG advances its strategic objective of ensuring that relevant markets function well, and its operational objective to protect and enhance the integrity of the UK financial system.

The FCA's operational objective: consumer protection

4.3 The proposals in this CP/GC do not directly address consumers. However, consumers benefit from resilient services through lower risk of disruption, failure, and related harms. The FCA considers that the proposals advance its objective to secure an appropriate degree of protection for consumers.

The FCA's operational objective and duty: competition

4.4 The guidance does not directly affect competition within the relevant markets under the FCA's competition objective. Consumers may be unable to assess a firm's cyber resilience, so firms' investment in resilience may not be fully rewarded. By strengthening firms' resilience, the guidance can address the consequences of this information asymmetry even where it does not directly impact market competition. The FCA considers that the proposals are compatible with its competition duty and objective.

The Bank's primary objective

4.5 The Bank considers that the proposals in the CP/GC support its primary objective of protecting and enhancing the stability of the UK financial system. Clarifying existing requirements through clear, outcomes-focused expectations for how firms should identify, manage and mitigate cyber risk can help to improve the reliability and resilience of their critical operations. This is particularly important because FMIs sit at the heart of the financial system, and disruption to their services could have significant consequences for financial stability.

4.6 The proposed SS/FG clarifies how existing regulatory requirements apply and consolidates related supervisory expectations and relevant good practices. The Bank considers that this should support a more consistent understanding and implementation of existing requirements and expectations across firms.

The PRA's primary objective

4.7 The PRA considers that the proposals in this CP/GC support its primary objective of promoting the safety and soundness of PRA-authorised firms and, for insurers, contributing to an appropriate degree of protection for policyholders.

4.8 Weaknesses in cyber risk management can lead to operational disruption, financial loss, harm to consumers and policyholders, and, in some circumstances, wider risks to confidence in, and the stability of, the financial system. The draft SS/FG does not introduce new regulatory requirements. Rather, it clarifies existing requirements, supervisory expectations and provides relevant good practice. The PRA considers that this greater clarity and coherence should support a more consistent understanding and implementation of existing requirements and expectations across firms.

4.9 By supporting more effective and consistent management of cyber risks, the proposals are intended to strengthen firms' operational resilience and reduce the likelihood and impact of cyber-related disruption.

The PRA's secondary objective: competition

4.10 Proportionality is embedded throughout the draft SS/FG so firms can achieve the intended resilience outcomes in a manner appropriate to their size, complexity and risk profile. Firms may also use existing governance arrangements, risk management frameworks and controls where they are effective. The PRA considers that this approach allows flexibility and helps to avoid unnecessary burdens, particularly for smaller and less complex firms, while supporting effective competition across the sector.

The FCA and PRA competitiveness and growth objective

4.11 Enhanced operational resilience of firms helps to ensure the UK's financial sector is underpinned by a stable and secure digital infrastructure. This is essential for international competitiveness and effectiveness in today's technology-driven environment. While the proposals may give rise to implementation costs for firms with gaps in their existing cyber resilience, the PRA and FCA have tried to minimise those costs through our outcomes-focused and proportionate approach. On balance, the PRA and FCA consider that the proposals facilitate international competitiveness and growth by supporting the resilience of regulated firms and maintaining confidence in the UK financial sector as firms adopt new technologies and pursue innovation.

4.12 The proposals in this CP/GC align, as far as possible, with international best practices and regulatory standards in other jurisdictions. This promotes regulatory consistency and facilitates cross-border operations, supporting firms with global footprints. This approach helps reduce fragmentation across regulatory frameworks, while still delivering the intended resilience outcomes.

The Bank's secondary objective

4.13 The Bank considers that the technology-neutral and outcomes-focused nature of the proposals set out in the CP/GC advances its secondary objective to facilitate innovation in the provision of central counterparty (CCP) and central securities depository (CSD) services.

4.14 By improving their cyber resilience, FMIs are able to innovate safely without disruption to the provision of their services. The expectations do not prescribe use of particular technologies or solutions, which provides FMIs with flexibility in how they achieve the required outcomes.

4.15 Proportionality is embedded in the Bank's proposed expectations, allowing FMIs flexibility to achieve the intended resilience outcomes in a manner appropriate to their size, complexity and risk profile. FMIs may also leverage existing governance arrangements, risk management frameworks and controls where these are effective. The Bank considers that this approach helps to avoid unnecessary burdens, particularly for smaller and less complex FMIs.

Significant factors to which the regulators have 'had regard'

The regulators have considered our various 'have regards'. Where a factor is relevant to more than one regulator, it has been considered jointly. We consider the following to be most relevant:

- **Proportionality**: The draft SS/FG clarifies how existing requirements apply in a cyber context rather than introducing new rules. We consider this a proportionate response to the risks being addressed. It gives firms greater clarity without the additional burden that could arise from new cyber-specific rules. The proposed expectations are principles-based and outcomes-focused, allowing firms to implement them in a manner appropriate to their size, complexity, business model and risk profile. Firms can draw on existing cyber capabilities and compliance activity, including work to meet relevant domestic and international standards, rather than duplicate it. Some firms may nevertheless need to strengthen their cyber resilience arrangements. We consider any resulting costs to be proportionate to the risks being addressed and justified by the benefits of stronger cyber resilience at the firm and across the sector.
- **Growth, competition and innovation:** We have had regard to the contribution of the financial services sector to overall economic growth and to creating a regulatory environment that facilitates growth through competition and innovation. By helping to reduce the likelihood and impact of cyber-related disruption, the proposals can help maintain confidence in the provision of financial services and support the safe adoption of new technologies. The proposed expectations do not prescribe particular technologies or implementation approaches, affording firms flexibility in their implementation, and leaving room for innovation while firms manage the risks they face. Alignment with domestic and international frameworks, where appropriate, should also reduce unnecessary duplication and regulatory complexity particularly for firms operating across jurisdictions.
- **Efficient and economic use of regulatory resources:** A clear, public articulation of our expectations should reduce the need for supervisors to clarify existing requirements with firms on a case-by-case basis. It should also support

greater consistency in supervisory assessments and a more structured, risk-based supervisory approach. The proposed SS/FG has been designed to complement existing regulatory frameworks which should support coherent supervisory judgments across related policy areas.

- **Transparency**: The proposals in this CP/GC are anchored on existing rules and expectations. We consider that providing greater clarity and guidance on how firms can meet these requirements and further strengthen their cyber resilience improves transparency regarding our supervisory expectations.

Significant factors to which the Bank has 'had regard'

4.16 When making policy for CCPs and CSDs, the Bank must 'have regard' to certain public policy considerations set out in the Bank of England Act 1998 as amended by FSMA 2023, and HMT's FMIC remit letter recommendations. The 'have regards' considered most significant to all regulators are discussed above in 'Significant factors to which the regulators have 'had regard'' above. Other have regards considered significant to the Bank are discussed below.

- **Financial Stability:** As noted above in the section discussing the Bank's primary objective, the Bank considers the expectations should improve the operational resilience of FMIs that typically operate globally, which improves the financial stability of both the UK and other jurisdictions.

Cost benefit analysis (CBA)

4.17 The PRA and FCA's CBA Panels were not consulted in connection with these proposals, as we are not proposing new rules and the annualised central cost estimate falls below the threshold for doing so.

The case for regulatory action

4.18 The financial sector is operating in an environment of heightened cyber risk. Exposure to sophisticated and persistent threats is intensifying as digitalisation accelerates, including through greater reliance on third-party services, advances in artificial intelligence, and development of increasingly interdependent supply chains.[1] These changes can support innovation and efficiency, but they also widen the channels through which cyber disruption can arise and propagate across firms, services and sectors.

4.19 Recent assessments of cyber resilience across UK financial firms continue to identify shortcomings in capabilities, governance, threat response and forward-looking risk management. The Bank's 2025 CBEST thematic identified gaps in firms' cyber defences across people, processes and technology. [2] CQUEST findings for smaller and medium-sized UK deposit takers similarly identified gaps.

4.20 FCA industry insights also highlight continuing challenges in third-party and threat and vulnerability management, threat-led penetration testing, legacy technology and emerging technologies.[3] Taken together, evidence suggests that, while firms have made progress, gaps remain in their ability to anticipate, prevent, withstand and

[1] Bank of England, '2025 CBEST thematic', 20 January 2026, https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/2025-cbest-thematic.

[2] Ibid.

[3] Financial Conduct Authority, 'FCA Cyber Coordination Group Insights 2024', published 14 August 2025, updated 27 August 2025, available at: https://www.fca.org.uk/publications/good-and-poor-practice/fca-cyber-coordination-group-insights-2024.

recover from cyber incidents. These gaps can affect not only firms' own safety and soundness, but also customers' and counterparties' confidence in the services they provide and, in some circumstances, the stability of the wider financial system.

4.21 It is in firms' own interests to be operationally resilient. They have private incentives to manage cyber risk effectively and to build and maintain their cyber resilience. For this reason, many firms continue to invest heavily in cyber resilience and regard this as a growing cost element, particularly in light of technological development such as frontier AI. However, market failures may nonetheless lead to firms underinvesting in cyber risk and resilience management, relative to the significance of the risks. As set out in the Government's impact assessment for the Cyber Security and Resilience Bill, these include information asymmetries, externalities, and coordination failures:[4]

- **Information asymmetries:** Firms, customers and counterparties may have incomplete information about the resilience of the organisations and technology providers on which they depend;
- **Externalities:** Weaknesses at one firm may impose costs on others through disruption to important services, shared infrastructure or interconnected supply chains; and
- **Coordination failures:** Effective resilience may in some respects require coordinated action across firms, service providers, infrastructure providers and public authorities.

4.22 These market failures can be compounded by rapid technological change and the cross-border nature of cyber threats. The outcome can be that firms may therefore invest less in cyber resilience than would be desirable for the wider financial system.

4.23 The regulators' principal response to these market failures is the framework of rules, expectations and guidance already in place and being acted on by firms in relevant areas including corporate governance, operational resilience, operational risk, and third-party risk management. However, the regulators consider that supplementing this existing framework with clear and proportionate expectations, specifically pertaining to cyber risk and resilience management, can further contribute to addressing the sector's observed shortcomings in this area.

4.24 By making the expected outcomes clearer, the draft SS/FG can help firms assess their existing arrangements, identify any shortcomings and prioritise proportionate remedial changes. It can also provide a clearer basis for supervisory engagement on those shortcomings. These changes should enhance firms' cyber risk and resilience management.

4.25 The proposals may thereby achieve benefits through reducing the likelihood or frequency of cyber incidents; or through the earlier detection and improved containment of cyber incidents, preventing manageable events becoming severe; or though more effective response and recovery arrangements that shorten disruption and allow firms to address incidents more promptly and effectively. The avoided (or reduced) consequences may include lost income, response and recovery costs, customer compensation, legal and professional fees, costs arising from data loss, and longer-term effects on reputation, customer retention and firm value. Customers and policyholders may benefit from more reliable access to services and better protection of confidential information. At the sector level, reducing the likelihood or impact of disruption at firms can help maintain confidence in the financial system.

[4] Department for Science, Innovation and Technology, Final stage impact assessment: Cyber Security and Resilience (Network and Information Systems) Bill, 12 November 2025, p. 9.

4.26 If the proposals were not introduced, existing rules, expectations and guidance would continue to apply. Firms would continue to invest in cyber resilience in response to their own incentives, existing requirements and the evolving threat environment. However, the regulators consider that without clearer and more consolidated expectations, some or all of the identified gaps may persist or take longer to address for some firms. The CBA analysis therefore focuses only on impacts that are attributable to the specific proposals, rather than costs and benefits of all improvements in firms' cyber resilience that firms are undertaking on their own initiative and in response to pre-existing rules and expectations.

Estimated costs of the proposals

4.27 It is challenging to quantitatively estimate the incremental costs of these policy proposals, as they do not introduce new rules but instead clarify how firms should apply existing rules to the management of cyber risk and resilience. A strict approach to cost attribution would exclude expenditure firms would already need to incur to comply with existing rules, even without the proposed SS/FG. It might therefore suggest little or no additional compliance cost in light of the expectations. In practice, however, publication of clearer and more specific expectations is likely to prompt firms to review their arrangements and, where necessary, make remedial changes. We have therefore estimated the marginal costs to firms to which the proposals are likely to give rise.[5]

4.28 The proposals are not intended to generate significant incremental work for firms, as the expectations are flexible, outcomes-focussed and proportionate. However, all firms will need to familiarise themselves with the expectations, identify any gaps in their current arrangements and, where needed, make changes to remedy them. The extent and cost of these changes will depend on firms' existing arrangements, with firms already largely meeting the intended outcomes expected to incur lower costs than those with more significant gaps. We do not consider that the expectations in themselves would entail costly new technology projects, even though firms may undertake such projects in their private interests or to meet existing requirements.

4.29 The estimates below reflect the current technology and threat environment. Significant changes in either, including advances in the cyber capabilities of frontier AI models, could materially affect the costs firms incur in meeting the expectations.

PRA-regulated firms[6]

4.30 For PRA-regulated firms, the PRA estimates one-off implementation costs of £14.9 million and annual ongoing costs of £2.5 million. Together, these equate to an annualised cost of £4.2 million over ten years.

Cost measure	Central estimate
One-off implementation costs	£14.9 million
Annual ongoing costs	£2.5 million
Annualised cost over ten years	£4.2 million

[5] The cost estimates cover 427 PRA-regulated firms, 10 Bank-regulated financial market infrastructures (FMIs), and approximately 1,700 FCA solo-regulated firms. These are the populations used for the cost modelling.

[6] Including PRA and FCA dual regulated firms.

4.31 The primary method the PRA used to produce these estimates was the PRA's Standard Cost Model (SCM). For each of the six substantive chapters of the draft SS/FG, the PRA identified incremental activities likely to arise from the publication of the expectations in that chapter, while seeking to exclude the cost of existing cyber-security, operational-risk and operational-resilience capabilities. The SCM converts estimated staff time into monetary costs using salary assumptions and includes allowances for project management and board oversight.

4.32 The cost estimates are primarily staff-driven, reflecting the time required for familiarisation, reviewing and updating policies and processes, and training. The PRA has therefore tested the sensitivity of its central cost estimates to a scenario in which the average staff effort required to meet the expectations is higher than anticipated. Increasing the assumed one-off and ongoing staff effort by 50% raises the annualised estimate from £4.2 million to approximately £6.2 million. This scenario illustrates the effect of changing some of the underlying assumptions of the CBA; it is not an estimate of the most likely additional cost.

4.33 In addition to this 'bottom-up' methodology for estimating costs, the PRA also used, as a cross-check, a 'top-down' methodology to arrive at a separate estimate of costs. This methodology adapted assumptions used in the European Commission's 2020 impact assessment for the Digital Operational Resilience Act (DORA), together with published benchmarks for cyber-security expenditure in financial services. Unlike the SCM, which builds up costs from the staff activities associated with individual expectations, the top-down approach starts from benchmarks for firms' overall cyber-security expenditure and estimates the additional spending that firms investing below those benchmarks might require. Applied to banking firms, this produced illustrative annual costs of £1.0 million–£2.6 million, depending on the benchmark used. These estimates provide a broad cross-check rather than a like-for-like comparison with the SCM, as they cover banking firms only and do not separately identify one-off implementation costs.

FMIs

4.34 Across the population of Bank-regulated FMIs, the Bank estimates one-off implementation costs of £730,000, annual ongoing costs of £58,000 and an annualised cost of £140,000 over ten years.

Cost measure	Central estimate
One-off implementation costs	£730,000
Annual ongoing costs	£58,000
Annualised cost over ten years	£140,000

4.35 The primary method the Bank used to produce these estimates was the PRA's SCM. For each of the six substantive chapters of the draft SS/FG, the Bank identified incremental activities likely to arise from the publication of the expectations in that chapter, while excluding the cost of existing cyber-security, operational-risk and operational-resilience capabilities.

FCA solo-regulated firms

4.36 For solo-regulated firms, the FCA estimates one-off implementation costs of £7.8m, annual ongoing costs of £1.7m and an annualised cost of £2.6m. As benefits have not been quantified, the Equivalent Annual Net Direct Cost to Business (EANDCB) is equal to the annualised cost of £2.6m.

Cost measure	Central estimate
One-off implementation costs	£7.8 million
Annual ongoing costs	£1.7 million
Annualised cost over ten years	£2.6 million

4.37 The FCA estimates there are around 1,700 in-scope FCA solo-regulated firms that are expected to incur costs to comply with the FG. These costs were estimated using the FCA's Standardised Cost Model (see Appendix 1 of the FCA's Statement of Policy on Cost Benefit Analyses) and vary by firm size. The estimates cover familiarisation, gap analysis, training and changes to existing processes attributable to the proposals, excluding the costs of existing capabilities.

Cost measure	Large firms	Medium firms	Small firms
One-off implementation costs	£25,000	£7,900	£1,400
Annual ongoing costs	£3,700	£1,700	£500

4.38 Across the three regulators, these cost estimates sum to an **expected total annualised cost of approximately £7.0 million** to PRA-regulated firms, FCA solo-regulated firms and Bank-regulated FMIs.

Benefits of the proposals

4.39 The regulators cannot produce a precise estimate of the reduction in cyber losses specifically attributable to the proposals. The regulators have therefore considered break-even analysis rather than forecasting a particular number of incidents prevented or mitigated.

4.40 The available evidence shows that cyber losses vary widely by incident type and severity and firm size. However, as an illustration, the regulators' analysis identified 33 reported cyber incidents involving a data breach in 2024. [7] The regulators considered this in conjunction with IBM's estimated average cost of £6.05 million for a UK financial services data breach. [8] The published IBM material does not establish how closely the firms underlying this average correspond to the firms in scope of these proposals, or how sensitive the average is to unusually costly breaches. The figure is therefore used as an illustrative benchmark, rather than a verified figure for losses across the regulated population. Multiplying the number of incidents by average cost gives an illustrative annual cost of incidents of approximately £200 million.

[7] Financial Conduct Authority, *Information on cyber incidents – May 2025*, Freedom of Information response FOI12270, 13 May 2025, available at: FCA information on cyber incidents.

[8] IBM, *IBM Report: Soaring Data Breach Disruption Drive Costs to Record Levels*, 30 July 2024, available at: IBM's UK 2024 Cost of a Data Breach findings.

4.41 Compared with the combined annualised cost estimate of £7.0 million across PRA-regulated firms, FCA solo-regulated firms and Bank-regulated FMIs, annual avoided losses of £7.0 million would be needed for the proposals to break even. This is equivalent to approximately 3.5% of the illustrative annual incident cost of £200 million. In other words, on this illustrative basis, if the proposals reduced the annual cost of cyber incidents by 3.5%, the resulting avoided losses would offset the estimated annualised costs of the proposals. This percentage is a break-even threshold, not an estimate of the reduction the proposals would achieve. Such a reduction could arise through fewer successful incidents, earlier detection, improved containment or faster recovery.

4.42 This comparison is clearly indicative. The incident count and average cost do not necessarily cover exactly the same population as the joint cost estimates for the regulators' proposals, and data breaches are only one category of incident relevant to the proposals. The calculation also does not quantify wider benefits to customers and policyholders, confidence or financial stability.

5 Additional information

Consultation with statutory panels

5.1 The FCA Practitioner Panel, Smaller Business Practitioner Panel, and Markets Practitioner Panel were consulted about all the proposals in this CP/GC. The PRA Practitioner Panel was consulted about all the proposals in this CP/GC.

Impact on mutuals

5.2 The regulators consider that the impact of the proposed expectations on mutuals is expected to be no different from the impact on other firms.

Equality and diversity

5.3 In developing its proposals, the regulators have had due regard to the equality objectives under s.149 of the Equality Act 2010. The regulators consider that the proposals do not give rise to equality and diversity implications because the expectations relate to firms' cyber risk and resilience management arrangements rather than to individuals.

Other factors to which the regulators have 'had regard'

5.4 In developing these proposals, the PRA and the FCA have had regard to the FSMA regulatory principles and the aspects of the Government's economic policy as set out in the relevant HMT recommendation letter from November 2024. The Bank, in respect of CCPs and CSDs, has had regard to certain public policy considerations set out in the Bank of England Act 1998 as amended by FSMA 2023, and HMT's FMIC remit letter recommendations. The regulators have set out their views on the 'have regards' they consider significant above.

5.5 The regulators have had regard to other factors as required. Where analysis has not been provided against a 'have regard' in this document, it is because the regulators consider that 'have regard' to not be a significant factor for these proposals.

1 Consultation questions

Q1: Do you have any general comments on the regulators' principles-based, outcomes-focused, technology-neutral expectations set out in the draft SS/FG?

Q2: Do you have any specific comments on the proposed expectations in the draft SS/FG across the technical chapters? In particular:

- Chapter 3-Governance
- Chapter 4-Identification and Assessment
- Chapter 5-Protection
- Chapter 6-Detection
- Chapter 7-Response and Recovery
- Chapter 8-Assurance and Continuous Improvement

Q3: Are there any areas where it would be helpful to have more detail on the cyber resilience outcomes firms are expected to achieve? If so, where?

Q4: Do you have any comments on the regulators' proposed approach to proportionality in the draft SS/FG? In your view, is further clarity needed on how firms should apply the expectations in a manner proportionate to their size, business model, risk profile, and systemic importance? If so, where, and in what way?

Q5: Do you agree with the proposal for firms in scope of the draft SS/FG to refer to the NCSC's Cyber Assessment Framework (CAF) to develop and assess their own cyber risk and resilience measures?

Q6: Do you have any comments on the regulators' approach to interoperability with other standards and frameworks?

Q7: Do you have any comments on the Cost Benefit Analysis (CBA), in particular, the distinction between incremental costs arising from the proposed expectations and the costs associated with existing legal or regulatory obligations or firms' own cyber risk and resilience management activities?

2 Responding to the consultation

Your personal information

2.1 By responding to the consultation, you share personal data with the regulators, which may include your name, contact details, (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

2.2 To read how the FCA will use your response and how it will be disclosed, visit: Consultation responses: your confidentiality and personal data | FCA . Further information about the FCA's use of personal data can be found on the FCA's website: Privacy notice | FCA.

2.3 For more information about how the PRA handles responses to PRA consultations see: PRA consultations and discussion papers - your personal data. You have several rights under data protection laws in relation to data held about you. For further information on exercising these rights, including how to contact the relevant Data Protection Officer, please visit Privacy and the Bank of England.

2.4 By responding to this consultation, you provide personal data to the Bank of England. This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself. The response will be assessed to inform our work as regulators and a central bank, both in the public interest and in the exercise of our official authority. We may use your details to contact you to clarify any aspects of your response. We will retain all responses for the period that is relevant to supporting ongoing regulatory policy developments and reviews. However, all personal data will be redacted from the responses within five years of receipt. To find out more about how the Bank deals with your personal data, your rights, or to get in touch please visit Privacy and the Bank of England.

Responses

2.5 The regulators invite responses to the proposals set out in this consultation by **Friday 26 February 2027**. Feedback on the separate AI and quantum effective practices can also be submitted along with feedback to this consultation.

2.6 Please indicate in your response if you believe any of the proposals in this consultation paper are likely to impact persons who share protected characteristics under the Equality Act 2010, and if so, please explain which groups and what the impact on such groups might be.

2.7 We will publish a general summary of responses to this consultation and are required to include respondents' names if consent is given. When responding, please clearly indicate whether or not you consent to us publishing your name, and/or the name of your organisation, as a respondent to this CP/GC. Please make it clear if you are responding as an individual or on behalf of an organisation. Consent can be withheld or withdrawn at any time. If you wish to withdraw your consent to us publishing your name, please contact the regulators using the contact details set out below. If you do

not give consent to us publishing your name, we may still collect, record and store your response in accordance with the information provided above.

2.8 Please address any comments or enquiries to GC26-9@fca.org.uk and CP17_26@bankofengland.co.uk.

Annex 1 Draft non-Handbook guidance / Supervisory Statement: Cyber risk and resilience management

1 Introduction

1.1 This document is issued jointly by the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA), and the Bank of England (the Bank) (collectively, the regulators). Where the document refers to 'we', 'us', 'our', this means the regulators collectively.

1.2 The document serves as Finalised Guidance (FG) in relation to the FCA and a supervisory statement (SS) in relation to the PRA and the Bank.

1.3 This SS/FG sets out principles-based, outcomes-focused expectations on how firms should manage their cyber risk and resilience. It builds on:

- existing rules, supervisory expectations, and guidance in relevant areas including corporate governance, operational resilience, operational risk, and third-party risk management
- cross-sectoral guidance, notably the National Cyber Security Centre's (NCSC) 'Cyber Assessment Framework' (CAF)
- regulation and guidance for the financial sector by global standard-setting bodies and non-UK financial regulators (see Annex 2 for a list of relevant sources)

1.4 The expectations in this SS/FG have also been informed by lessons learned from:

- cyber incidents affecting the financial sector
- our supervision of cyber risk and resilience across firms, including thematic findings from CBEST and STAR-FS tests, firms' CQUEST, ORQUEST questionnaires and operational resilience self-assessments
- analysis of information requests and firm surveys relating to cyber risk resilience
- technological developments, notably in artificial intelligence (AI) and quantum computing

1.5 This SS/FG applies regardless of the technology firms use. Where appropriate, it highlights cyber risks associated with specific technologies, such as AI and quantum computing and ways for firms to use these technologies defensively. We have also published two effective practices documents setting out in greater detail how firms can manage cyber risks relating to AI and quantum computing respectively. We may update these periodically to reflect rapidly evolving changes in technology, risk and industry practices.

1.6 The expectations in this SS/FG set out fundamental, technology-agnostic outcomes that firms should achieve in their cyber risk and resilience management. We have also issued other publications in response to specific developments in technologies such as AI and will continue to do so in future if appropriate. Some of these

publications outline granular, targeted ways in which firms can strengthen their cyber risk and resilience in the context of specific technologies. Such publications may be issued in response to specific developments, such as breakthroughs in a technology or a heightened risk environment. Firms should treat all our relevant publications as complementary and mutually reinforcing.

1.7 The expectations in this SS/FG apply to both malicious and non-malicious cyber disruption, although the emphasis is mostly on the former.

1.8 To promote consistency, we have used existing terminology as defined in the Financial Stability Board's (FSB) Cyber Lexicon, our respective Rulebooks, and established cross-sectoral and global standards.

Scope

1.9 This SS/FG is relevant to all:

- UK banks, building societies and PRA-designated investment firms (banks)
- UK Solvency II firms, the Society of Lloyd's, and its managing agents (insurers)
- UK central counterparties, UK central securities depositaries, UK recognised payment system operators and UK specified service providers, collectively referred to as financial market infrastructures (FMIs) supervised by the Bank
- FCA solo-regulated firms subject to operational resilience requirements in SYSC 15A of the FCA Handbook. In addition to the dual-regulated firms referred to above, this includes:
  - an enhanced scope Senior Managers and Certification Regime (SM&CR) firm
  - a UK Recognised Investment Exchange (RIE)
  - an electronic money institution, a payment institution or a registered account information service provider
  - a consolidated tape provider
  - a qualifying cryptoasset firm (from 25 October 2027)

1.10 Entities in scope of this SS/FG are collectively referred to as 'firms'.

1.11 This SS/FG does not apply to UK branches of overseas firms and non-UK FMIs. However, we may refer to the expected outcomes of this SS/FG when we assess a UK branch's implementation of its cyber risk and resilience framework developed at parent or group level.[9]

1.12 The expectations in this SS/FG also do not apply to credit unions, non-Solvency II insurers and FCA solo-regulated firms that are not subject to SYSC 15A. Nevertheless, these firms should manage their cyber risk and resilience in line with our objectives, the PRA's Fundamental Rules, FCA's Principles for Businesses and other relevant requirements. These firms are also encouraged to consider this SS/FG and other relevant guidance, such as that issued by the NCSC. We recommend that these firms consider whether Cyber Essentials is suitable to their business and assess the potential benefits of having appropriate cyber insurance in place to help mitigate the costs and impact of a cyber-attack.

[9] For third-country branches of insurance firms, para 1.8 of SS44/15 – Solvency II: third-country insurance and pure reinsurance branches also applies.

Proportionality

1.13 Firms should meet the expectations in this SS/FG in a manner appropriate to their size, internal organisation and the nature, scope, and complexity of their activities. This is consistent with how proportionality applies to our policies on operational resilience and third-party risk management. For instance, smaller, less complex firms may take a proportionate approach to expectations that would require investment or resources beyond their reasonable capabilities.

1.14 All firms in scope of this SS/FG should refer to the NCSC's CAF's outcomes, objectives, and indicators to inform the development and assess the maturity of their cyber risk and resilience. We have signposted relevant sections of the CAF to which firms should refer throughout this SS/FG. We will use the CAF, and future versions thereof, as a key benchmark in our supervisory engagement with firms. Internationally active firms should also consider relevant legislation, regulation and guidance in their home jurisdictions and other jurisdictions where they operate. FMIs supervised by the Bank should consider the CPMI-IOSCO Principles for FMIs and related guidance. The Bank will use these as a global benchmark of FMIs' cyber risk and resilience management.

Structure of this SS/FG

1.15 The SS/FG is structured into the following chapters:

- Chapter 2: **Overarching Principles** sets out the key principles behind our expectations
- Chapter 3: **Governance** sets out how firms should embed cyber risk and resilience management in their corporate governance and risk management frameworks
- Chapter 4: **Identification and Assessment** sets out how firms should identify, assess, and understand their assets, cyber risks they face and the potential implications for their resilience
- Chapter 5: **Protection** sets out how firms should protect themselves against cyber risk and enhance their cyber resilience
- Chapter 6: **Detection** sets out what firms should do to detect cyber events and incidents
- Chapter 7: **Response and Recovery** sets out how firms should respond to and recover from cyber incidents
- Chapter 8: **Assurance and Continuous Improvement** sets out expectations on how firms should gain assurance on the effectiveness of their cyber risk and resilience management capabilities and controls and continuously improve them

2 Overarching Principles

Relationship between cyber risk and resilience, operational resilience, operational risk, and third-party risk management

2.1 This SS/FG aims to help firms meet our existing requirements and expectations on operational resilience, operational risk and third-party risk management by clarifying how they should apply them to their cyber risk and resilience management. We do not have specific rules for cyber risk and resilience management, and this SS/FG does not add new rules. However, we will use this SS/FG when we supervise and enforce firms' compliance with the rules listed in Annex 2 where they relate to cyber risk and resilience management. It follows that a firm's cyber risk and resilience management should be consistent with and integrated into its existing frameworks on operational resilience, operational risk and third-party risk management.

2.2 The overarching objective of this SS/FG is to ensure that firms strengthen their operational risk management and resilience by:

- integrating cyber risk management into their organisational structures and decision-making processes so they can address cyber risks in line with their strategy and risk appetite
- reducing the likelihood of cyber incidents by effectively identifying, evaluating and mitigating cyber risks and implementing appropriate protective controls
- reducing the impact of cyber incidents (which they should assume will occur) by promptly detecting, responding to, recovering from and learning from them
- obtaining assurance that their cyber risk and resilience management capabilities are effective through testing, exercises and other activities
- ensuring that their operational and cyber risk and resilience management capabilities remain effective despite rapid changes in technology and the threat landscape

2.3 When identifying which of its business services should be classed as important business services, a firm should assess the risks that severe but plausible disruption to those services, including disruption caused by cyber risks, may pose to the firm and our objectives. For certain firms and services, this may include risks to financial stability.[10] For instance, FMIs, which are digitally connected and interdependent with a larger ecosystem (such as participants in that FMI, linked FMIs, and third-party service providers) should consider bidirectional interdependencies when identifying, managing and mitigating the cyber risks they face from (and pose to) the entities in their ecosystems.

2.4 The cyber threat landscape is evolving rapidly. This may mean firms need to recalibrate their cyber risk management practices, including cyber risk appetite, tolerance and mitigations, more frequently and rapidly than for other risks. Moreover, it may not be possible in practice for firms to bring all cyber risks at any given time within risk appetite or risk tolerance, which may in turn require consideration of compensating controls. Firms may need to find ways to continue delivering important business services to minimum levels of service in degraded or sub-optimal conditions following a cyber incident.

[10] See also SS1/21 – Operational resilience: Impact tolerances for important business services para 2.5.

Alignment to cross-sectoral and international standards

2.5 In addition to referring to the NCSC's CAF, firms are expected to consider relevant guidance from the NCSC (as the UK's technical authority for cyber security) and the National Protective Security Authority (as the UK's technical authority for personnel and physical security). Internationally active firms should also consider relevant cross-sectoral guidance in the jurisdictions where they operate, including but not limited to the US National Institute of Standards and Technology (NIST) Cyber Security Framework, Cyber Risk Institute (CRI) Profile, and International Organization for Standardization (ISO) standards (see Annex 2(d)).

2.6 To the extent practicable, the expectations in this SS/FG are interoperable with relevant guidance and standards developed by global standard-setting bodies, the G7 Cyber Expert Group (CEG), and regulation in other jurisdictions (see Annex 2(e)). Firms are responsible for demonstrating to the regulators that they meet our expectations, but they may use their compliance with these global and non-UK standards as supporting evidence. A firm should be able to demonstrate how it is meeting our requirements and expectations, even where it is subject to group policies and procedures set outside the UK.

Use of third parties

2.7 Where a firm relies on third parties, the firm and its senior management remain accountable for meeting applicable requirements and expectations, including those in this SS/FG. This is consistent with our framework on outsourcing and third party (OATP) risk management. Accordingly, a firm's OATP policy should consider the cyber risk and resilience management of its material third parties and, as far as possible, key nth parties and other key components of their material third parties' supply chains. It should also consider the cyber resilience of third parties that fall outside the formal definition of a material third party arrangement, but which could materially impact the firm's cyber resilience – for example, basic utility providers.[11]

Integrated approach

2.8 A firm should meet the expectations in a holistic and integrated way, recognising that the effectiveness of its cyber risk and resilience capabilities depends on how they operate collectively. A firm should consider how its capabilities in one area (such as detection) interact with and support those in other areas (such as response and recovery).

Collective action

2.9 In addition to the work they do individually, firms should look for ways to collaborate, share knowledge and expertise, and support collective solutions, as appropriate. They should keep informed of and engage with collective action and incident response frameworks to enhance their individual and collective cyber risk and resilience management, including but not limited to the Cross-Market Operational Resilience Group (CMORG), FCA Cyber Co-ordination Groups (CCGs) and the Financial Services Cyber Collaboration Centre (FSCCC).

[11] For example, electricity, gas, water, telecommunication services which constitute the provision of a public electronic communications network or a public electronic communications service within the meaning of section 151 of the Communications Act 2003). See SS2/21 – Outsourcing and third party risk management Table 6.

3 Governance

Outcomes: The firm has clear and effective governance of cyber risk and resilience management led by the board ('cyber governance'). The board approves and oversees the firm's cyber risk and resilience strategy and holds senior managers accountable for its implementation. The board and senior managers allocate appropriate resources to cyber risk and resilience. Cyber risk is addressed as part of the firm's enterprise-wide risk management framework. Where appropriate, major cyber incidents and risks[12] are escalated to the board and senior management, who oversee an appropriate and timely response.

3.1 Firms should refer to the NCSC CAF outcomes, objectives and indicators for **Objective A - Managing security risks – Principles A1: Governance, A2: Risk Management and A3 Asset Management** to inform their cyber governance.

Board oversight and accountability

3.2 A firm's board is accountable for approving and overseeing the firm's cyber governance and ensuring it remains effective. Effective cyber governance should: [13]

- support the firm's business strategy
- align with the firm's risk appetite and risk tolerance
- be embedded in the firm's enterprise risk management framework
- consider the cyber threat landscape, evolving business models, the impact of legacy or out-of-date assets and developments in technology

3.3 Among other elements, effective cyber governance includes:

- the board owning the firm's cyber risk and resilience management framework and effectively overseeing its implementation by management
- clear accountability for cyber risk and resilience management throughout the firm
- timely escalation to the board and senior management of developments that could have a material impact on the firm or the regulators' objectives. These include significant cyber incidents, changes in the cyber threat landscape and risks from information and communications technology (ICT) change programmes
- board and senior management visibility and oversight of material third-party dependencies and risks
- assurance of the effectiveness and maturity of the firm's cyber risk and resilience management
- embedding lessons learned from relevant incidents, near-misses, and assurance activities

3.4 Firms that are subsidiaries of non-UK groups may be subject to policies on cyber risk and resilience management set at group or parent level. They may receive ICT

[12] For the purposes of this SS/FG, a *major incident* is any cyber incident (i) that is reportable under the operational incident reporting requirements in the Notifications Part and Regulatory Reporting Part of the PRA Rulebook and/or under SUP 15.18 (Notification of operational incident) of the FCA Handbook or (ii) of which the regulators would expect notice under the PRA's Fundamental Rule 7 and/or Principle 11 of the FCA's Principles for Businesses. The Bank of England policy on Operational Resilience of FMIs uses the alternative term 'extreme but plausible'. In this SS/FG, reference to 'severe but plausible' disruption should be interpreted as 'extreme but plausible' when applied to FMIs.

[13] See, Corporate governance: Board responsibilities and CAF Principle A1.a Board Direction and Cyber Governance Code of Practice.

services via intra-group arrangements. In these scenarios, the UK board and senior management should retain enough expertise to adequately manage the subsidiary's cyber risk and resilience (including any important business services it provides), ensure that group policies on cyber risk and resilience adequately consider UK regulatory requirements and expectations (including this SS/FG) and manage cyber risks from intra-group services.

3.5 Control functions (ie compliance, risk and internal audit) should be functionally independent, and have sufficient power, resources and skills to review, challenge and validate decisions relating to cyber risk and resilience, escalate issues directly to the board and senior management, provide appropriate assurance and ensure the firm complies with applicable requirements and expectations.

3.6 The board and senior managers should allocate appropriate financial and non-financial resources (including people, training and technology) to deliver the firm's cyber risk and resilience strategy and manage or mitigate risks and vulnerabilities that could (individually or in combination) impact the firm or our objectives. That includes assets approaching their end-of-life or end-of-support stages.

The board's experience, knowledge and skill

3.7 A firm's board should ensure that its collective cyber risk experience, knowledge, and skills are sufficient and up to date. It should not rely too much on a single specialist to effectively oversee and challenge the firm's cyber risk and resilience management.

3.8 Board members should develop their knowledge of cyber risk and keep it up to date through regular training and consultation with internal, and where appropriate, external experts. This does not require every board member to become a specialist in cyber risk. However, all board members should maintain enough knowledge to exercise their oversight duties.

3.9 The board's individual and collective experience, knowledge and skills relating to cyber risk and resilience should be considered as part of board effectiveness reviews, which should suggest improvements where appropriate. Where the board lacks sufficient collective cyber expertise, they should be able to explain to the regulators what steps they plan to take to mitigate and remediate these shortcomings. These might include, for instance, regular workshops on key cyber issues and emerging trends; awareness and training sessions by internal or external experts; discussions of case studies involving real life cyber incidents and near-misses; and participation by board members in exercises and other assurance activities.

Cyber insurance

3.10 A firm should consider the availability and suitability of cyber insurance policies. Where a firm has such policies in place, it should assess their adequacy, including the potential impact of any exclusions and limitations on cover. Having a cyber insurance policy in place does not limit or reduce the importance of firms having effective cyber risk and resilience management capabilities and controls. However, a cyber insurance policy may provide complementary benefits to firms such as access to external specialist expertise during cyber incidents, or incentives (via potentially lower premiums) to align to established cybersecurity standards.

Risk culture

3.11 The board and senior managers should actively shape a proactive cyber risk culture where all staff are responsible for managing cyber risk and resilience.[14]

3.12 The board should ensure that all staff have appropriate awareness and, where appropriate, training to understand the cyber risks facing the firm, their role in controlling these risks, and the resources available for them to do so. This applies to employees, consultants, contractors, secondees and key contacts at material third parties. The board and senior managers should promote collaboration on cyber risk management and resilience across the firm and with material third parties.

Documentation and management information (MI)

3.13 A firm should appropriately document its cyber risk and resilience strategy, policies, procedures, and measures (including its assurance programme and activities). It should update the documentation as appropriate, for instance, during annual updates to the operational resilience self-assessment. It should provide it to the regulators on request.[15]

3.14 The board should make sure it receives accurate, clear, regular, useful, and timely MI on the firm's cyber risk and resilience. The form and content will vary from firm to firm, but it should enable effective board oversight, decision-making, and challenge. MI should cover both business-as-usual cyber risk and resilience management, and the firm's preparedness for severe but plausible cyber scenarios. It should include qualitative and quantitative key risk and control indicators to allow the board to assess the firm's management of cyber risks.[16] It should highlight any cyber risks that the firm cannot currently manage within risk tolerance, along with proposals for remediation (including timelines) and/or compensating controls.

3.15 The MI should provide a clear and accurate view of the firm's current cyber resilience, distinguishing between current capabilities, planned improvements, and improvements that the firm has implemented and validated.

3.16 Subject to proportionality considerations, MI on cyber risk and resilience should include, but not be limited, to:

- information on key risks posed by people, third parties, processes, and technology
- general findings such as overall risk ratings and audit findings;
- performance data on the firm's
  - identification and protection, such as backlogs relating to assets with unpatched or critical vulnerabilities; assets nearing or beyond their end-of-life or end-of-support stages, or out of policy credentials
  - detection capabilities, for example, the mean time to detect potential major incidents
  - response and recovery, for example, major incidents and time taken to resolve them, including the number and/or percentage resolved within

[14] The Cyber security culture principles can help firms inform the development and operationalisation of a sound cyber risk culture.

[15] See Rules 6.1 and 6.3 of the Operational Resilience Parts of the PRA Rulebook and Rules 6.1 and 6.3 of the Insurance - Operational Resilience Parts of the PRA Rulebook, and SYSC 15A.6 (Self-assessment and lessons learned exercise documentation) of the FCA Handbook.

[16] See Cyber resilience toolkit: practical considerations for FMIs – consultative report p.8 for an extensive list of example metrics for measuring cyber risk and resilience. While aimed at FMIs, several metrics are applicable to firms more widely.

recovery objectives, such as impact tolerances for important business services; and recovery testing outcomes

- information on privileged access, including recently completed reviews
- findings and recommendations from assurance activities (such as testing and exercises)
- third-party and supply chain cyber risks, such as:
  - data on firm-wide concentration on third party datasets, geographic locations; third party service providers or technology
  - material third parties that have not provided appropriate assurance on their cyber risk and resilience
- information on the firm's current and proposed AI use cases, key dependencies and risks, and
- emerging and new risks identified through horizon-scanning.

3.17 The board should review the MI regularly considering changes to cyber threats, technologies, processes, and business operations. The firm's senior management and control functions should ensure that board members understand the MI on cyber risk they receive, including its implications and how it differs from MI on other operational and financial risks. For instance, MI showing a high percentage of patched vulnerabilities may not provide an accurate or complete view of the firm's overall cyber risk position.

Senior management responsibilities

3.18 Senior managers should implement the cyber risk and resilience management strategy approved by the board and maintain effective capabilities and controls.[17]

3.19 For regulated firms subject to the Senior Managers and Certification Regime (SM&CR), the Chief Operations Function (SMF24) should ordinarily have overall responsibility for implementing the firm's cyber risk and resilience strategy and reporting on it to the board. However, a firm may, if appropriate, allocate this responsibility to another SMF manager with appropriate authority, experience, and functional independence (such as the Chief Risk Officer (SMF4). In all cases, the relevant person should be sufficiently senior and able to directly access and maintain an effective dialogue with the board.

3.20 For firms not subject to the SM&CR, responsibility for the cyber risk and resilience strategy should be assigned to an appropriate senior manager. Likewise, Bank-regulated FMIs, which are not subject to the SM&CR, should allocate accountability and responsibilities based on applicable governance requirements in the UK European Market Infrastructure Regulation, UK Central Securities Depositories Regulation, the Bank's Codes of Practice and the Fundamental Rules for FMIs (and future revisions thereto).[18]

3.21 All senior managers should take responsibility for managing cyber risk in their respective areas by:

- ensuring they maintain appropriate cyber hygiene[19]

[17] See CAF A1.b Roles and Responsibilities.

[18] These requirements place similar responsibilities for cyber risk and resilience management on senior management and other key personnel, which should be supported by appropriate organisational structures, reporting lines and clearly defined responsibilities. They also require senior management and key personnel to have the authority, expertise and oversight necessary to manage cyber risk and resilience effectively.

[19] As defined by NIST, 'recommended mitigations for the small number of root causes responsible for many cybersecurity incidents'.

- preventing, monitoring, and managing people-related cyber risks in their areas (for example, from malicious and non-malicious insiders or social engineering attacks)
- preventing and detecting shadow ICT (such as people using unauthorised applications) and either ensuring it undergoes proper review and approval or, if appropriate, removing it. This includes managing the unauthorised use of AI and the unauthorised development and use of software applications and tools using generative AI; and
- when delegating responsibility, ensuring that people understand their responsibilities, and have the experience and tools they need.[20]

[20] See CAF A1c 'Decision-making'.

4 Identification and Assessment

Outcomes: The firm identifies, assesses and understands: (i) which assets are relevant to its cyber risk and resilience (including any interconnections and dependencies between them); and (ii) the key cyber risks it faces. Identification and assessment need to be forward-looking and up to date so the firm can make informed decisions and prioritise risks in a rapidly evolving threat landscape. That supports informed and risk-based cyber protection, detection, response and recovery, informs the firm's risk management and assurance activities, and enables the firm to assess if its cyber risk and resilience strategy is fit for purpose and where it could be strengthened.

4.1 Firms should refer to the NCSC CAF outcomes, objectives and indicators for **Objective A - Managing security risks** to inform the development and assess the maturity of their identification of assets and cyber risks, respectively. In particular, they should refer to **Principle A2: Risk Management,[21] A3: Asset Management and A4: Supply Chain.**

Identification of assets

4.2 A firm should identify all assets relevant to its cyber risk and resilience, including those that support its important business services and critical operations. These include but are not limited to data, facilities, hardware, telecommunication networks, people, services, software (including proprietary, third-party and open source), supporting infrastructure (for example, energy supply) and third-party and key supply chain dependencies (including intra-group dependencies).

4.3 We expect a firm to:

- maintain an accurate, thorough and up-to-date asset inventory
- update its inventory and analysis regularly and in response to certain events, such as cyber incidents or material changes in its ICT infrastructure
- identify assets that should be prioritised for investment or subject to stricter controls due to their importance
- monitor and manage the lifecycle of its assets to manage obsolescence-related risks, such as decommissioning, degradation, end-of-life or end-of-support
- identify and map interconnections and interdependencies among assets to understand and manage the potential knock-on effects of disruption to certain assets, and
- identify concentrations and common dependencies that could cause correlated disruption across multiple important business services, group entities, or recovery arrangements (for example, due to data, infrastructure, third parties, underlying technology, or specialist resource). A clear, documented understanding of concentrations and common dependencies can help the firm identify potential forms of risk mitigation, such as assessing the substitutability of material third parties or diversifying certain third-party relationships.

4.4 When identifying and documenting its assets, a firm should use data from existing relevant documentation, including:

[21] Including but not limited to A2.a Risk Management Process and A2.b: Understanding Threat

- asset inventories and bills of materials developed in line with legal or regulatory requirements or cross-sectoral guidance in the UK or other jurisdictions (for example, cryptographic bills of materials, AI inventories, hardware and software bills of materials)
- model inventories[22]
- material third party arrangements registers, and
- operational resilience maps and self-assessments.

4.5 In line with our requirements and expectations on third-party risk management, a firm should have appropriate visibility of key assets in the supply chain of any third party it relies on for material services.

Identification of cyber risks and vulnerabilities

4.6 To inform risk-based prioritisation, a firm should regularly identify, assess, and understand:

- the external and internal cyber threat landscape
- the cyber risks it faces (including from its vulnerabilities and material third parties), and
- the potential impact of these threats and risks.[23]

4.7 A firm should identify, assess, and document its cyber risks in line with other operational risks [24] and categorise them using consistent taxonomies. It should have a clear and documented mapping and aggregation methodology to report these risks (and proposed responses) to the board and senior management.

4.8 A firm's identification of cyber risks should cover internal risks, such as technology misconfiguration risks or insider risks; and external risks, such as attacks by advanced persistent threat actors, hacktivists, and organised criminals. These risks are not mutually exclusive and may co-exist.

4.9 A firm should identify, assess, and document physical risks that could materially impact its cyber resilience, such as risks to its premises and those of its material third parties. As far as possible, it should identify and monitor risks to the infrastructure supporting its important business services and critical operations. This may include data centres, energy supply, hardware, telecommunications infrastructure and undersea cables.

4.10 A firm should proactively monitor developments that could create new cyber risks or amplify existing ones, such as rapid changes in technology or geopolitical events. It should be prepared to respond to these developments in a timely manner.

Use of threat intelligence

4.11 To understand the nature and impact of cyber attacks, a firm should undertake regular threat assessments informed by appropriate intelligence. It should use a proportionate combination of internal capabilities, sector threat assessments by the NCSC, industry groups or similar organisations (such as FS-ISAC) and specialist threat intelligence providers. Threat intelligence should inform the firm's cyber risk

[22] See SS1/23 – Model risk management principles for banks | Bank of England – the UK's central bank Principle 1.2.

[23] See also Risk management.

[24] Principle 6 of the BCBS PSMORs provides tools for identifying and assessing operational risks that firms may find helpful for their identification of cyber risk.

and resilience management decisions, both tactical and strategic, including decisions regarding prioritisation.

4.12 All firms can use external sources for threat intelligence. Where proportionate, a firm should also maintain appropriate internal threat intelligence capabilities. Sources of threat intelligence include:

- actual and potential incidents and near-misses at the firm, its material third parties and its peers;
- cyber scenarios, identified by the firm, included in scenario libraries or suggested by collective action and incident response frameworks;
- the Government's National Risk Register and equivalent non-UK registers;
- advisories issued by technical authorities, such as the NCSC;
- specialist threat intelligence providers;
- vulnerability databases; and
- publicly available intelligence.

4.13 A firm should be able to explain to the regulators how its identification and assessment of cyber risks informed and supported its cyber risk and resilience strategy (including recent updates), and its decisions about allocation of resources, prioritisation and choice of cyber capabilities, controls and tools.

Identification of vulnerabilities

4.14 To determine the cyber risks it faces, a firm should identify, assess, and understand its vulnerabilities, including through vulnerability assessments on its assets. Where possible, it should extend these assessments to the infrastructure supporting those assets, or review vulnerability assessments undertaken by material third parties (for example, data centre operators) or in the public domain.

4.15 A firm's board and senior management should set a risk appetite on key control indicators for vulnerability management, such as an appropriate frequency and scope for assessments and management. Technology, such as automated vulnerability scanning tools, can enhance the effectiveness and frequency of its assessments.

5 Protection

Outcomes: A firm implements strong, risk-based, cyber and multi-layered protective controls that reduce the likelihood of cyber incidents and limit their impact (including to important business services) when they happen. Protective controls safeguard the confidentiality, integrity, authenticity, and availability of the firm's assets. They are regularly reviewed, tested, and adapted to ensure their continuing adequacy, considering changes in the firm's business model, threat landscape and technology.

5.1 Firms should refer to the NCSC CAF outcomes, objectives and indicators for **Objective B: Protecting against cyber-attacks** to inform the development and assess the maturity of their identification of assets and cyber risks, respectively. In particular, they should refer to **Principles B1 Service protection policies, processes, and procedures, B2: Identity and Access Control, B3: Data Security, B4: System Security, B5: Resilient Networks and Systems and Principle B6 Staff awareness and training.**

5.2 A firm should have appropriate and proportionate protective capabilities and controls to reduce the likelihood and impact of cyber risks. These should complement a firm's response and recovery capabilities by pre-emptively limiting the impact of incidents on a firm's important business services, assets and critical operations.

5.3 A firm should regularly assess its capabilities against published lessons learned and thematic findings from exercises and tests (such as CBEST, STAR-FS, SIMEX and the Cyber and Operational Resilience Stress Test) irrespective of whether they took part in them. Recurring findings from these exercises and tests underscore the importance of:

- defence-in-depth, which involves layering interlocking controls (people, processes, and technology) to anticipate situations where one or more controls fail,
- infrastructure, network, and data security, including embedding controls from inception (secure by design), configuring secure networks, and applying strict controls as a baseline (secure by default), and
- identity and access management controls including restricting access privileges to the minimum necessary to accomplish tasks (least privilege) with regular review.

Identity and access control

5.4 A firm should implement appropriate identity and access controls to ensure that only appropriately authorised users can access its critical assets. The term 'users' includes human users, as well as services and technology, for example, AI agents and automated processes.

5.5 A firm should apply least privilege to all users, which includes understanding who or what has access to its assets, the level of access they should have, why it is needed and (if applicable) how long for. It should have documented access management policies and testing procedures, including 'break-glass' accounts[25] for emergencies.

[25] Also called 'emergency access accounts' which provide tightly controlled, highly privileged access to critical systems when normal authentication mechanisms or administrative accounts are unavailable, compromised, or inaccessible.

5.6 A firm should verify, authenticate and authorise identities before granting access. It should use stronger authentication, such as multi-factor authentication, where compromise could affect the delivery of important business services or critical operations.

5.7 A firm should maintain effective, timely processes for creating, changing, reviewing and removing identity and access rights. These processes should reflect 'zero trust' principles, where access rights are not assumed based on network location or prior access, but are regularly verified and restricted to the minimum level necessary.

5.8 A firm should review access rights on a risk-based cadence and pay particular attention when circumstances change (including user responsibilities). Where possible, firms should automate aspects of their identity and access management to improve efficiency and speed. Access that is no longer required should be amended, suspended, or removed as soon as practicable. This should be reflected in human resource processes governing leavers, movers and access for contractors.

5.9 A firm should ensure that user credentials comply with the policies and procedures in place and review them regularly in line with relevant regulatory and industry guidance.

5.10 A firm should monitor and review access activity so it can detect and investigate unauthorised, inappropriate, or unusual access.

Data security

5.11 A firm should:[26]

- identify and classify data according to criticality (including its importance for important business services), sensitivity and risks to its confidentiality, integrity, authenticity, or availability
- protect data throughout its lifecycle including creation, storage, use, sharing, archival, deletion and retention. This should include minimising the number of copies of sensitive data, keeping them in segregated systems and removing functionality that could be misused to grant unauthorised access
- provide read-only access to sensitive data if broader access is unnecessary;
- ensure data is adequately protected at rest, in use and in transit, for instance by implementing transport layer security for data-in-transit
- implement appropriate cryptographic controls. While these may vary depending on the firm and the sensitivity of different data, firms should follow established cryptographic standards, including post-quantum cryptographic (PQC) standards where relevant
- manage risks where data is processed in external environments ie by third parties. This includes knowing which jurisdiction(s) the data is processed in and managing associated risks[27]
- ensure that data remains accurate, complete and protected from unauthorised modification. This could include validation, integrity checks and audit trails;
- implement backup processes to recover data, such as data vaulting, regular transfers and secure storage and testing of backups, and

[26] See additional NCSC guidance on areas such as device security Device security guidance.

[27] See SS2/21 – Outsourcing and third party risk management Ch.7.

- securely dispose of data that the firm no longer needs across all the assets it is stored in, including by securely sanitising devices such as laptops or mobile phones that are being decommissioned.

System security

5.12 A firm should reduce the risk of cyber incidents through effective system security. This includes, but is not limited to, system design, configuration and vulnerability management.

System design

5.13 A firm should adopt a secure and resilient-by-design approach to embed effective cyber risk and resilience practices into system design. In line with our operational resilience framework, a firm should assume that disruption will occur and proactively seek to minimise its impact. Effective system design controls may include, but are not limited to, segregating critical services, networks and systems into higher security zones and implementing resilient and secure by design and by default controls to limit the blast radius of cyber incidents.

Configuration management

5.14 A firm should have controlled, consistently applied and well-governed configuration management practices that support the integrity, security and resilience of its assets. These may include, but are not limited to, using a standard, secure 'baseline build' for all systems and keeping an up-to-date record of 'known good' system configuration.

System management

5.15 A firm should manage ICT systems supporting important business services and critical operations to enable and maintain security. This includes ensuring that they are managed by authorised privileged users from trusted devices, reviewing, updating and safely storing technical information about these systems, and removing malware and unauthorised assets.

Patching and vulnerability management

5.16 A firm should remain aware of and address known vulnerabilities to minimise the risk of threat actors exploiting them. For example, it should:

- conduct regular vulnerability and security assessments, for example, vulnerability scans and penetration tests including, where applicable, CBEST and STAR-FS
- identify and patch in a timely manner vulnerabilities identified in third party or open-source software
- maintain systems to the latest patch level, in line with proportionality and a risk-based approach and only apply authentic vendor-sourced and validated updates;
- manage obsolescence including by implementing compensating controls for end-of-life and end-of-support assets
- limit access to assets with known vulnerabilities by segregating them, and

- implement and test processes to address risks and unintended consequences of patching such as rollback procedures and emergency change governance.[28]

Physical security

5.17 A firm should maintain robust physical security to safeguard its physical ICT assets and infrastructure. This may include:

- identity-based access restrictions
- monitoring and logging of physical access to sensitive areas
- measures to protect from risks such as extreme weather and natural disasters, and
- appropriate assurance about the physical security of material third parties.

5.18 Physical security controls should be designed to prevent, detect and respond to attempts to gain unauthorised access to a firm's assets, networks, data, or operational technology through physical means. This could be by insiders, contractors or hostile actors. Controls may include:

- secure disposal and destruction of assets and media
- protection of infrastructure, network cabinets and critical facilities, and
- physical resilience to protest activity, sabotage or hostile state activity.[29]

People security

5.19 A firm should implement and periodically review appropriate preventative controls for insider risks (whether due to malicious acts or human error), as part of a secure-by-design approach. These controls should include acceptable use policies covering areas such as bring-your-own-device (BYOD) and social media use. BYOD raises specific challenges such as the need to prevent devices from becoming additional threat vectors for cyber-attacks, and simultaneously safeguarding firm data and non-work personal data on a single device.

Digital customer journeys

5.20 Where relevant, a firm should consider the cyber security and resilience of its customers' end-to-end digital journeys including application programming interfaces (APIs), authentication and consent, data exchanges, external dependencies and service interfaces. Controls should address risks such as abnormal transactions, compromised credentials, loss of availability or integrity of services, manipulation or replay of customer communications and unauthorised access.

[28] See CAF Principle B4 'System Security'.

[29] A firm should also consider relevant guidance on physical security from the National Protective Security Authority, including but not limited to Security Best Practices, System & Information Security, Setting the foundations: Five principles for a shared approach to Insider Risk | Insider Risk Guidance & Insider Risk Guidance.

6 Detection

Outcomes: The firm's capabilities support proactive, timely and accurate detection and analysis of cyber events and incidents (in real time or near real time). The firm uses technology to strengthen its detection capabilities.

6.1 Firms should refer to the NCSC CAF outcomes, objectives and indicators for **Objective C: Detecting Cyber Security Events** to inform the development and assess the maturity of their identification of assets and cyber risks, respectively. In particular, they should refer to **Principles C1: Security Monitoring and C2: Threat Hunting.**

6.2 Accurate and timely incident detection is critical for effective response and recovery and therefore key to a firm's cyber risk and resilience management. A firm's processes should support proactive, timely and accurate detection and analysis of 'cyber incidents' and other 'events'[30] that may adversely impact its cyber resilience. This should occur in real time or near-real time to enable effective response and recovery.

Monitoring

6.3 A firm's monitoring should be proportionate and risk based. It should prioritise monitoring assets, systems and material third-party dependencies that support the delivery of important business services and critical operations. It should monitor for a broad range of threats. However, the way it monitors insider threats may differ from external threats given the greater access and knowledge insiders have.

6.4 A firm's monitoring capabilities should also include, where proportionate:

- advanced technologies to detect and prevent intrusion at the earliest possible stage (including from advanced persistent threat actors) and facilitate containment and recovery
- integrating internal and external threat intelligence to inform detection and evaluation of compromises and threats, and
- the capability to detect covert, pre-attack cyber activity designed to operate without detection (for example, pre-positioning attacks).[31]

6.5 In line with a defence-in-depth approach, a firm's monitoring capabilities should be layered. It should have an integrated view of risk across its key assets. This includes material third party and supply chain dependencies, although how it monitors these may differ from the monitoring of its internal assets. For instance, a firm may rely on information, threat intelligence and tools (such as dashboards) from material third parties. It may also deem it appropriate to use third parties for their monitoring, such as managed service providers and external security operations centre providers. The firm should ensure that third parties deliver equal or greater detection capabilities to those we expect of the firm itself.

6.6 A firm's monitoring capabilities should differentiate between normal and malicious activity, including by using behavioural baselines (defined reference points

[30] This SS/FG adopts the definitions of 'cyber incident' and 'cyber event' set out in the FSB Cyber Lexicon.

[31] See NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure networks.

representing normal or expected activity). It should triage and prioritise monitoring outputs based on its confidence that an incident has occurred (ie eliminating false positives) and, if so, the potential impact. To support this, monitoring data should be enriched with relevant contextual information, including information about known vulnerabilities, external threat intelligence and expert judgment. This includes identifying known attack patterns and indicators of compromise.

6.7 A firm should supplement its monitoring with appropriate logging to support detection. Logging should provide a clear audit trail, allow the firm to identify threats and incidents promptly and facilitate prompt containment, recovery and root cause analysis. The information in logs should be immutable, kept secure, available to relevant stakeholders on request (including the regulators) and retained for an appropriate period.[32]

6.8 A firm should review and update its logging capabilities and tools periodically to reflect the evolving threat landscape and changes in technology, such as the emergence of AI agents with high levels of autonomy (which may require granular logging of steps to identify potential issues).

6.9 A firm should use technology to progressively strengthen its detection capabilities. For instance, AI and other technology can improve the detection of anomalous behaviour and biometric fraud (ie deepfakes) by augmenting behavioural analysis through active liveness (biometric security checks that involve the person seeking access performing requested randomised actions, in real time, for example, turning their head).

6.10 A firm should implement proactive threat-hunting capabilities and deception/decoy techniques where appropriate to identify threats that may evade standard monitoring, such as 'living off the land attacks'.[33]

[32] See CAF Principle C1 'Security monitoring'.

[33] See CAF Principle C2 'Threat hunting' and NCSC and partners issue warning about state-sponsored cyber attackers hiding on critical infrastructure networks.

7 Response and Recovery

Outcomes: The firm can respond to and recover from cyber incidents in a way that limits disruption to important business services and critical operations, safeguards the confidentiality, integrity, availability and authenticity of assets, and minimises adverse impacts.

7.1 Firms should refer to the NCSC CAF outcomes, objectives and indicators for **Objective D: Minimising the impact of cyber security incidents** to inform the development and assess the maturity of their response and recovery capabilities. In particular, they should refer to **Principle D1: Response and Recovery Planning.**

7.2 In developing its cyber strategy, a firm should assume that operational disruption from cyber incidents will occur and maintain effective response and recovery arrangements to limit the impact. This is consistent with the regulators' operational resilience framework.

7.3 A firm should consider relevant guidance and evolving industry practice when considering how to meet the expectations in this chapter, including the regulators' Effective Practices on Firms' Cyber Response and Recovery Capabilities and industry guidance, including from CMORG.

7.4 A firm's response and recovery arrangements should be informed by timely detection and analysis of cyber incidents. Response arrangements should ensure the firm can analyse, contain, mitigate and eradicate a cyber threat. Recovery arrangements should ensure secure and timely restoration of the firm's services (including resuming important business services within impact tolerances) and assets (including data and ICT systems).

Incident response and recovery planning

Governance

7.5 A firm should maintain a cyber incident response and recovery strategy underpinned by appropriate and timely governance featuring:

- inclusion of key stakeholders from across the business areas
- clear allocation of roles, responsibilities and decision-making authority during a cyber incident, which should cover arrangements for transitioning from business-as-usual to incident or crisis management (and vice-versa) where appropriate, and
- risk-based, timely decision-making including where information is incomplete, uncertain or rapidly changing.

Cyber incident response and recovery plan

7.6 As part of its strategy, a firm should maintain a documented cyber incident response and recovery (CR&R) plan to facilitate a clear, consistent and timely response to and

recovery from cyber incidents. In this SS/FG, 'CR&R plan' is an umbrella term for all documents relating to cyber incident response and recovery.[34]

7.7 There is no prescribed or specific template for a firm's CR&R plan. It may maintain a combination of related plans, policies, procedures and playbooks provided they are consistent and deliver the outcomes in this SS/FG.

7.8 A firm that is part of a group should either maintain its own CR&R plan and ensure it is compatible with any group CR&R plan or equivalent, or ensure that the group CR&R plan adequately reflects the risks the firm may be exposed to and includes appropriate risk mitigation.

7.9 A firm's CR&R plan should set out key response and recovery actions and decision points including:

- triage procedures including classification, prioritisation, and escalation;
- triggers for activating, escalating and deactivating response and recovery processes
- arrangements for external and internal stakeholder communication and co-ordination
- clear, measurable response and recovery objectives aligned to impact tolerances for important business services
- assets and capabilities needed for cyber response and recovery, and
- assumptions, constraints, dependencies, legal and regulatory obligations and accepted limitations underpinning the plan.

7.10 The CR&R plan should support a firm's response to and recovery from cyber incidents of varying severity, including severe but plausible scenarios. It should be informed by threat intelligence and relevant guidance, and updated as appropriate to reflect new and emerging threats and lessons from assurance activities.

Communication, co-ordination, and record-keeping

7.11 A firm's CR&R plan should include detailed arrangements for effective and timely communication and co-ordination with key internal and external stakeholders during and after a cyber incident. This includes business areas, senior management, customers, counterparties, regulators, public authorities, the media and material third parties. The plan should include details of key contacts, set out the information to be shared (which may vary according to the type of stakeholder) and the timing of communications.

7.12 A firm should consider within its CR&R plan how it can communicate with customers (including those identified as vulnerable) during disruption to ensure they make informed decisions, access available services and mitigate potential harm.

7.13 A firm should seek to ensure the resilience of its communication capabilities during and after a cyber incident, for instance, by keeping alternative communication channels available (including for counterparties, customers, markets and other external stakeholders) where usual channels are compromised, unavailable or unsuitable.

7.14 A firm should maintain and preserve secure records of response and recovery actions (for example, logs) and forensic data to establish an audit trail and support post incident and root cause analysis.

[34] See CAF Principle: D1 Response and Recovery Planning.

7.15 In addition to any applicable reporting obligations to the regulators and other authorities, a firm should consider whether it should report a cyber incident to the NCSC, so that the NCSC can provide support (in the event of significant crises) or monitor the incident and learn from it. A firm may need to provide the NCSC with relevant indicators of compromise to facilitate this.

Co-ordination and collective incident response

7.16 Effective co-ordination across the financial and other sectors can be key if there is a sector-wide or systemic cyber incident. A firm's CR&R plan should include measures for coordinating with Collective Incident Response Frameworks during cyber incidents that are known to have affected multiple firms or the wider financial sector. These frameworks include the Sector Response Framework (SRF), which is owned and maintained by CMORG, and the FSCCC, but the list is non-exhaustive. Internationally active firms may need to engage with collective incident response frameworks in multiple jurisdictions.

7.17 A firm's CR&R plan should consider the links between its response and recovery capabilities and those of entities it relies on for the delivery of important business services. For example, central banks, trading venues, exchanges, FMIs and third parties including, where applicable, Critical Third Parties, AI providers and open-source communities.

7.18 A firm should test its ability to coordinate and communicate with key external stakeholders during disruption, including by participating in joint exercises where appropriate.

Response

7.19 When a firm detects a cyber incident, it should promptly activate the relevant parts of its CR&R plan. It should first analyse and then try to contain and eradicate the incident.

Analysis

7.20 A firm should triage and categorise each cyber incident and decide on a proportionate response considering its nature and potential impact.

7.21 A firm should prioritise its cyber response, considering the:

- impact tolerances assigned to its important business services, including metrics such as duration of disruption, value and volume of interrupted transactions or critical activities
- the potential impact of the disruption to its important business services on our objectives

7.22 For high severity cyber incidents, a firm should prioritise:

- important business services whose disruption could affect financial stability, the firm's viability or cause intolerable harm to consumers
- the core elements of those important business services it must deliver ('minimum level of service')

- the assets required to deliver those important business services to their minimum level of service, such as core infrastructure, essential internal services or minimum data

Containment and mitigation

7.23 A firm should have appropriate capabilities (which may be internal or supported by third parties) to contain cyber incidents and promptly mitigate their impact. For instance, it should be able to:

- isolate compromised assets, such as endpoint devices
- use identity and access controls, for example, revoking compromised users' credentials
- block or quarantine malicious inbound and outbound traffic[35]

7.24 A firm should assess, document and oversee the risks associated with its containment strategy. This may include critical decisions around taking core systems or resources supporting important business services offline. A firm should consider guidance on disconnection and reconnection frameworks and co-ordinate any such action with relevant stakeholders (including but not limited to customers, relevant sector response groups, law enforcement, national cyber security agencies, cyber insurance providers and regulators).[36]

7.25 A firm should consider using automation to respond at speed and contain incidents before they propagate, for instance, to triage and validate evidence of the attack and to automate steps in its CR&R plan. Approaches such as infrastructure as code (a method for managing infrastructure using machine-readable code instead of manual configuration) can expedite and facilitate cyber recovery.

Remediation and eradication

7.26 A firm should be able to remediate and eradicate cyber incidents to prevent them reoccurring. The nature and order of a firm's remediation and eradication activities may vary depending on the incident, but may include:

- re-confirming which assets were affected
- removing malware
- disabling and replacing compromised accounts
- patching and hardening vulnerable systems
- reviewing and updating controls
- testing assets to confirm successful eradication

Recovery

7.27 A firm should maintain effective cyber recovery arrangements and capabilities. These should be complementary to, but distinct from, its cyber incident response. A firm's recovery arrangements and capabilities should be designed to support recovery across a range of cyber incidents and adapted to their nature and severity.

7.28 Recovery should focus on resuming the delivery of important business services within impact tolerances and restoring affected assets to a trusted operational state

[35] See CAF Principle C1.

[36] See G7 Cyber Expert Group: Reconnection Framework Technical Annex and Reconnection Framework.

following severe cyber incidents that destroy or severely affect their confidentiality, availability, authenticity and integrity.

7.29 Cyber-attacks can be destructive, persistent and pervasive. Consequently, recovery to business-as-usual within a short, time-based impact tolerance might be challenging. A firm should consider additional, relevant metrics beyond time-based ones when it sets impact tolerances for its important business services. It should identify critical activity within its impact tolerances so it can define the right parameters for providing a degraded service that minimises the risk of intolerable harm to customers, protects its safety and soundness and, where applicable, financial stability while full recovery is ongoing. Depending on the firm and important business service, non-time-based metrics may include value, volume, critical activity, end-users and types of payments. These metrics may in turn enable a firm to identify priority actions to complete in a degraded state, such as critical payments, while full recovery is ongoing.

7.30 A firm's CR&R plan should recognise that recovery may involve rebuilding assets (applications, data, infrastructure etc) in constrained, degraded, or segregated environments. It should also recognise external and internal dependencies on data, infrastructure, people, processes, services and material third parties etc. Consequently, a firm should test whether its recovery arrangements remain effective where these dependencies are compromised, degraded or unavailable.

7.31 A firm should develop appropriate and proportionate capabilities to deal with high severity cyber incidents affecting its important business services. It should be able to:

- prioritise and sequence recovery activities to restore important business services within impact tolerances. For example, setting clear priorities for rebuilding, reconciling, and restoring core applications, data, infrastructure, and services (considering their inter-dependencies)
- recover and operate in a clean environment that is resilient to further compromise by threat actors, for example, by restoring critical applications, data, and infrastructure from trusted and immutable back-ups
- rebuild critical technology from a known trusted state following severe compromise, for example, conducting a bare metal recovery in a clean environment where the firm's applications, data and operating system can be rebuilt from scratch without relying on potentially compromised backups or infrastructure
- demonstrate its rebuild capabilities to its board, the regulators, and other relevant stakeholders.

7.32 Regardless of the recovery option(s), a firm should protect the integrity of its recovery assets and mechanisms. For instance, recovery data, systems, and assets should be protected from unauthorised modification, deletion, or compromise and capable of supporting the safe resumption of important business services. A firm should have processes to prioritise and verify the integrity, security and suitability of its recovery options before restoration. For example, it could test back-ups in isolated recovery environments to ensure they are clean and uncompromised and verify the integrity of recovery data.

7.33 Recovery of assets and important business services may involve residual risks that a firm should understand, document and (if accepted) appropriately oversee. A firm

should not consider recovery complete until it has assessed whether there are residual risks to its delivery of important business services, its customers, counterparties, data or regulatory obligations and taken appropriate action to manage or mitigate these risks.

8 Assurance and Continuous Improvement

Outcomes: A firm obtains assurance that its cyber risk and resilience management strategy, controls and capabilities are appropriately designed and implemented. The firm obtains evidence of its ability to prevent, detect, respond to and recover from cyber incidents and to continue delivering important business services within impact tolerances. The firm gains assurance that its controls and capabilities work as intended, both individually and in combination. Assurance activities support timely identification of weaknesses, gaps and vulnerabilities and drive informed decision-making, remediation and continuous improvement.

8.1 Firms should refer to the NCSC CAF outcomes, objectives and indicators for **Objective A – Managing Security Risk – Principle A2 Risk Management and Objective D: Minimising the Impact of Cyber Security Incidents – Principle D2: Lessons Learned** to inform the development and assess the maturity of cyber assurance activities and ways to drive continuous improvement.

8.2 In this SS/FG, 'assurance' is an umbrella term for all the activities a firm does to provide confidence that its cyber risk and resilience controls and capabilities are working effectively. This SS/FG focuses primarily on two assurance activities, testing and exercises, due to their prominence in our operational resilience framework and supervisory approach. However, a firm should use a wider range of assurance activities to evaluate the effectiveness of its cyber risk and resilience management, such as internal and external audits or risk and controls self-assessment (RCSA).

Assurance programme

8.3 A firm should establish and maintain a cyber assurance programme that assesses the effectiveness of its cyber capabilities and controls individually and in combination. The programme should provide documented, objective and reliable evidence to the board and senior management to support effective oversight and decision-making, including the identification of material weaknesses.

8.4 A firm's assurance programme should cover all aspects of cyber risk and resilience management, and assess effectiveness at the capability, control, service, firm and, where relevant, sector levels. At the same time, the programme should set a proportionate and risk-based level of frequency and resource intensity for the firm's assurance activities.

8.5 The firm's assurance programme should be supported by clear, functional, measurable, and transparent performance measures (for example, reductions in incident detection times, increases in the number of recovered assets, and speed of recovery). It should be informed by a range of sources, including audit findings, lessons learned from incidents, threat intelligence, supervisory (including thematic) feedback, and changes to technology and the threat landscape.

8.6 The firm's assurance programme should allocate clear roles and responsibilities and (where appropriate) include participation by business areas, control functions and

independent challenge. It should address the firm's collaboration with material third parties and other key external stakeholders where possible, including through joint assurance activities.

Choice of assurance activities

8.7 A firm should select a combination of assurance activities that reflects its circumstances (for example, its business model, risk appetite) and the evolving threat and technology landscape. The resource intensity, frequency and sophistication should be proportionate to the firm's characteristics and systemic importance.

8.8 Assurance activities should be varied enough to assess all the firm's cyber risk and resilience controls and capabilities, recognising that some may be better suited to assessing certain controls and capabilities.

8.9 A firm should assess the effectiveness of its cyber capabilities and controls regularly. It should prioritise certain capabilities and controls for more frequent or intensive assurance based on identified weaknesses (for example, from audit findings or supervisory feedback) or changes to the threat or technology landscape.

Testing

8.10 A firm's assurance activities should include various forms of testing. For instance, the regulators' operational resilience framework requires firms to test their ability to continue providing important business services within their impact tolerances in severe but plausible scenarios. This framework includes expectations on how a firm should approach this testing, including selecting scenarios and calibrating their severity. Collective action and incident response frameworks also maintain scenario libraries that a firm can use to identify and select scenarios. Guidance by international standard-setting bodies also covers scenario selection, including potential add-ons to adjust the complexity or severity of a scenario (for example, simultaneous or coordinated attacks, or the use of disinformation or misinformation to amplify an attack's impact).[37]

8.11 Testing should not focus exclusively or unduly on assessing the firm's protective and detective capabilities. It should also adequately focus on its response and recovery capabilities. Where proportionate, response and recovery testing should move beyond traditional tabletop exercises and assess areas, such as how quickly a firm could complete a bare metal rebuild. It should consider the effectiveness and sustainability of alternative arrangements or workarounds as well as the firm's ability to support customers, manage the impact of disruption and return to normal in a controlled and timely manner.

8.12 A firm should ensure that, as far as possible, individuals and teams involved in testing are functionally independent from those that developed and use the assets or services. It should use external testers where appropriate and proportionate. This can promote an optimum balance between in-house testing skills, and evolving industry good practice that the firm may not be familiar with.

[37] Cyber resilience toolkit: practical considerations for FMIs – consultative report, pp.16-17 Box 3.

Threat intelligence led assessments

8.13 Where proportionate, a firm should consider threat intelligence led assessments, such as red team exercises or ransomware simulations. The frequency, nature and scope of assessments should reflect the firm's cyber threat exposure, operations and risk profile.

8.14 Our supervisory toolkit for cyber risk and resilience includes two types of threat intelligence led assessments ie CBEST and STAR-FS UK[38]. While the regulator-led CBEST applies only to certain firms, all firms should consider its published thematic findings when they assess their cyber risk and resilience controls and capabilities and remediate any shortcomings. Firms should consider participating in STAR-FS, which is voluntary, designed to be accessible to a wider range of firms and incorporates threat-led penetration testing to help identify vulnerabilities. Internationally active firms may also be subject to threat intelligence led assessments under the regulatory frameworks of other jurisdictions they operate in.

8.15 A firm should consider other forms of cyber risk and resilience testing. For example, a firm that is considering using AI to support its delivery of important business services should consider relevant testing, such as red or purple teaming, to test against technology-specific risks, such as model or system evasion, data poisoning, prompt injection and model extraction attacks.

Exercises

8.16 Exercises simulating cyber incidents can be valuable to assess a firm's response and recovery capabilities and its ability to coordinate with external stakeholders, such as material third parties.[39]

8.17 Firms should consider published lessons from SIMEX exercises and Cyber and Operational Resilience Stress Tests, which are key parts of our toolkit for strengthening operational resilience. Where appropriate and feasible, firms should participate in collective and industry-wide exercises. These can strengthen their collective ability to collaborate and coordinate to manage or mitigate the impact of incidents capable of impacting financial stability. These exercises include, but are not limited to, the incident management playbook exercises carried out by critical third parties that a firm receives material third party services from.

Continuous improvement

8.18 A firm should continuously improve its cyber risk and resilience, drawing on:

- the outcomes and recommendations from its assurance activities
- lessons from analysing incidents and near-misses (including forensic analysis, root cause analysis, and trend analysis where appropriate)
- feedback from testing and exercising including CBEST and SIMEX
- the CAF and other cyber assessment frameworks
- other relevant sources

[38] Details on CBEST and STAR-FS can be found at Operational resilience of the financial sector | Bank of England, CBEST Threat Intelligence-Led Assessments and STAR-FS UK Implementation Guide.

[39] G-7 Fundamental Elements of Cyber Exercise Programmes and Effective steps to cyber exercise creation for guidance on participating in and scoping cyber exercises.

8.19 A firm's assurance activities should result in the identification, risk-based analysis and prompt remediation of weaknesses supported by clear accountability, appropriate oversight and assurance that risks have been reduced to an acceptable level. A firm should progressively evolve from point-in-time assurance activities to automated assurance, where possible, which can facilitate faster remediation of issues and vulnerabilities.

Annex 2 Regulation and guidance relevant to this draft SS/FG

Annex 2(a): Existing FCA requirements and guidance particularly relevant to this SS/FG

Rules and guidance in the FCA Handbook
The Principles for Business (PRIN) sourcebook of the FCA Handbook.
The Senior Management Arrangements, Systems and Controls (SYSC) sourcebook of the FCA Handbook, in particular: • SYSC 2 (Senior management arrangements) • SYSC 3 (Systems and controls) • SYSC 4 (General organizational requirements) • SYSC 5 (Employees, agents and other relevant persons) • SYSC 7 (Risk control) • SYSC 8 (Outsourcing) • SYSC 9 (Record-keeping) • SYSC 13 (Operational risk: systems and controls for insurers) • SYSC 14 (Risk management and associated systems and controls for insurers) • SYSC 15A (Operational resilience) • SYSC 21 (Risk control: additional guidance) • SYSC 24 (Senior managers and certification regime: Allocation of prescribed responsibilities)
MAR 9 (Data reporting service) in the Market Conduct (MAR) sourcebook of the FCA Handbook.
The following chapters of the Supervision manual (SUP) of the FCA Handbook: • SUP 10C (FCA senior managers regime for approved persons in SMCR firms) • SUP 15.18 (Notification of operational incident) which comes into force on 18 March 2027 • SUP 15.19 (Notification of material third party arrangements) which comes into force on 18 March 2027 • SUP 16.33 (Material third party arrangements register) which comes into force on 18 March 2027
REC 2 (Recognition requirements) in the Recognised Investment Exchanges (REC) sourcebook of the FCA Handbook.
Non-Handbook guidance
FG26/3: Operational incident reporting
FG26/4: Material third party reporting

FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services
Regulations
The Payment Services Regulations 2017 (SI 2017/752), in particular: • regulation 6 (Conditions for authorisation as a payment institution) • regulation 10 (Cancellation of authorisation) • regulation 12 (Variation of authorisation on FCA's own initiative) • regulation 98 (Management of operational and security risks)
The Electronic Money Regulations 2011 (SI 2011/99), in particular: • regulation 6 (Conditions for authorisation) • regulation 10 (Cancellation of authorisation) • regulation 11 (Variation of authorisation on Authority's own initiative)

Annex 2(b): Existing requirements and expectations for banks and insurers particularly relevant to this SS/FG

Banks	**Insurers**
Rules	
Fundamental Rules Part of the PRA Rulebook	
The General Organisational Requirements Part of the PRA Rulebook, chapters 2 and 5. In particular, those rules on corporate governance, business continuity, contingency planning and data protection.	The Conditions Governing Business Part of the PRA Rulebook, chapters 2, 3, 7. In particular, those rules on corporate governance, business continuity, contingency planning, data protection and outsourcing.
Operational Resilience Parts of the PRA Rulebook, supported by SS1/21 (below).	Insurance – Operational Resilience Parts of the PRA Rulebook
The Senior Management Functions Part of the PRA Rulebook, supported by SS28/15 (below).	The Insurance – Senior Management Functions Part of the PRA Rulebook
Rules 10.1 and 10.2 of the Internal Capital Adequacy Assessment Part of the PRA Rulebook.	
Expectations	
SS28/15 Strengthening individual accountability in banking	SS35/15 Strengthening individual accountability in insurance

SS5/16 Corporate governance: Board responsibilities
SS1/21 'Operational resilience: Impact tolerances for important business services'
SS2/21 'Outsourcing and third party risk management'
'Operational resilience: Operational incident and outsourcing and third-party reporting' Policy Statement 7/26

Annex 2(c): Existing requirements and expectations for Financial Market Infrastructure firms (FMIs) particularly relevant to this SS/FG

UK CCPs	**UK CSDs**	**UK RPSOs and SSPs**
Rules		
Fundamental Rules, particularly: • Fundamental Rule 5: An FMI must have effective risk strategies and risk management systems. • Fundamental Rule 6: An FMI must organise and control its affairs responsibly and effectively. • Fundamental Rule 7: An FMI must deal with its regulators in an open and co-operative way and must disclose to the Bank appropriately anything relating to the FMI of which the Bank would reasonably expect notice. • Fundamental Rule 9: An FMI must maintain sufficient operational resilience. • Fundamental Rule 10: An FMI must identify, assess and manage the risks that its operations could pose to stability of the financial system.		
UK Central Counterparties Instrument 2027 • **Annex B, Management and Governance, Parts 2.1–2.3 and 2.6 | A26: General provisions:** CCPs must maintain robust governance, clear reporting lines and effective risk-management processes. • **A27:** Senior management and the board: CCPs must ensure senior management and	**Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories (the Central Securities Depositories Regulation (CSDR)), articles:** • **A22:** Review and evaluation: CSDs must provide information required for the Bank's review	**BoE CoP on Governance:** • **Systemic Risk Manager** – Manage risks to financial stability through an effective risk-management framework. • **Governance Arrangements** – Maintain clear and transparent governance, accountability and control arrangements. • **Composition of the Board** - Ensure boards have appropriate skills,

boards are suitably experienced, accountable and regularly assessed. • **A28:** Risk committee: CCPs must establish a risk committee to advise the board on risk matters. • **A31**: Information to the competent authority: CCPs must notify the Bank of relevant governance changes and provide required information. • **Annex E, Business Continuity, Part 2.1 | A34: Business continuity:** CCPs must maintain arrangements to preserve critical functions and recover from disruption. • **Annex F, Operational Resilience, Parts 2.1–2.4 | A35:** Outsourcing: CCPs must manage outsourcing risks while retaining responsibility for compliance.	of their compliance and risks. • **A26**: General provisions: CSDs must maintain robust governance, clear responsibilities and effective risk management. • **A27**: Senior management, management body and shareholders: CSDs must ensure key personnel are suitable and notify the Bank of relevant changes. • **A30**: Outsourcing: CSDs must manage outsourcing risks and retain responsibility for compliance. • **A42**: General prudential requirements: CSDs must manage their legal, business, operational and other risks. • **A44**: General business risk: CSDs must manage business risks and maintain sufficient resources for recovery or wind-down. • **A45**: Operational risks: CSDs must identify, monitor and manage operational risks and dependencies.	experience, integrity and independence. **BoE CoP on Outsourcing:** • Section 2: Governance and record keeping - ensure board accountability and maintain outsourcing policies and records. • Section 3: Pre-outsourcing - Assess criticality and risk, conduct due diligence and notify the Bank. • Section 4: Outsourcing agreements. - Maintain written agreements with safeguards, access rights and controls over sub-outsourcing. • Section 5: Data security - Protect data accessed or transferred through third-party arrangements. **BoE CoP on Operational Resilience:** • **Section 2: Operational Resilience** - identify important business services (IBS), set impact tolerances and remain within them during disruption. • **Section 3: Strategies, Processes, and Systems** – Maintain proportionate arrangements to identify and manage resilience risks.

		• **Section 4: Mapping** - Map resources needed to deliver each IBS. • **Section 5: Scenario Testing** – Regularly test ability to remain within impact tolerances. • **Section 6:** Written Records - Document and maintain evidence of resilience arrangements. • **Section 7**: Governance - Obtain board approval and review of key resilience decisions.
Draft Bank rules (Equivalent UK EMIR Regulatory Technical Standard (RTS)) • **A3**: Governance arrangements: CCPs must maintain clear governance arrangements and appropriate accountability. • **Annex B, Management and Governance, Parts 4.1–4.11 | A4**: Risk management and internal controls: CCPs must maintain effective risk-management, compliance and internal-control frameworks. • **A7**: Organisational structure and reporting lines: CCPs must maintain clear organisational	**UK Regulatory Technical Standards for CSDs, articles:** • **A49**: Responsibilities of key personnel: CSDs must clearly allocate and document the responsibilities of key personnel. • **A66–A69**: Operational risks: CSDs must identify, monitor and control operational risks, incidents and dependencies. • **A70**: Operational risk-management framework: CSDs must maintain a comprehensive framework for managing operational risk. • **A71**: Enterprise risk-management system: CSDs must integrate	

structures and appropriately separated reporting lines. • **Annex F, Operational Resilience, Parts 3.1–3.10 | A9**: Information technology systems: CCPs must maintain secure, resilient and appropriately controlled IT systems. • **A11**: Internal auditing: CCPs must maintain an independent internal-audit function that regularly assesses their controls. • **Annex E, Business Continuity, Parts 3.1–3.4 | A17:** Business continuity strategy and policy: CCPs must maintain a strategy for continuing critical functions during disruption. • **Annex E, Business Continuity, Parts 4.1–4.4 | A18:** Business impact analysis: CCPs must identify critical functions and assess the effects of disruption. • **Annex E, Business Continuity, Parts 5.1–5.3 | A19:** Disaster recovery: CCPs must maintain arrangements for the timely recovery of critical operations. • **Annex E, Business Continuity, Parts 6.1–6.2 | A20:**	operational risk into their enterprise-wide risk-management system. • **A72**: Operational risk-management function: CSDs must maintain a function responsible for overseeing operational risk. • **A73–A74**: Testing to address operational risks: CSDs must regularly test their operational resilience against relevant scenarios. • **A75**: Information technology tools: CSDs must maintain secure, resilient and appropriately controlled IT systems. • **A76**: Business continuity strategy and policy: CSDs must maintain a strategy for continuing critical operations during disruption. • **A77**: Business impact analysis: CSDs must identify critical operations and assess the effects of disruption. • **A78**: Disaster recovery: CSDs must maintain arrangements for the timely recovery of operations and data. • **A79**: Testing and monitoring: CSDs must regularly test and monitor their business-continuity arrangements.	

Testing and monitoring: CCPs must regularly test and monitor their business-continuity arrangements. • **Annex E, Business Continuity, Parts 7.1–7.4 | A21**: Maintenance: CCPs must regularly review and update their business-continuity arrangements. • **Annex E, Business Continuity, Parts 8.1–8.4 | A22**: Crisis management: CCPs must maintain clear crisis decision-making and escalation arrangements. • **Annex E, Business Continuity, Parts 8.4 and 9.1 | A23**: Communication: CCPs must maintain procedures for effective communication during a crisis.	• **A80**: Maintenance: CSDs must review and update continuity arrangements following tests, incidents and material changes.	
Expectations/Guidance		
Operational Resilience: Central Counterparties Supervisory Statement March 2021	Operational Resilience: Central Securities Depositories Supervisory Statement March 2021	Operational resilience: recognised payment system operators and specified service providers
Outsourcing and third-party risk management Supervisory Statement		
Operational incident and outsourcing and third-party reporting requirements (IOREP)		
The Bank's supervisory approach to onboarding new FMIs		
SS6/24 – Critical third parties to the UK financial sector		

Annex 2(d): Cross-sectoral guidance relevant to this SS/FG (non-exhaustive)

UK National Cyber Security Centre
• Cyber Essentials • Cyber Assessment Framework • Cyber Governance Code of Practice; • Government Supplier Assurance Framework
Other guidance
US National Institute of Standards and Technology (NIST) • Cyber Security Framework. • Cyber Risk Institute Profile **The International Organization for Standardization (ISO)** • ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements; • ISO 22301:2019 – Security and resilience — Business continuity management systems — Requirements.

Annex 2(e): Publications by standard-setting bodies (SSB), the G7 and non-UK financial regulators relevant to this SS/FG (non-exhaustive)

SSB and G7 publications
Basel Committee on Banking Supervision's (BCBS) • Principles for Operational Resilience (2021) • Revised Principles for the Sound Management of Operational Risk (2021) • Principles for the Sound Management of Third-Party Risk (2025)
Committee on Payments and Market Infrastructures-International Organization of Securities Commissions' (CPMI-IOSCO): • Principles for financial market infrastructures (PFMIs) (2012) • Guidance on cyber resilience for financial market infrastructures (2016) • IOSCO Principles on Outsourcing (2021) • Cyber resilience toolkit: practical considerations for FMIs

Financial Stability Board (FSB)

- Effective Practices for Cyber Incident Response and Recovery (2020)
- Cyber Lexicon (2023);
- Enhancing Third-party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities (2023)
- Sound Practices for Responsible Adoption of Artificial Intelligence (AI) – A Toolkit for Financial Institutions (2026)

International Association of Insurance Supervisors (IAIS)

- Application Paper on operational resilience objectives and toolkit (2026)

G7 Cyber Expert Group

- Fundamental Elements series

Publications by non-UK financial regulators (non-exhaustive)
European Union (EU) • Digital Operational Resilience Act (DORA**)**
New York State Department of Financial Services • Cybersecurity Regulation 23 NYCRR Part 500
Australian Prudential Regulation Authority's (APRA): • Prudential Standard CPS 230 and Prudential Guidance CPG 230 'Operational Risk Management' • Prudential Standard CPS 234 and Prudential Guidance CPG 234 'Information Security'
Monetary Authority of Singapore (MAS) • Technology Risk Management Guidelines (2021)
Canada's Office of the Superintendent of Financial Institutions (OSFI) • Guideline on Technology and Cyber Risk Management (2022)