

Operational Resilience in the UK Financial Sector

Practical Guidance

by R.D. Chanon, L. Habahbeh, P. Klumpes* and S.
Mann

12 August 2024

Disclaimer; The views expressed in this publication are those of invited contributors and not necessarily those of the Institute and Faculty of Actuaries. The Institute and Faculty of Actuaries do not endorse any of the views stated, nor any claims or representations made in this publication and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this publication. The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this publication be reproduced without the written permission of the Institute and Faculty of Actuaries.

Abstract

This paper provides practical guidance to UK-based financial institutions (UKFIs) which are subject to the “operational resilience” guideline requirements of the Bank of England, Prudential Regulatory Authority and Financial Conduct Authority issued in 2021, and fully effective for 31 March 2025. It contains practical suggestions and recommendations to assist UKFIs in implementing the guidelines. The scope of the paper covers issues related to (a) overviewing the latest equivalent operational resilience guidance in other countries and internationally (b) identifying key issues related to risk culture, risk appetite, information technology, tolerance setting, risk modelling, scenario planning and customer oriented operational resilience (c) identifying a framework for operational resilience based on a thorough understanding of these parameters and (d) designing and implementing an operational resilience maturity dashboard based on a sample of large UKIFs. The study also contains recommendations for further action, including enhanced controls and operational risk management frameworks. It concludes by identifying imperative policy actions to ensure that the implementation of the guidelines is more effective.

Keywords

Operational resilience; risk appetite, risk culture, information technology, customer oriented operational resilience, scenario risk management framework, maturity dashboard, cybersecurity, operational risk, enterprise risk management, financial services, industry, regulators, third party risk management, DORA,

Correspondence details

*Correspondence to: Paul J M Klumpes, Aalborg University Business School, Aalborg University, Aalborg East 9220, Denmark, E-mail: pjmk@business.aau.dk

Authors:

Robert Daniel Chanon, Lawrence Habahbeh, Paul Klumpes, Suky Mann

1. Introduction

This paper aims to provide practical guidance for UK financial firms in implementing the operational resilience requirements of the FCA and PRA issued in 2022, effective in 2025. In the absence of significant implementation guidelines provided by the regulatory authorities, this study fills the gap between theory and practice by first identifying the key differences between UK and overseas and international guidance on the topic, and then identifying major issues and areas that require further clarification. It then provides a comprehensive blueprint for the design of a scenario's mature operational resilience system and considers the implementation issues. Finally, it develops an operational resilience maturity dashboard to evaluate the effectiveness of operational resilience by a sample of UK regulated firms.

It covers the following topics. Section 2 provides a brief overview of relevant UK regulatory requirements and comparison with other jurisdictions and international guidelines. Section 3 provides a discussion of outlines major subject area issues related to enhancing operational resilience. Section 4 develops a blueprint for an operational resilience scenario testing strategy. Section 5 discusses implementation issues and develops and implements an operational resilience maturity dashboard based on a sample of large UKFIs. Section 6 identifies key skill sets and competencies of actuaries that are relevant to developing a comprehensive operational resilience management system. Section 7 concludes.

2. Overview of regulatory guidance and international comparisons

This section motivates this report by providing the institutional background required to understand the major issues affecting the implementation of operational resilience frameworks in the UK financial sector. It first provides a brief description of the relevant PRA, FCA guidelines (section 2.1) and then section 2.2 provides an overview of other national guidelines related to the topic (i.e. EU, Australia, Canada, Hong Kong and Singapore), and an overview of international guidelines promulgated by the International Standards Organisation (ISO) is provided in section 2.3. Section 2.4 identifies the limited sectoral guidance on the topic.

2.1. Overview of relevant PRA, FCA guidelines and TPR code of conduct

The PRA initially established the framework for the operational resilience policy by clarifying in relation to how firms should comply with the rules in the “General Organisational Requirements, Skills, Knowledge and Expertise, Compliance and Internal Audit, Risk Control, Outsourcing and Record Keeping” parts of the PRA Rulebook. The initial guidance concerning business continuity in 2015 was subsequently updated in 2017 with a clarification of risk governance policy.

The BofE, FCA and PRA jointly issued a discussion paper concerning undertaking a “dialogue” with the financial services industry concerning expectations of the regulators and the wider public about the operational resilience of UK financial services institutions (BofE, FCA and PRA, 2018). This was subsequently implemented through an “Operational Resilience Policy,” which required UK financial sector firms to be “operationally resilient against multiple forms of disruption (including cyber related attacks) to minimize the harm caused to consumers and markets (BofE, FCA and PRA, 2021).¹

Simultaneously in March 2021 the PRA issued an operational resilience “Statement of Policy”. This clarified that all banks and insurers subject to the regulations should be “operationally resilient” through prevention, adaptation, and recovery mechanisms (PRA, 2021a). Although not specifically mentioning cyber-risk sources of disruption, the Policy Statement further required that regulated firms to connect their operational resilience with their governance, operational risk policy business continuity planning and outsourcing activities.

¹ Besides specified regulatory coordination actions, the PRA and FCA also initiated a series of questionnaires, including a “cyber triage questionnaire” concerning financial sector firms remediation activity (FCA and PRA, 2019).

The PRA also issued more specific statements of policies concerning impact tolerances for important business services (PRA, 2021b, supplemented by an amended supervisory statement PRA, 2022), internal management (PRA, 2021c). It also amended its PRA Rulebook concerning operational resilience (2021d) and provided more specific policy and supervisory statements regarding outsourcing and third-party management, respectively (PRA, 2021e, 2021f).

Additionally, the PRA (2021g) issued an implementation guide to provide UK regulated banks and insurers participating in the CBEST intelligence-led penetration testing with an updated framework. The purpose of the framework was to help deal with cyber-risk as an “important element of operational risk”.

Subsequently, speeches were made by three different PRA managers in the period March to May 2022 (Bank of England, 2022a, 2022b, 2022c) which sought to clarify and interpret different policy, supervisory risk and regulatory operations aspects of the operational resilience guidance, respectively. These sought to embellish and provide further clarification of the various definitional and implementation aspects of the original 2021 policy statements.

2.2. Other national guidelines

In contrast to the PRA/FCA guidance, which is very principles based and at a relatively high level of granularity, equivalent regulatory supervisors in other jurisdictions require significantly more detailed requirements related to the implementation of operational resilience by financial organisations. This section summarises the recent key operational resilience requirements of the European Union (EU), as well as five other OECD countries (Australia, Canada, Hong Kong, New Zealand and Singapore). The EU requirements are more focused on operational resilience that is contextualised to ICT related risks, while the Australian and Hong Kong guidance is at a much more detailed level of granularity. The New Zealand requirements are based on cyber and systems resilience, while the Singapore guidelines are limited to business continuity planning and are more consumer oriented. By contrast, the Canadian guidance is more principles based but also more comprehensive in scope.

2.2.1. EU Requirements

The European Union issued a range of various cybersecurity-related policies and legal instruments, at a significant level of granularity and detail (e.g., EU Cybersecurity strategy, NIS2 Directive, Cybersecurity Act, Cyber Resilience Act, etc.). However, these are generally kept at the information and communication technology level, and do not more broadly address operational resilience as a strategic enterprise risk management level issue. The key aspects of these requirements are briefly overviewed below:

- *EU Cybersecurity strategy (2020)*. This strategy updated the former 2018 strategy, and contains concrete proposals for deploying three principal instruments -regulatory, investment and policy instruments - to address three areas of EU action of cybersecurity and related terminology related to:
 1. resilience, technological sovereignty, and leadership.
 2. building operational capacity to prevent, deter and respond; and
 3. advancing a global and open cyberspace.
- The *Cybersecurity Act (EU 881 / 2019)* establishes a certification scheme about the cybersecurity features of ICT products, ICT services and ICT processes to tackle the current fragmentation of the internal market.
- *NIS 2 (EU, 2022)*. The NIS2 directive provides the overall EU-wide legislation on cybersecurity.
- *DORA*. The *Digital Operational Resilience Act* is an EU regulation which entered into force in January 2023 and applies from January 2025. Its objective is to strengthen the IT security of financial (and other key infrastructure based) entities that are based in the EU and ensure that the European Union financial sector can stay resilient in the event of a severe operational disruption. It applies to a wide range of financial entities and ICT third party service providers.

DORA covers the following elements in some detail:

- Principles and requirements of ICT risk management framework.
- ICT third party risk management: monitoring of third-party risk providers and contractual provisions.
- Digital operational resilience testing (basic and advanced).
- Reporting of ICT-related incidents to authorities.
- Exchange of information and intelligence on cyber threats and cyber-attacks.

- Oversight framework of critical of third-party providers.

2.2.2. Australia

The Australian Prudential Regulation Authority (APRA) issued a *Prudential Practice Guide DPG 230 Operational Risk Management* (APRA 2024a) to implement prudential standard *CPS 230 Operational Risk Management* (APRA, 2023), effective from 1 July 2025.

The standard sets out, at a high-level, its expectations for Australian APRA-regulated financial entities to undertake the following:

- strengthen operational risk management by introducing new requirements to address identified weaknesses in existing controls.
- improve business continuity planning to ensure they are positioned to respond to severe disruptions.
- enhance third-party risk management by ensuring risks from material services providers are appropriately managed.

The standard is intended to ensure that “regulated entities set and test controls and maintain robust continuity plans to respond if disruptions do occur” (APRA, 2024b).

2.2.3. Canada

The Office of the Superintendent of Financial Institutions Canada (OSFIC, 2023) issued a draft guideline concerning operational resilience and operational risk management in October 2023. It applies to federally regulated financial institutions (FRFIs). Unlike the high-level PRA and FCA guidance, it provides more detailed guidance both on overall guiding principles and outcomes related to implementing operational resilience and its broader connections to governance and to operational risk frameworks. These are summarised briefly below.

The guidelines contain eight principles of operational resilience, which includes a generic principle related to governance. The generic principle 1 specifies the operational resilience approach and operational risk management framework are implemented, governance and reported through the appropriate structures, strategies, and frameworks

Additionally, it specifies three principles concerning the following elements related to operational resilience with outcomes that the FRFI can be expected to deliver its critical operations through disruption:

- Identify and map critical operations - the FRFI should identify its critical operations and map internal and external dependencies (principle 2).
- Establish tolerances for the disruption of critical operations - the FRFI should establish tolerances for the disruption of critical operations (principle 3).
- Scenario testing and analysis - the FRFI should develop and regularly conduct scenario testing on critical operations to gauge its ability to operate within established tolerances for disruption across a range of severe but plausible operational risk events (principle 4).

It also includes a further four principles related specifically to operational risk management including:

- Operational risk management framework (ORMF); the FRFI should establish an enterprise-wide operational risk management framework (principle 5).
- Operational risk appetite; the FRFI should set a risk appetite for operational risks (principle 6).
- Operational risk management practices. The FRFI should ensure comprehensive identification and assessment of operational risk using appropriate operational risk management practices (principle 7).
- Conduct ongoing monitoring of operational risk to identify control weaknesses and potential breaches of limits/thresholds, provide timely reporting, and escalate significant issues (principle 8).

Additionally, it also covers, at a broad level, a further seven operational risk management subject areas that strengthen a regulated FRFI’s operational resilience, comprising:

- Business continuity management (BCM).
- Disaster recovery.
- Crisis management.
- Change management.

- Technology and cyber risk management.
- Third party risk management.
- Data risk management.

2.2.3. Hong Kong

The Hong Kong Monetary Authority issued a Supervisory Policy Manual new module OR-2 on “Operational Resilience” (HKMA, 2022a) together with a revised module TM-G-2 on “Business Continuity Planning” (HKMA, 2022b) in May 2022.

The Operational Resilience OR-2 module specifies the HKMA’s overall approach to operational resilience. In contrast to the relatively high level BofE, PRA and FCA (2021) guidelines, it provides more detailed guidance regarding:

- An overall operational resilience framework, which also specifies a step-by-step approach to developing a holistic operational resilience framework.
- the role of the board and senior management.
- operational resilience parameters.
- mapping interconnections and interdependencies underlying critical operations.
- preparing for and managing risks to critical operations delivery.
- testing ability to deliver critical operations under severe but plausible scenarios.
- responding to and recovering from incidents.

Unlike regulatory authorities in other national jurisdictions, the HKMA has additionally imposed a two-step prescriptive process for implementation of its guidance for every authorised institution (AI):

1. Have developed its operational resilience framework and determined the timeline by which it will become operational resilient (by May 31, 2023); and
2. become operationally resilient as soon as their circumstances allow and no later than May 31, 2026.

2.2.4. New Zealand

The New Zealand Financial Markets Authority (FMA) (FMA, 2022) has issued a high-level cybersecurity security and operational systems resilience information sheet which requires New Zealand market services licensees to “enhance the resilience of their cyber and operational systems”.

It refers to Part 6 of the *Financial Markets Conduct Act 2013*, which requires that New Zealand based licensed entities must have “effective cybersecurity and operational systems resilience controls, processes, policies and people capability in place, including supply chain risk”. The entities are required to have the “appropriate governance, training, incident response management, reporting and remediation structures in place. It also requires that entities self-evaluate their cyber resilience against the United States’ National Institute of Standards and Technology (NIST) Cybersecurity Framework Functions.²

2.2.5. Singapore

The Monetary Authority of Singapore (MAS) issued detailed guidelines on business continuity management on regulated Singapore-based financial institutions (FIs) within its jurisdiction (MAS, 2022). Unlike other jurisdictions, the MAS detailed a broader range of specific regulatory guidance which it expects FIs to implement to “better manage the increasingly complex operating environment and threat landscape to enable the continuous delivery of services to their clients” (MAS, 2022b). These include specific regulatory requirements for FIs to:

- Adopt a more service-centric approach through timely recovery of critical business services facing customers (e.g. by specifying service recovery time objectives).
- Identify their end-to-end dependencies that support critical business services, and address any gaps that could hinder the effective recovery of such services (dependency mapping); and
- Enhance their threat monitoring and environmental scanning systems, and conduct regular audits, tests, incident and crisis management, and participate in industry-wide exercises.

² NIST Cybersecurity Framework (NIST, 2024).

2.3 International guidelines

There are also some international-level guidelines concerning operational resilience which are specifically focused on financial entities. However, at a more generic, high level, the ISO issued some standards related to both risk management generally, and security and resilience specifically, in relation to business continuity management systems. These is briefly outlined below³:

- *ISO 22301 (2019): Security and Resilience; Business Continuity Management Systems*. This standard specifies generic requirements for organisations to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to, and recover from disruptions when they arise. The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCMS.⁴ It also requires business impact assessment to be undertaken, which it defines as comprising: a) implement and maintain systematic processes for analysing the business impact and assessing the risks of disruption; b) review the business impact analysis and risk assessment at planned intervals and when there are significant changes within the organization or the context in which it operates.
- *ISO 31000 (2018): "Risk Management Guidelines"*. This standard proposes a generic risk management framework, to assist the organization in integrating its risk management system into its most significant operational activities and functions. The framework development encompasses integrating, designing, implementing, evaluating, and improving risk management across the organization. It comprises six generic elements:
 1. *Leadership and commitment*: Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organizational activities and should demonstrate leadership and commitment.
 2. *Integration*: Integrating risk management relies on an understanding of organizational structures and context. Structures differ depending on the organization's purpose, goals, and complexity. Risk is managed in every part of the organization's structure. Everyone in an organization has responsibility for managing risk.
 3. *Design*: When designing the framework for managing risk, the organization should examine and understand both its external context (e.g. stakeholders, legal context) and internal context (e.g. organisational culture, strategy, and objectives)
 4. *Implementation*: The organization should implement the risk management framework by developing an appropriate plan including time and resources, identifying where, when, and how different types of decisions are made across the organization, and by whom, modifying the applicable decision-making processes where necessary, and ensuring that the organization's arrangements for managing risk are clearly understood and practised.
 5. *Evaluation*: The organization should: — periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour; — determine whether it remains suitable to support achieving the objectives of the organization.
 6. *Improvement*: The organization should continually monitor and adapt the risk management framework to address external and internal changes. In doing so, the organization can improve its value. The organization should continually improve the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated.

2.4 Industry specific guidelines

This section briefly outlines more granular levels of regulatory guidance concerning operational resilience requirements which are directly related to specific types of financial entity:

There are relatively greater levels of regulatory guidance concerning operational risk for banks than for insurers. This section briefly outlines these requirements below.

³ ISO also issued a specific standard related to information technology and security techniques (*ISO 27000 (2018): Information Technology and Security Techniques*). Although of direct relevance to DORA implementation, it is not sufficiently generic in nature to cover "operational resilience" and so is not reviewed.

⁴ ISO subsequently issued an amendment to ISO 31000 in 2020 which added the generic sentence "The organization shall determine whether climate change is a relevant issue."

Banks

- *Bank for International Settlements. (2020)*. This explained how the Covid-19 pandemic of 2020 refocused regulatory discussion about operational resilience which had been driven by vulnerabilities brought about primarily by technological change and in increasingly hostile cyber environment. The Covid 19 pandemic caused widespread and long-lasting disruption associated with their personnel.
- *Basel Committee on Banking Supervision (2020)*. This provides a comprehensive overview of the key considerations affecting banks implementing effective operational resilience systems. It explained that operational resilience is much more than simply the outcome of the process of operational risk management.

Insurers

The International Association of Insurance Supervisors (IAIS) (2019) issued a high-level “IAIS Holistic Framework for the assessment and mitigation of systemic risk in the insurance sector” (“Holistic Framework”).⁵ The Holistic Framework is an integrated set of supervisory policy measures that includes a Global Monitoring Exercise (GME) and supplementary implementation assessment activities. It was subsequently endorsed by the Financial Stability Board in 2022. Subsequently, the IAIS issued a public consultation document for revisions to the Holistic Framework in 2024.

⁵ This framework primarily applies to national insurance regulatory supervisors when responding to systemic risk events, rather than addressing the operational resilience of regulated entities.

Key Issues Impacting Operational Resilience

In this section, we identify a few subject-related issues related to the implementation of an effective framework of operational resilience which require further clarification. These related to the following topics: risk appetite and risk culture (sections 3.1 and 3.2), the need for a solid IT foundation for the management of IT risks (section 3.3), risk model maturity (section 3.4), sophistication of scenario testing approaches (section 3.5), and monitoring operational resilience effectiveness (Section 3.6). Finally, section 3.7 identifies a potential ERM framework related to those jurisdictions (such as Singapore) where customer protection is fully integrated as a key aspect of an effective system of operational resilience.

3.1. Risk Culture

As summarised in section 2.3 above, ISO 31000 highlights the importance of organizational risk culture as the relevant internal context to the design of an effective system of operational risk resilience, by reinforcing the need to integrate risk management into the overall culture of the organization.

A strong risk management culture is therefore essential for building operational resilience and customer focus. It refers to the prevailing attitudes, values, and behaviours determining how employees approach risk. A positive risk culture is one where risk is seen as an opportunity for improvement, not something to be hidden or ignored. Employees at all levels are encouraged to identify and report risks, and management is committed to taking appropriate action to mitigate them.

Organisations must take risks to deliver value and for the following reasons:

- *Growth and innovation:* Playing it safe all the time limits opportunities for growth and innovation. Taking calculated risks allows organisations to explore new markets, develop new products or services, and gain a competitive edge.
- *Adapting to change:* The business landscape is constantly evolving. By taking risks, organisations can adapt to new technologies, customer demands, and market conditions. Those who cling to the status-quo may be left behind.
- *Seizing opportunities:* The best opportunities often lie outside of comfort zones. Taking calculated risks allows organisations to capitalise on new market opportunities, strategic partnerships, and technological advancements; and
- *Learning and improvement:* Taking risks, even if they don't always pan out, can be valuable learning experiences. Organisations can learn from their successes and failures, improve their decision-making processes, and become more resilient.

It is important to remember that risks shouldn't be taken blindly. Effective risk management involves careful analysis, weighing potential rewards against potential downsides with a customer focus, and taking steps to mitigate risks before acting. Taking calculated risks is essential for organisational growth and achieving objectives. However, the prevailing risk culture within an organisation dramatically impacts its ability to manage these risks effectively.

A strong risk culture also fosters informed risk-taking and enhances performance. Conversely, an inappropriate culture can lead to activities that contradict established policies and procedures. In such cases, individuals or teams may engage in risky behaviour, while others turn a blind eye or fail to recognise the issue. This can significantly hinder the achievement of goals and, in severe cases, lead to reputational and financial ruin.

Risk culture failures are often at the heart of organisational scandals and collapses. For instance, the Walker report on UK banks' corporate governance post-financial crisis highlighted the importance of behavioural change and cultural transformation over mere compliance exercises (Walker, 2009). Similarly, the Baker (2007) report on the BP Texas City explosion pinpointed leadership, competence, communication, and cultural deficiencies as contributing factors to the tragedy.

Risk culture is a double-edged sword. While a cautious culture can stifle innovation by overemphasising rigid processes, an overly risk-averse culture can lead to uncontrolled risk-taking due to a disconnect between formal policies and actual behaviour.

National cultures also play a role in shaping organisational risk culture.⁶ Varying interpretations of communication, like "yes" signifying different levels of commitment, and differing cultural attitudes towards risk and shame can influence both risk management and reporting. African cultures, for instance, emphasise inclusivity and allowing everyone to contribute, while European and North American cultures may move on to decisions faster. These are cultural differences, not right or wrong approaches, each with its strengths and weaknesses.

While advancements have been made in enhancing the quality of risk management frameworks and processes in recent years, strong risk culture remains the missing link. Effective risk management goes beyond just rules and procedures. Even the most well-defined framework can be misinterpreted or deliberately ignored. Understanding and fostering a strong risk culture is critical for balancing risk and reward in decision-making, ultimately leading to organizational success.

In conclusion, for an organisation to be successful, key characteristics of a strong risk management culture should include the following aspects:

- *Customer Focus*: Listening to the customer and delivering on the promised service or product.
- *Risk awareness*: Employees at all levels of the organization understand the importance of risk management and their role in identifying and mitigating risks.
- *Open communication*: There are open channels of communication for employees to report risks without fear of reprisal.
- *Management commitment*: Senior management is visibly committed to risk management and sets the tone for the organization.
- *Continuous improvement*: The organization has a continuous improvement process in place for identifying and addressing risk management weaknesses.

There are many benefits resulting from a having a strong risk management culture. A strong risk management culture can provide organizations with the following benefits:

- *Enhanced service quality*: Higher levels of customer satisfaction and brand loyalty.
- *Reduced risk of disruptions*: By proactively identifying and mitigating risks, organisations can reduce the likelihood of disruptions to their operations.
- *Improved decision-making*: A strong risk culture encourages employees to consider the potential risks of any decision.
- *Enhanced reputation*: Organizations with a strong risk management culture are seen as more reliable and trustworthy by their stakeholders.
- *Competitive advantage*: A strong risk management culture can give organizations a competitive advantage.

There are several actions that organisations can take to foster a stronger risk management culture, including:

- *Leadership commitment*: Senior management must visibly demonstrate their commitment to risk management and to delivering for customers.
- *Communication and training*: Employees need to be trained on risk management principles and procedures.
- *Risk assessment*: Organisations should conduct regular risk assessments to identify potential risks.
- *Incident reporting*: Employees should be encouraged to report all incidents, near misses, and risk observations.
- *Performance measurement*: Organizations should track and measure their risk management performance.

Organisations adopting these actions create a stronger risk management culture that will help them build their operational resilience and thereby achieve their strategic organisational objectives.

3.2. Risk Appetite

OSFIC (2023) Principle 6 requires regulated entities to produce an “operational risk appetite statement” which should be “integrated into the FRFI’s enterprise-wide risk appetite framework as described in OSFI’s Corporate Governance Guideline”. Similarly, the PRA (2021) guidelines identify a relationship

⁶ For example, Hofstede (2001) provides a well-known five-dimensional model of national risk culture.

between risk appetite and impact tolerances. However, the regulations reviewed in section 2 do not explicitly define what is meant by the term “risk appetite” and its relationship to operational resilience. This section briefly identifies the key relevant issues.

In today's dynamic business environment, organisations need to balance pursuing the potentially conflicting business objectives of both achieving growth and safeguarding themselves from disruption. This balancing act hinges on two key concepts: risk appetite and operational resilience. Although distinct, they are intricately linked, forming the foundation for a robust and sustainable organization.

3.2.1. Risk Appetite: Defining Your Comfort Zone

Risk appetite essentially defines the level of risk an organisation is willing to accept in pursuit of its strategic goals. Risk capacity is the ability to absorb the loss or how much the organisation can bear, based on its wealth, considering the constraints of its risk bearing activities, in pursuit of its strategic objectives. It reflects the organization's tolerance for potential losses or setbacks. A high-risk appetite might prioritize rapid growth, even if it means venturing into uncharted territory. Conversely, a low-risk appetite prioritizes stability and may favour established paths with lower potential for disruption.

3.2.2. Operational Resilience: Bouncing Back from the Unexpected

Operational resilience focuses on an organization's ability to withstand and recover from operational disruptions. It encompasses proactive measures to identify potential threats, build in safeguards, and ensure business continuity even in the face of unforeseen events. A cyberattack, natural disaster, or even a critical equipment failure can all be operational disruptions. A resilient organization can not only absorb the initial shock but also adapt, respond, and recover with minimal downtime.

3.2.3. Synergy Between Risk and Resilience

While seemingly opposing forces, risk appetite and operational resilience work in tandem. An organization's risk appetite informs its approach to building operational resilience. For instance, an organization with a high-risk appetite might prioritize investments in cutting-edge technology, even though it may carry inherent risks. To mitigate these risks, they would then need to build strong operational resilience by ensuring robust cybersecurity measures and contingency plans for potential technology glitches.

A well-defined risk appetite can further empower operational resilience in the following dimensions:

- *Prioritization:* Risk appetite helps identify the critical business services that must be protected at all costs. Resources can then be strategically allocated to fortify those services against potential disruptions.
- *Scenario Planning:* Understanding your risk tolerance allows for the development of realistic scenarios that test the organization's resilience. By simulating potential disruptions, organizations can identify weak spots and develop contingency plans to address them.
- *Investment Decisions:* Risk appetite guides investment decisions related to building operational resilience. It helps determine the appropriate level of resources to allocate towards backup systems, redundancy measures, and staff training on incident response protocols.

3.2.4. Building a Culture of Resilience

A strong operational resilience framework cannot exist in isolation of overall strategic business objectives. It requires a cultural shift in management culture whereby risk awareness and preparedness are embedded into the organization's business objectives. This culture can be cultivated by:

- *Leadership commitment:* Senior leadership needs to champion the importance of operational resilience and ensure its integrated into all aspects of the organization's strategy.
- *Communication and training:* Regularly communicate risk scenarios and response plans to all employees. Provide them with the knowledge and skills to identify, report, and respond to business disruptions more effectively.
- *Continuous improvement:* Operational resilience is not a one-time exercise. Regularly test and review overall business operational resilience plans, learn from incidents, and adapt to the evolving risk landscape.

3.2.5. Journey Toward Long-Term Success

By striking a balance between calculated risk-taking and robust operational resilience, organizations can navigate the ever-changing business landscape with greater confidence. A clear understanding of risk appetite provides the compass for building a resilient organization, capable of weathering storms and emerging stronger. *Operational resilience* isn't about avoiding risk; it's about embracing it with a long-term strategic business plan.

3.3. Building a Solid Information Technology Foundation for managing IT Risk

A solid IT foundation comprises a well-organized set of technologies and applications that are effectively managed and supported, minimising risks. It possesses the following characteristics:

- Standardised infrastructure with the necessary technology configurations and no more.
- Well-integrated applications that are only as complex as necessary.
- Documented data structures and consistent process definitions throughout the enterprise.
- Controlled access to data and applications, with built-in mechanisms to prevent unauthorised actions and detect anomalies.
- Support staff knowledgeable about each application and its support for business processes.
- Maintenance processes that keep technology up to date with required security patches and upgrades, providing adequate protection in case of a technology failure.

A Scenario based Framework for effective IT Risk Management

In the domain of IT risk management, a fundamental challenge lies in identifying pertinent risks within the context of potential IT-related issues across the enterprise. An effective technique for addressing this challenge is the development of risk scenarios, which offer clarity and organisation to the intricate domain of IT-related risks. Once established, these scenarios are employed in risk analysis to estimate their frequency and business impact. Figure 1 summarises the requirements (ISACA, 2024):

Figure 1

Risk Scenario/ Loss Event Structure and Components (ISACA)

Risk Scenario/Loss Event Structure and Components



There are two principal methods for deriving risk scenarios:

1. *Top-down approach*: This approach entails using the enterprise's mission strategy and business objectives as a foundation to identify and analyse risks that are both plausible and pertinent to desired outcomes. When impact criteria align well with the enterprise's real value drivers, relevant risk scenarios can be formulated.

2. *Bottom-up approach*: This method begins with important enterprise assets, systems, or applications and compiles a list of potential threats or generic loss scenarios. Subsequently, this list is utilised to define a set of specific, custom-tailored scenarios that are applicable within the enterprise context. While

commonly employed in cyber threat and vulnerability assessments, the bottom-up approach may limit visibility or obscure business impact if its results are not considered in conjunction with the top-down approach.

Both the top-down and bottom-up approaches are complementary and should be used together. A risk taxonomy may aid in correlating their results by providing a framework for classifying sources and categories of risk. The journey from a cyber threat to a developed and documented risk necessitates the decomposition of the risk statement into actionable components. The risk taxonomy offers a common language for discrete sources and categories, facilitating effective communication of risk to stakeholders and ensuring that risk scenarios are relevant and linked to real business or mission risk.

Following the definition of a set of risk scenarios, they are utilised in risk analysis to evaluate the frequency and impact of each scenario. An integral component of this evaluation is the consideration of risk factors, which influence the frequency and/or business or mission impact of risk scenarios. Risk factors can be classified into two major categories:

- Contextual factors (internal or external): The primary distinction lies in the level of control that the enterprise has over these factors. Internal contextual factors are largely within the control of the enterprise, albeit not always easy to change. In contrast, external contextual factors largely lie outside the enterprise's control.

- Capability factors (indicating the ability to execute IT-related activities): These factors are pivotal in achieving successful outcomes in risk management. Capability factors are ingrained within various ISACA tools, techniques, methods, and frameworks, supporting an enterprise in defining and enhancing the necessary IT and related processes to sustain IT-related activities. These factors address questions concerning IT-related risk management capabilities and IT-related business or mission capabilities.

An IT risk scenario delineates an IT-related event that can lead to a business impact should it occur. For risk scenarios to be comprehensive and viable for risk management and decision analysis, they should encompass the following elements as depicted in Figure 2.

Figure 2

IT Scenario Development (ISACA)



- The entity generating the threat, which can be internal or external, human or nonhuman
- The type of condition or nature of the event, encompassing malicious, accidental, process failure, natural (force majeure), business cycle, etc.
- The type of impact or outcome from the event, such as disclosure of information, system interruption, unintended modification or change, theft, destruction, etc.
- The target asset or resource, which could be adversely affected and lead to business or mission impacts. For example, IT hardware is a critical resource since all IT-related applications depend on it.

Establish the base of the IT Pyramid

The IT risk pyramid (figure 3) further helps organisations to prioritise their IT risk and resilience management efforts. By focusing on the foundation of the pyramid (availability), organisations can reduce the risk of cascading failures that can impact higher levels of the pyramid (access, accuracy, and agility).

Figure 3
IT Risk Pyramid (Westermann, 2005)



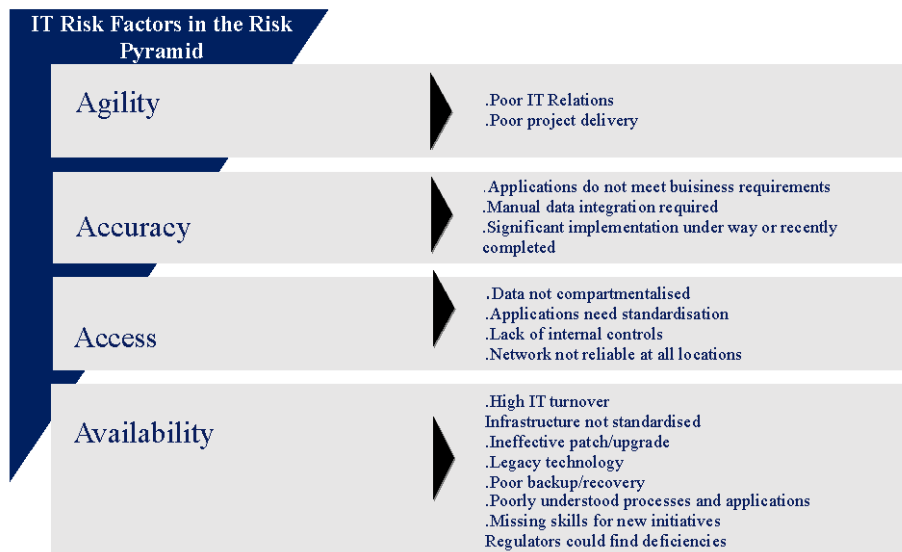
The IT risk pyramid comprises the following elements:

- *Availability* sits at the base of the pyramid, representing the foundation. It refers to the risk of IT systems being unavailable or experiencing downtime. This can lead to lost productivity, revenue, and customer satisfaction.
- *Access* refers to the risk of unauthorized users gaining access to IT systems or data. This can lead to data breaches, fraud, and other security incidents.
- *Accuracy* refers to the risk of data being inaccurate or unreliable. This can lead to poor decision-making, operational inefficiencies, and reputational damage.
- *Agility* sits at the top of the pyramid, representing the most complex and impactful risk. It refers to the risk of IT systems not being able to adapt to changing business needs. This can lead to missed opportunities, competitive disadvantage, and ultimately, business failure.

Each factor in the pyramid is contagious to another, giving rise to primary and other consequential and interconnected risks. For example, the availability of a non-standardised infrastructure can affect all the risk factors in the rest of the pyramid.

Risk factors associated with each of these five elements are summarised in figure 4.

Figure 4
IT Risk Factors in the Risk Pyramid (Westerman, 2005)



Addressing the risk factors from bottom to top is the easiest path to reducing IT risks and organisational impact. With this approach, the following organisational issues associated with IT risk management are easier to manage at the base of the pyramid:

- ROI is easier to justify for reducing risks in the lower tiers, where risk can be easily quantified, and key risk indicators implemented to monitor risk reduction.
- Risks are less quantifiable on the upper tiers of the pyramid.
- ROI at the top of the pyramid may take years, start with the low-hanging fruit.
- Higher-tier risks cannot be fully solved until the base is under control.

Fixing the Foundation

The foundation as summarised above can be further improved by undertaking the following process:

1. Availability risks must be addressed first by managing business continuity, to ensure the organisation can recover quickly when a major incident occurs.
2. Use the skills of IT audit (e.g. CISA and CRISC qualified staff), the knowledge of the IT team to risk assesses and address availability and access risks.
3. Implement a remediation plan to address availability and access risks.
4. Implement best practice IT controls (e.g. COBIT, NIST, ISO 27000) and best practices to monitor the status of the base and prevent future vulnerabilities in the organisation.
5. Coordinate control efforts with the organisation's risk management team by leveraging their expertise.
6. Automate the monitoring of the IT controls by leveraging generative AI to keep on top of the fast-moving internal and external environment.

3.4. Risk Model Maturity

Risk models is a framework that helps organisations to identify assess and prioritise potential risks and opportunities. It is the road map for navigating uncertainty. The maturity of a risk model refers to the sophistication and effectiveness of the risk management framework. A mature risk model goes beyond simply listing risks, it is the fundamental basis for risk analysis, scenario planning, and continuous improvement processes. Risk models are essential to establishing operational resiliency. Organisations at the initial stage will not have the agility to change or convert to increase their resilience, as represented in figure 5.

Figure 5
Risk Maturity Model (Carnegie Mellon)


	CONTINUUM	CAPABILITY ATTRIBUTES	METHOD OF ACHIEVEMENT
 Process Evolution	Optimizing	(Continuous Feedback) Risk management a source of competitive advantage	<ul style="list-style-type: none"> • Increased emphasis on exploiting opportunities • “Best of class” processes • Knowledge accumulated and shared
	Managed	(Quantitative) Risks measured/managed quantitatively and aggregated enterprisewide	<ul style="list-style-type: none"> • Rigorous measurement methodologies/analysis • Intensive debate on risk/reward trade-off issues
	Defined	(Qualitative/Quantitative) Policies, processes and standards defined and institutionalized	<ul style="list-style-type: none"> • Process uniformly applied across the organization • Remaining elements of infrastructure in place • Rigorous methodologies
	Repeatable	(Intuitive) Process established and repeating; reliance on people continues	<ul style="list-style-type: none"> • Common language • Quality people assigned • Defined tasks • Initial infrastructure elements
	Initial	(Ad Hoc/Chaotic) Dependent on heroics; institutional capability lacking	<ul style="list-style-type: none"> • Undefined tasks • Relies on initiative • “Just do it” • Reliance on key people

Figure 5 shows that an organisation's approach to risk management progresses through five stages:

1. *Initial*: Risk management is undocumented and relies mostly on individual efforts.
2. *Repeatable*: Risk is inconsistently defined and managed in separate areas with weak process discipline.
3. *Defined*: A standardised risk assessment/response framework is established. The organisation provides leadership and the board with an organization-wide view of risk, often in the form of a list of top risks. Action plans are implemented to address high-priority risks.
4. *Managed*: Risk management activities are coordinated across business areas. Where appropriate, risk management techniques and tools are used, with enterprise-wide risk monitoring, measuring, and reporting. Alternative responses are analysed with scenario planning and techniques like monte Carlo simulation. Process metrics are in place, but the focus remains on managing a list of risks. Discussions about risk are separate from discussions about strategy and performance.
5. *Optimising*: The focus shifts to managing risk within the context of enterprise objectives rather than managing a list. Strategic planning, capital allocations, and daily strategic and tactical decision-making all consider potential risks. Decision-makers have a reasonable level of assurance that they are taking the right risks at the right level to achieve success, not just to avoid failure. Early-warning systems are established to notify the board and leadership of specific risks that exceed the organisation's established risk appetite or risk-capacity thresholds, and when enterprise objectives are in danger. Discussion of risk at both the top management and board levels is fully integrated with the discussion of strategy and performance.

Risk Model Maturity and the Impact on Operational Resilience

Model risk maturity also directly impacts the organisation's operational resilience in the following ways:

- *Proactive risk identification*: a mature risk models goes beyond identifying common threats and opportunities. It delves deeper, considering emerging risks and potential domino effects such as contagion and risk interconnectivity this allows organisations tend to space issues before they become issues or crises.
- *Enhanced risk awareness*: Risk maturity models facilitate a comprehensive understanding of risks across the organization. By assessing current practices against industry standards, organizations can identify blind spots and areas needing improvement. This heightened awareness enables proactive risk mitigation.
- *Data-driven decision-making* mature IST models leverage data to quantify risks and identify mitigation strategies that are needed to ensure that resources are allocated more effectively to address the most critical threats and opportunities to operational continuity.
- *Scenario planning and testing*: mature risk models incorporate scenario planning allowing organisations to test their preparedness for various disruptions this helps identify weaknesses and refine response plans.
- *Continuous improvement*: the hallmark of risk maturity is a process of continuous monitoring and improvement of the risk model itself. As the organisation and the risk landscape evolves, the model adapts to remain relevant and effective.
- *Optimised resource allocation*: With a clear understanding of risk maturity, organisations can allocate resources more efficiently. They can prioritize investments in risk management initiatives based on identified gaps and critical areas, ensuring resources are directed where they are most needed.
- *Improved decision making*: Organizations with mature risk management practices make more informed and strategic decisions. By embedding risk considerations into decision-making processes, organisations are more likely to anticipate and address potential risks early, thereby minimising the probability of surprises and disruptions.
- *Stronger resilience*: A mature risk management framework also enhances organisational resilience. By systematically identifying, assessing, and managing risks, organisations become better equipped to navigate uncertainties and adapt to changing environments, thus safeguarding their continuity and competitiveness.

Benefits of a risk mature model

The benefits of a mature risk model extend beyond just improved operational resilience organisations can also result in the following:

- *Reduced costs*: proactive risk management helps prevent disruptions, which can be far costlier than untimely mitigation efforts.
- *Enhanced customer confidence*: customers are more likely to trust organisations that demonstrate A commitment to operational resilience.
- *Improved regulatory compliance*: many organisations require robust management practices. A mature risk model therefore helps to ensure improved regulatory compliance.
- Improved organisation's risk strategy.
- *Increased organisational performance*: Industry studies suggest that organisations with more mature risk models increase their organisational performance by up to a third

3.5. Robustness of the impact tolerance setting process

Where relevant, impact tolerances should generally and clearly align with the firm's defined risk appetite categories as both are focussed upon potential disruption and risk taking beyond which is unacceptable. However, operational resilience impact tolerances are likely needed to be set at a point beyond the risk appetite limit as the operational resilience limit is probably at a point beyond the often commercially driven desire of the board (which is reflected within risk appetite limits) and will therefore potentially result in intolerable harm and/or clear risks to wider market stability. What is the appropriate level for setting and monitoring impact tolerance levels, and how can these be justified and validated? Impact tolerances naturally should attach to the important business services that a firm has identified. These tolerances should have a clear relationship to specific points or components of the important business service, or to the service. A firm should challenge itself if its impact tolerances are set at an overall

important business service (IBS) level only. It should challenge itself on whether more granular tolerances would add more value in enabling the firm to more effectively identify resilience requirements and status within a particular process/service indicators that may be used to monitor IBSs and their components, thus providing a granular views of resilience status / risk. These should also be clearly linked back to the overall IBS level impact tolerances. Impact tolerances should be set at the point at which firms feel that disruption to an IBS would pose a risk to the safety, soundness, financial stability, or policyholder protection. It is therefore crucial that firms ask themselves "is there a lower level / more granular level of impact whereby significant disruption could be identified and responded to more quickly?" - if the answer is yes, then impact tolerances should be set at a more granular level.

How should data information sources be used to supplement expert judgements? Internal data sources should be used to inform and test expert judgements. This includes incident / loss / near miss data (including information on resulting impacts) that first-line teams as well as second-line risk teams may hold (e.g., back testing). This should be supplemented by externally sourced information, including the following:

- Periodic research / ongoing scanning of industry and wider news where incidents, research and other content may add evidential value to the firm's thinking.
- Scanning should include industry news / media, as well as news/media that is focussed on operational resilience topic specific items such as cyber security and physical asset management.
- Both internal and external sources of data and information can be used to both build and challenge scenarios that help develop a firm's thinking.

How can firms accommodate the heterogeneity in the end users of IBS?

- Firms should leverage work that they undertake to identify their target market to help define the characteristics of end users. Disruptive events / scenarios can be placed against these to help the firm work through and identify the potential impacts that these events may have on them.
- If a firm knows that it has a significant proportion of end users that are outside of its target market, it should seek to broadly understand their profile and characteristics to undertake the same exercise.

How can standard duration-based tolerance improve their ORF by specifying tolerances with additional metrics? Duration-based tolerances will be a core part of a firm's tolerance set in relation to operational resilience. These can be supplemented by relevant SLA based tolerances and risk-based tolerances (KRIs), to build an overall picture of resilience, which takes account of the following:

- Duration of outages or disruptions.
- Service quality.
- Threat/vulnerability sources (e.g. weaknesses identified via audit, overdue remediations, lack of key people to support the running of a key IBS, external cyber-attacks).

Duration-based tolerances can also therefore be supported by additional metrics that can act as a flag of potential vulnerabilities before any duration-based disruption occurs, which can trigger planned responses to investigate or take pre-emptive action.

3.6. Sophistication of scenario testing approaches

This section covers key aspect of scenarios and their importance to operational resilience. It first outlines the key concepts, which then lead to the development of a scenario based operational resilience system in the next section. Risk practitioners and decision makers are faced with a range of information when conducting risk assessments and planning.

A comprehensive operational risk framework requires an organisation to develop and undertake full scenario analysis to generate forward-looking synthetic data to imagine a plausible range of hypothetical events and the corresponding propagation of consequences to estimate their corresponding impact. One way to develop those futures is alternative futures analysis (AFS), which is defined as a set of techniques used to explore different future states developed by varying a set of key trends, drivers and/or conditions (US Department of Homeland Security, 2010). AFS is best suited to environments with high uncertainty and too complex, to trust a single point prediction. In a complex emerging risk environment, there is a wide range of factors that are likely to influence the crystallization of the risk. AFS can help analysts, decision-makers, and policy makers contemplate multiple futures or scenarios, challenge their assumptions, and anticipate surprise developments in various scenario analysis contexts, for example as applied to wide range of environmental modelling contexts, such as

modelling biocomplexity associated with multiple alternative uses of landscape environments (e.g. Bolte et al., 2006).

In general, scenarios refer to a range of detailed, longer-term narratives used to explore how the world might look in the future. Scenario planning is a futures-oriented planning technique used for medium to long-term strategic risk analysis and planning. It is used to explore plausible futures and to develop policies and strategies that are robust, resilient, flexible, and innovative. Scenarios are narratives set in the future, which describe how the world might look in, say, ten, twenty, fifty or even a hundred years. They explore how the world would change if certain trends were to strengthen or diminish, or various events were to occur.

Usually, a range of scenarios are developed, which represent a range of different possible futures outcomes, associated with different trends and events in a most likely, optimistic, and pessimistic future states. These scenarios are then used to review or test the operational resilience profile of a firm under a range of disruptive events. Scenarios can be used to identify critical dependencies and guide measures designed to increase resilience. They are also a useful means of identifying early warning indicators that signal alternative future outcome possibilities.'

A scenario planning tool describes a particular set of conditions that might impact a firm's operational resilience risk profile over a specified horizon. The task of a firm undertaking scenario analysis is to determine the following:

1. the impact of an external disruptive risk event on a firm's critical business operations.
2. the actions of management.
3. how firms may respond to the unfolding events described by the scenario.

It should be noted that these scenarios are not limited to purely quantitative econometric forecasts but can also be used to model a series of events that might impact a firm or the economy. They also do not necessarily represent a firm wide consensus view on how to address an operational resilience issue, but rather, they are intended to provide a basis on which different strategic issues can be analysed.

3.7. Customer-Centric Operational Resilience

Consumer duty and conduct risk are critical foundations for operational resilience not only for financial services but for all customer-facing businesses. A customer-centric foundation ensures that firms not only withstand and recover from disruptions but also maintain their obligations to customers and uphold fair market practices. As noted in section 2, legislation in the UK (Financial Conduct Authority, Conduct Risk and Consumer Duty) and Singapore (Monetary Authority of Singapore) safeguard consumers' interests and promote fair dealing. These elements interconnect in several ways.

Moreover, consumer duty and conduct risk are crucial for operational resilience in all customer-facing businesses, not just financial services. Recent legislation in the UK and Singapore aims to safeguard consumers' interests and promote fair dealing. Fair dealing has also been a focus from insurers in France, where customer loyalty has made insurers move away from the traditional business model to more customer-centric models (Chanon, 2021). The following section highlights some of the key aspects.

3.7.1. Definition and Principles

Consumer duty and conduct risk refers to the regulatory requirement that financial firms act in the best interests of their customers. This common-sense approach aims at providing fair value, clear communication, and suitable products and services. It encompasses principles like fairness, transparency, and the need to ensure that customers understand the products they are using and are treated well throughout the product lifecycle.

3.7.2. Consumer Duty

This refers to the regulatory requirement that financial firms act in the best interests of their customers. Principles like fairness, transparency, and the need for customers to understand the products they are using are encompassed in consumer duty. Prioritising consumer duty helps firms to design their

operations with the customer in mind, building systems and processes that are resilient and ensuring services remain accessible during disruptions. Adhering to consumer duty can also build improved trust and confidence in the firm by their customers, thereby facilitating more smoother communication and cooperation during operational stress. Furthermore, firms that are committed to consumer duty are more likely to have robust monitoring and response mechanisms, thereby enabling more proactive problem resolution.

3.7.3. Conduct Risk

Conduct risk involves the risk of inappropriate, unethical, or unlawful behaviour by a firm's employees and management. Managing conduct risk requires a firm to establish a strong culture of compliance, ethics, and accountability. Focusing on conduct risk ensures that operations are aligned with legal and regulatory standards, reducing the risk of breaches, and promoting ethical behaviour. Managing conduct risk also allows firms to avoid practices that might lead to significant operational failures and enhances decision-making processes.

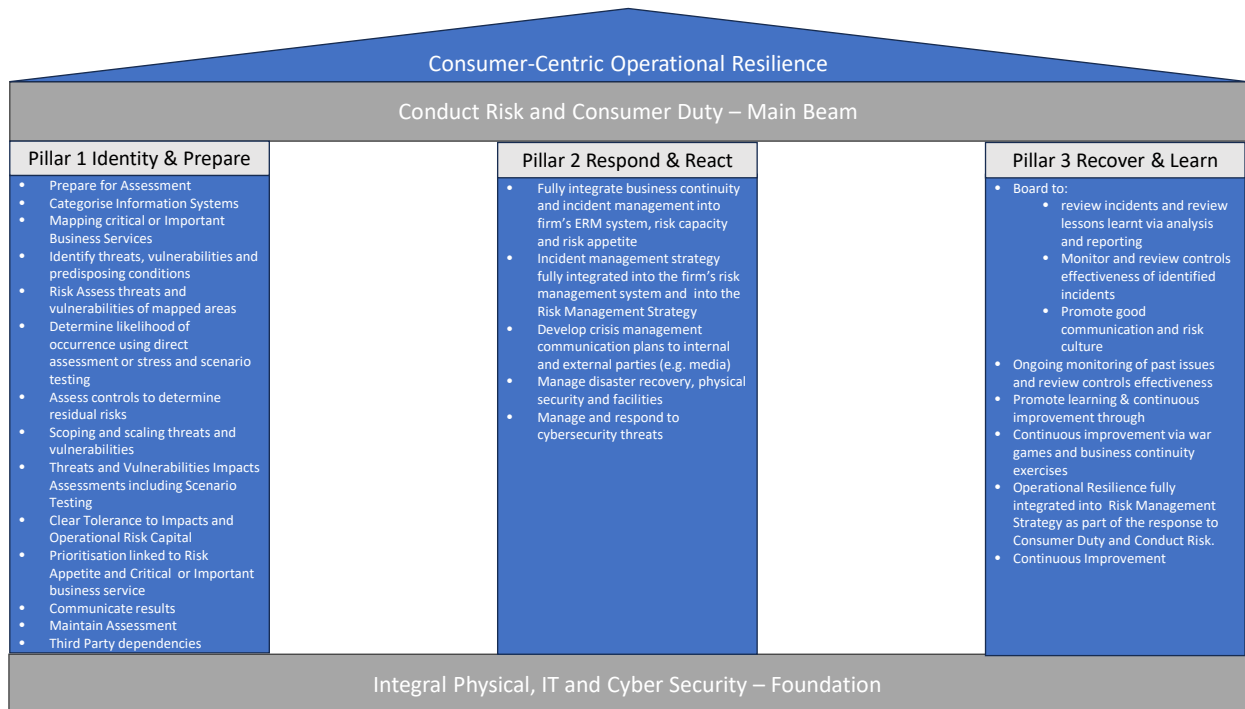
3.7.4. Integration into Operational Resilience

Effective consumer duty and conduct risk management also drive the development of robust IT systems and systems supporting customer delivery which can withstand disruptions while continuing to serve customers effectively. Feedback loops from monitoring consumer outcomes and incidents help to continuously improve operational resilience frameworks. Firms that prioritize consumer duty and conduct risk are therefore better prepared to communicate clearly and transparently with customers during a crisis. An emphasis on ethics and compliance furthermore ensures that the firm's response to operational disruptions is fair and just, thereby protecting the firm's reputation and legal standing.

In conclusion, consumer duty and conduct risk management are essential for operational resilience, by enabling firms to be more focused on the importance of upholding high standards of ethical behaviour, regulatory compliance, and customer-centric practices, ensuring long-term stability and success of a business as it encourages the right ethics and behaviours within an organisation, driving brand-loyalty.

Figure 6 summarises the inter-relationship between a consumer- centric operational resilience system, conduct risk and consumer duty as the main beam, the three pillars of identify and prepare, respond and react and recover and learn. It then identifies the Integral physical, IT and cybers security as the foundation.

Figure 6
Consumer-Centric Operational Resilience



In summary, the analysis in this section and Figure 6 suggests that operational resilience should be fully integrated into the firm's risk management strategy as part of its response to the demands of meeting regulatory requirements for consumer duty and conduct risk. The following aspects are highlighted:

The main beam comprises three "pillars":

1. *Pillar 1 – identify and prepare* – categorise key information systems, map important business services, identify and assess risk threats and vulnerabilities of mapped areas, determine likelihood of occurrence, assess controls to determine residual risks, scope and scale threats and vulnerabilities, undertake impact assessments, identify tolerance to impacts, prioritise based on risk appetite, communicate results, identify third party dependencies
2. *Pillar 2 – respond and react* – fully integrate both business continuity and incident management strategy into ERM system and link to firm's risk capacity and appetite; develop crisis management communication plans to both internal and external parties (e.g. media), manage physical security and facilities and cybersecurity risk threats
3. *Pillar 3 – recover and learn* – board to review report of incidents and review lessons learned, monitor issues and review controls effectiveness, promote learning and continuous improvement via war games and business continuity exercises.

4. An Operational Resilience Scenarios Framework

This section outlines an operational resilience scenarios framework originally developed by Habahbeh, (2024) that can be used in implementing an operational resilience strategy for a firm subject to the FCA/PRA guidelines.⁷ Section 4.1 first identifies the key emerging risks that should be considered when developing the framework. Section 4.2 then identifies various threats to operational resilience that need to be taken account of. Section 4.3 then outlines the major issues to be considered in undertaking an operational resilience assessment. Section 4.4 provides an overview of the various pathways and dependencies which can affect the robustness of an operational resilience system. Section 4.5 identifies the main factors to be considered when developing a robust operational resilience framework. Finally, section 4.6 concludes.

⁷ A more specific operational resilience system related to IT is separately discussed in section 3.3.

4.1. Emerging Risks

The Corona-virus pandemic, geopolitical polarization, the ongoing wars in Ukraine and the Middle East, and threats of nuclear events have become daily news. At the same time, recent bank runs in the U.S, ripple effects through the financial markets bring back memories of the global financial crisis of 2008-9. These turbulent times have led financial sector organizations to a renewed focus on emerging risk planning and preparedness and an enhanced focus on assessing the effectiveness of their enterprise risk management frameworks in categorizing, planning, and mitigating the effects of a wide range of emerging, Systemic events. Against this backdrop and in their business-as-usual environment, organizations are faced with four risk types, as summarized in table 1:

1. Known risks: these are easily identified, and organizations have plans and strategies to avoid and mitigate their consequences.
2. Emerging (unknown known affecting both model and/or data) risks: these are also known, but the full extent of their immediate, short- and long-term ramifications and their interaction with other types of risks are yet not fully clear; and
3. Unknown risks: Black Swans, these are unprecedented, and unimagined, extremely rare events, with massive impact, “intrinsically unpredictable” due to lack of or non-existent, reliable historical data on these events (Taleb, (2007); Taleb and Blyth (2011)).

Table 1
Risk Classification

Risk Classification		
Class	Model	Data
Known Knowns	Yes	Yes
Unknown Knowns	Yes	No
Known Unknowns	No	Yes
Unknown Unknowns	No	No

4.2. Threats to Operational Resilience

The operational resilience of Firms is at risk from a variety of discrete, linked and compound events (Cutter, 2024). Emerging risks such as control failures, third-party disruptions, infrastructure outages, technology failures, cyber incidents, geopolitical incidents, pandemics, and natural disasters tied to extreme weather events and biodiversity loss are significantly more complex and different than traditional risks. These types of risks function as amplifiers to existing risks. They are characterized as “systemic” in nature because they are *concurrent and diversified*; they happen to everyone at the same time, and they have the potential to cause a system-wide breakdown or significant disruption to human-caused economic, financial, and security systems supporting our way of life. Furthermore, emerging risks create common consequences that can cluster and cascade, because of the multiple consequences triggered by the risks. These consequences combine and accelerate within a certain risk context, and they generate unforeseen effects.

Cascading and clustering of consequences further increases the magnitude of the total systemic risk. Examples of emerging risks to financial firms include attacks on AI-enabled financial trading models, bond dumping by foreign holders of equity and debt securities, deep-fakes used to spread misinformation used to manipulate beliefs and behaviors of investors. Thus, they pose increasing threats to firms operating systems and to the supply of products and services to customers.

Linked risks are risks that have the same cause; for example, in 2010, the same meteorological weather anomaly over Russia sparked extreme heat and persistent wildfires in Russia as well as heavy rainfall fueling heavy flooding in Pakistan. Compound risks are risks that have independent causes, but their effects join in a certain risk context and amplify the consequence(s). For example, the ongoing wars in Ukraine and between Israel and Hamas, amplified by the continuous attacks on ships in the Red Sea amplifying the risks to global supply chains and raising the cost of war risk insurance and transportation costs.

In general, emerging risk is defined as the product of the likelihood and consequence of an outcome. Systemic, disruptive operational events are high-impact, low-probability events and they are considered

unlikely. Therefore, risk managers often omit to assess the impact associated with these types of risk because they do not realize that such very unlikely risks have an impact that is so large, that they dominate the calculation of total risk and thus they are worthy of special attention.

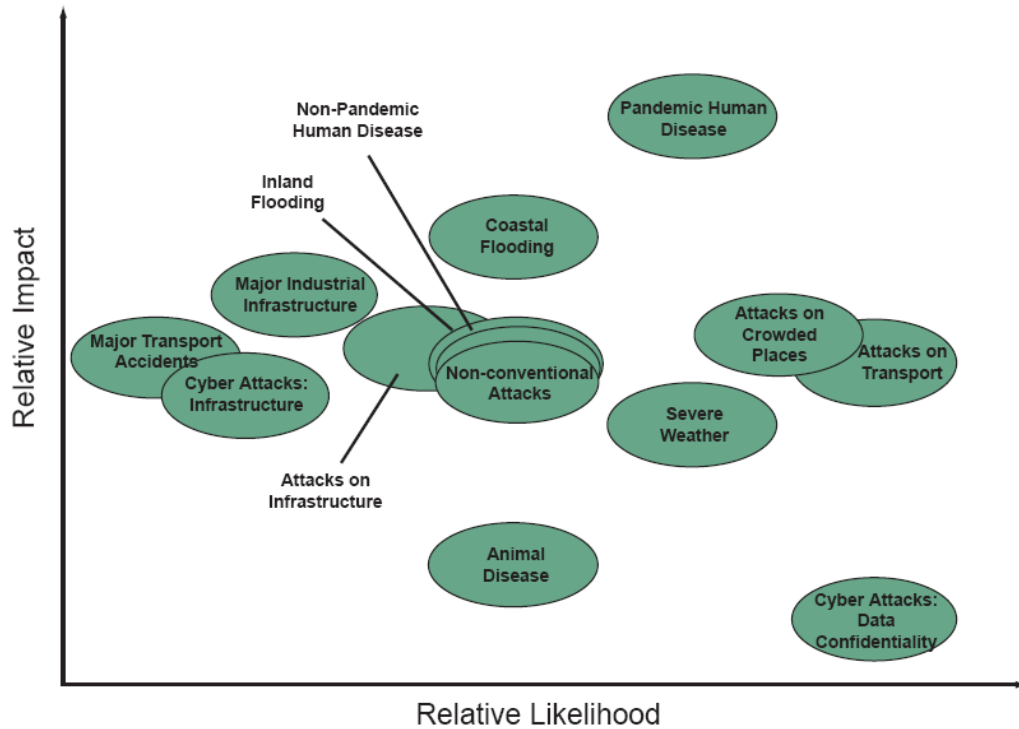
Consequently, the identification and assessment of threats posed to firms' operational resilience requires fresh thinking by considering unlikely risks and moving beyond an assessment of the risks of individual events such as cyber-attacks, wars, power grid failure, based on historical data alone, and assess *scenarios* of these events and their associated 1st, 2nd, 3rd, 4th, etc. order, societal and economic consequences over the immediate, short, medium, and possibly long term. Therefore, by identifying these types of systemic, disruptive scenarios, firms can minimize service disruptions associated with emergencies that arise from these types of risks.

Therefore, an effective ERM system should incorporate *a robust operational resilience framework (ORF)* to enhance the ability of the firms to withstand, adapt to, and recover from such events while continuing to deliver their critical operations by undertaking the following three steps:

1. identify the firms' critical operations and mapping the internal and external dependencies (e.g., people, systems, processes, third parties, facilities, etc.) required to support critical operations.
2. establish tolerances for disruption in respect of a firm's critical operations.
3. conduct scenario testing to gauge the ability of the firm to operate within its tolerances for disruption across a range of severe but *plausible scenarios*, including high impact, low probability events, and considering the normal and radical uncertainty associated with scenario design and evolution across single and multiple time horizons (King, 2020).

Figure 7 illustrates the trade-off between the relationship between the relative impact and relative likelihood of several types of events which may cause business disruption.

Figure 7
Trade-off between relative impact and likelihood of low probability, high consequence risks
(HM Government, 2023)



4.3. Operational Resilience Risk Assessment

The UK financial sector regulatory authorities defined the concept of impact tolerances as “the types of failure which would be intolerable for both their customers and financial services market providers” (BoE, PRA and FCA, 2018). Operational resilience requires a dynamic method to risk assessment rather than the static approach of looking for longer term reviews on an annual basis. The goal of an ORF is to enable management to model what may lie beyond the horizon by thinking the unthinkable in identifying, and handling unexpected events that disrupts their critical operations and to offer management an array of possible futures. Extreme risks generate *downstream, knock-on consequences and a range of triggered, linked and compound risks*. These risks tend to cause similar cascading consequences such as a failure of a nations electric power distribution systems, with knock-on effects on food, energy, transportation, and supply chains.

For example, the geopolitical threat posed by emerging technologies such as an Electromagnetic Pulse weapon (EMP) developed by an adversarial non-State actor posse a systemic threat that can hold a society at risk with catastrophic consequences (Congressional Research Service, 2008). A discrete EMP attack on a single nation, or an EMP attack on a group of nations simultaneously has the capability to produce significant damage to a nations critical infrastructures including a nations electric power grid, telecommunications, banking and financial services, fuel, energy, food and water, and transportation infrastructures. For example, In the highly networked and inter-dependent banking and financial services industry, millions of transactions happen electronically on an hourly basis. All transactions are recorded and stored electronically, and they depend on the speed, processing, and storage capabilities of electronic information technology. A large-scale terrorist attack on a developed nation electricity infrastructure using an EMP weapon can disrupt all critical infrastructure, including power, transportation, and telecommunications systems. Consequently, essential operations in key financial markets may be severely disrupted, thereby in turn increasing the systemic risks of the global financial system (McAndrews and Potter, 2002). A potential EMP attack can cause widespread functional collapse of the electric power system in the area(s) affected, and consequently disrupt the infrastructure,

utilities, global supply chains, and resource networks that service financial sectors of nations around the world.

Moreover, the risk of disinformation is increasing. Recent news reports and analysis have highlighted the risk of the use of artificial intelligence methods in enabling increasingly realistic photos, audio, and video digital forgeries, known as "deep fakes". According to a recent report on CNN, a finance worker at a multinational firm was tricked into paying out \$25 million to fraudsters using deepfake technology to pose as the company's chief financial officer (CNN, 2024).

Furthermore, deepfakes can be potentially used as character assassination tools for people working in various organizations. Further some even suggested that AI tools such as ChatGPT could be used to create a full digital "patterns of life" in which an individual digital footprint is mapped against malicious and fake personal information such as spending habits, job history to create comprehensive digital personal profiles that can be used potentially to generate false news, influencing public discourse, manipulating beliefs and behaviours, and eroding public trust, in publicly listed companies across the world, with far reaching financial implications.

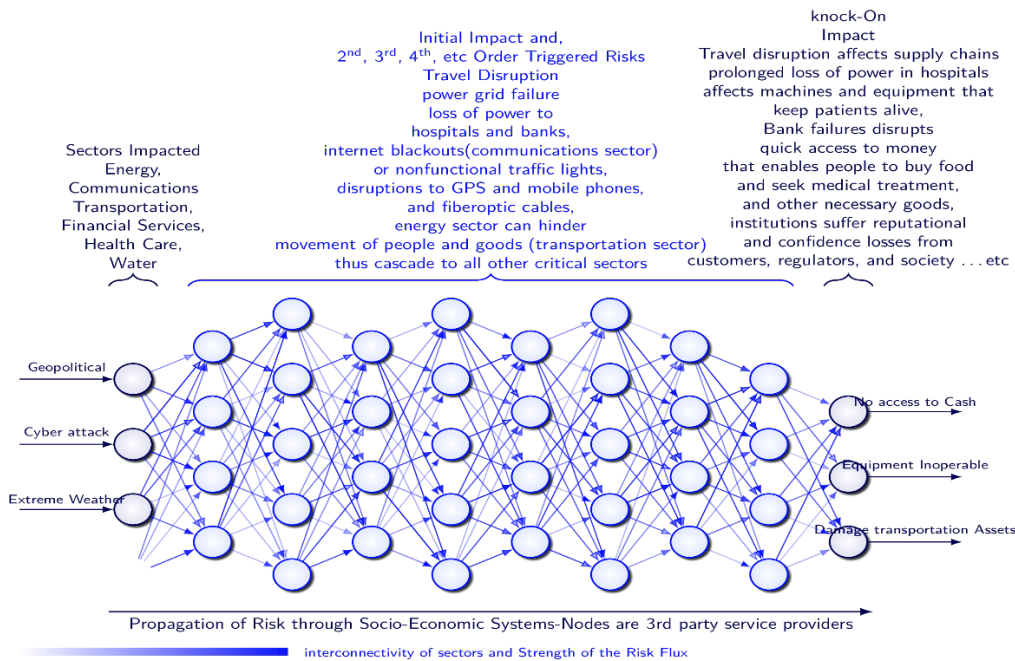
4.4. Mapping the Consequences of Operational Disruptions

A robust ORF therefore requires fresh thinking by considering unlikely risks and moving beyond an assessment of the risks of individual events causing disruption to critical business services based on historical data alone, and more focus on the *multiple pathways of cascading consequences* that these events may trigger. Moreover, a robust ORF assesses reasonable worst case (RWC) scenarios of these events and their associated 1st, 2nd, 3rd, 4th, etc quantifiable direct impacts (e.g., financial losses, deaths, injury), as well as their non-quantifiable indirect impacts (e.g., psychological damage), over the immediate, short, medium, and possibly longer term. Top-down (feed forward) and bottom-up (feed backward) Cause → Consequence analysis framework, to provide a holistic view of "what might happen?" and thereby provide the risk owner - decision maker with an enhanced understanding of the multiple pathways of linked, and compound secondary and higher risks and pathways of cascading impacts triggered by these events.

This framework provides an enhanced method of how to assess the likelihood of these events and removes some of the biases associated with low probability events by thinking in terms of the higher likelihood of the cascading consequences triggered by these events, impacting firms' critical operations, instead of the likelihood of the events themselves. The discussion below highlights the interrelationship and interdependencies between different types of events and their implications for analysis.

4.4.1 Feed Forward Emerging Risk analysis (FFA): Primary Cause → primary impact → 2nd effect → 3rd effect → 4th effect This is summarised in Figure 8 (Hababbeh, 2022b).

Figure 8
Propagation of Risk through Socio-Economic Systems

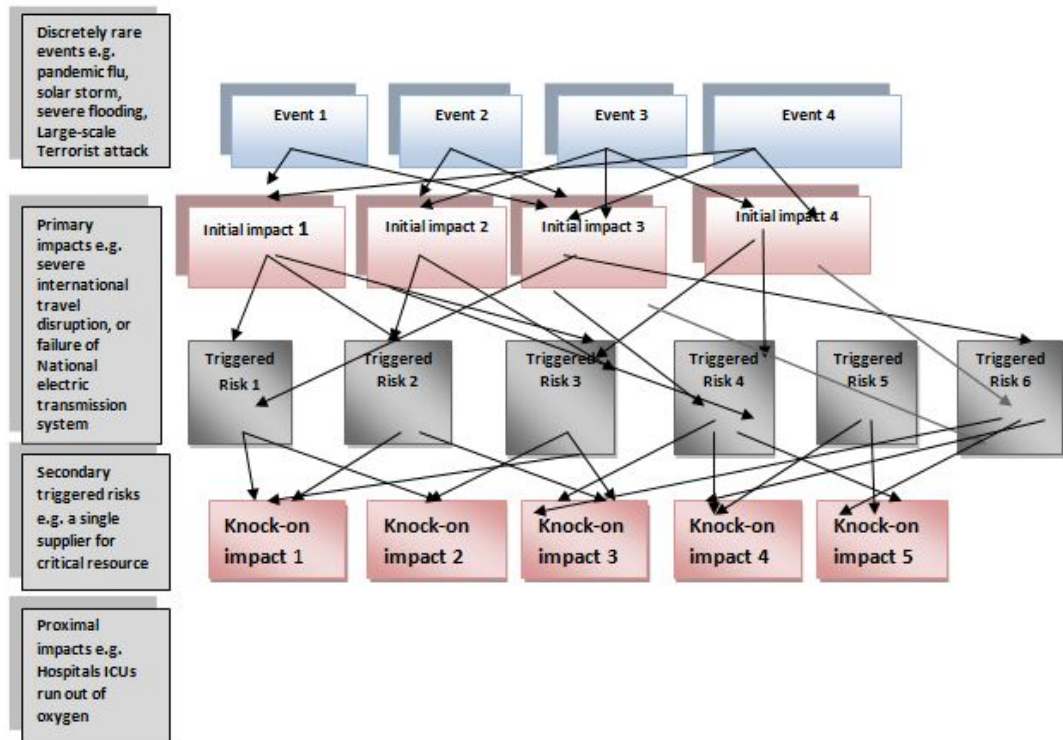


An extreme space weather event is one of several potentially high impact, but low probability natural hazards that pose a significant systemic risk to the functioning of financial markets that impact the operational resilience of financial firms. For instance, a large solar storm has multiple consequences such as loss of power and loss of low Earth orbit satellite functionality providing services to customers across the globe. These consequences might cascade into other risks such as failure of energy, food, telecommunication, and supply chains and financial markets. These impacts can be felt immediately, and the damage can be spread over the short, medium, and long-time horizons. There may also be second order impacts of events creating IT incidents. Operational incidents may also be a trigger for a cyber-attack / cyber fraud where consumers data and money are stolen. There may also be contagion effects to 3rd party providers, where one financial institution that is reliant on it for critical services (e.g. access to payment systems or telecommunications systems) can no longer serve its own customers. For example, the failure of any one of the Central Clearing Counterparties (“CCPs”) that provide collateral management, and reliable payment processes.

4.4.2. *Feed Backward Emerging Risk analysis (FFA): → 4th effect → 3rd effect → 2nd effect → -primary cause*

Financial organisations may not be aware of which scenarios lead to the risk of organisational failure. This requires the identification and assessment of the circumstances that may cause the firm’s business model to become unviable or result in its counterparties losing confidence to a critical point. For example, assess the impact of how many configurations of triggered primary and secondary risks leads to multiple, simultaneous financial services failures where customers withdraw cash from multiple banks leading to multiple, simultaneous bank runs. Figure 9 illustrates the issue in the context of emerging risks and their common consequences

Figure 9
Emerging Risks and Common Consequences



4.5. Key Considerations when Building an ORF

This section suggests that the following issues are relevant to evaluating and implementing an OR:

1. Recognise at the board level that firms' operational resilience profile needs explicit management, and they need to be considered from a holistic system based multidisciplinary approach and view.
2. The design of scenario testing should be proportional to the size, complexity, business, and risk profile of the firm, as well as its level of interconnectedness to the financial system.
3. To build a robust scenario framework that considers a range of risks, hazards, and shocks, engage with external experts to identify, evaluate and monitor these risks and the different approaches to cope with these risks properly.
4. Develop an operational resilience analysis framework for the systematic identification of emerging threats to important business services that are considered improbable, or unlikely, and develop a framework for understanding, assessing, modelling, mitigating emerging, systemic risks, and anchoring the framework in the latest theories and reliable data
5. The framework should also include the following considerations:
 - Horizon scanning to identify the most significant extreme risks to firms' critical operations.
 - Categorization of risks into three classes *discrete, concurrent, or cascades*, identify the underlying causes (drivers); do they have the same underlying cause or independent causes; are the consequences(s) discrete, compound, and cascading?
 - How likely are they to happen?
 - The range of plausible worst-case outcomes?

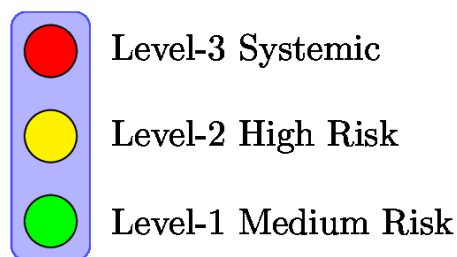
- What is the likelihood of consequences if the risk happens, and how will the risk(s) affect the firm's important business services?
- What is the timing of the consequences, are they immediate, short term, medium term, or long term?
- Assess to a reasonable degree the multiple cause-and-effect relationship driving emerging risks and the complex, cascading consequences the set-in motion.
- understand the correlations between risks focus on higher order cascading effects of the risk
- Develop reporting strategies to communicate judgement about risks to senior management in a timely manner considering the importance of using the correct vocabulary when explaining risk. Further, when reaching a judgement about a risk the following factors need to be accounted for:
 - a. Quantify the certainty level of all key judgements about the risks.
 - b. Identify explicitly the critical assumptions

6- Define the 3rd party service providers

7. Define Level of Disruption Potentially Caused to Customers

- **Level one:** disruptive event does not significantly impair the ability of banks or insurance companies' senior management to run the firm but causes a minor inconvenience to customers.
- **Level two:** disruptive event impacts the financial and/or operations safety and soundness of a firm and causes significant stress to customers.
- **Level three:** disruptive event results in a significant increase in systemic risks which threatens the operational resilience of the firm, with the potential to cause financial instability, consequentially it may cause significant disruption to the reliability and/or integrity of the quality of services provided to customers. Figure 10 summarises the different levels of disruption.

Figure 10
Levels of Disruption



8. Identify essential resources (people, technology, facilities) that support critical business services.

9. Identify impacts.

- Quantifiable impacts such as financial losses, loss of life, and injury.
- non-quantifiable psychological impacts such as the dread factor.

10. Undertake Scenario Testing Techniques and Learning Outcomes:

- Run simulations or workshop exercises based on the designed scenarios.
- Learn from the outcomes, identify weaknesses, and refine your operational resilience strategies.

- Ensure that senior management and relevant stakeholders understand the scenario methodology.
- Clearly define roles and responsibilities during disruptions.
- Establish effective communication channels to coordinate responses.

4.6. Conclusion

A robust operational resilience framework requires a firm to implement a system level view of multiple risks, and invest effort into undertaking discussions of reasonable and plausible scenarios impacting firm's critical operations in a variety of situations for each plausible risk event, based on the best available historical, statistical, and scientific evidence, and analysis of the key trends and uncertainties that will shape the strategic emerging risk landscape so that firms can minimize the strategic shocks associated with emergencies that arise from these types of operational risks.

5. Implementation issues

This section identifies some key implementation issues that affect the ability of an organisation to develop an effective operational resilience risk management framework. Section 5.1 considers the issues involved in developing operational resilience risk management systems as outlined in section 4 and identifies frameworks and examples in action. Section 5.2 then develops and implements how an operational resilience maturity dashboard can be used to evaluate how a sample of UKFI regulated banks, asset managers and insurers are dealing with the need to comply with the upcoming requirements.

5.1. Implementing Operational Resilience Frameworks

Like many frameworks, to effectively implement an ORF, the following things need to be considered / achieved:

- There needs to be clear, consistent, and strong commitment from senior management (Board and below) to emphasising the importance of the ORF and its effective operation. They need to ensure that they maintain oversight of its implementation and ongoing effectiveness. This includes ensuring the adequate provision and direction / allocation of resources.
- Wherever possible avoid developing and implementing a framework that introduces siloed and parallel processes to existing frameworks / ways of working that unnecessarily add to people's workloads. This will result in a lack of buy in and commitment to operating them effectively.
- The requirements of an ORF should be stitched into 1st line firm-wide and functional objectives, roles and responsibilities and resource plans.
- These should be integrated with existing roles and responsibilities that relate to the likes of service design and delivery, IT infrastructure, physical asset management, risk management and control, customer service and outcomes, business continuity, and disaster recovery.
- This points to the need to avoid where possible adding new policies and procedures, instead focussing on augmenting, and updating existing ones to help make OR a part of a "business as usual" working and thinking (and not a separate exercise).
- Likewise, new MI and reporting will need to be developed, but this should be incorporated where possible and appropriate into existing governance bodies and committees (changing the terms of reference of relevant committees to incorporate). Again, this re-enforces the fact that an effective ORF should be part of a firm's usual thought processes, oversight, and decision-making.
- Like any new framework or change in ways of working, close attention should be paid to user experience and feedback in operating that framework. It is likely that areas of improvement will be identified, including in relation to the adequacy of impact tolerances, the nature of scenarios and response plans. Feedback should be consistently sought to help iron out any design and operational challenges or opportunities to build further enhancements.
- As would be the case with business continuity and disaster recovery relevant events, lessons learnt following any OR event should consider the adequacy of the ORF in enabling the effective management of that event.

- From a second line perspective, firms should seek to enable an appropriate level of integration between their ORF, as both will leverage each other e.g. risk appetites and KRIs helping to provide key contextual guidance and understanding around exposures, and insights from operational resilience monitoring helping to inform the firm's understanding and assessment of its risk profile. It is crucial that insights generated by both frameworks inform the other, and do so in efficient, non-duplicative ways e.g. use a single approach/process to identify, record and assess incidents and near-misses. Risk universes, risk policies and procedures, assessment methods, monitoring tools and metrics should take account of OR and build related requirements, responses and thinking around threats and mitigation/control into them. This will also help enable the provision of effective second line oversight of OR and ORFs.

Examples of Successful Implementation

1. *COSO ERM Framework*: The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2017) developed the Enterprise Risk Management (ERM) framework, which is widely used as a risk maturity model. Industrial organizations like Microsoft and Nestlé have leveraged this framework to enhance their risk management practices. By adopting COSO ERM, these companies have strengthened their ability to identify, assess, and respond to risks strategically.

2. *Capability Maturity Model Integration (CMMI Institute, 2023)*: Although originally focused on software development, CMMI has been adapted for broader organizational processes, including risk management. Organizations such as Boeing and Lockheed Martin have applied CMMI to enhance risk management maturity within their projects and operations, leading to improved project success rates and reduced operational disruptions.

3. *ISO 31000 (see discussion also in section 2.3 above)*: The ISO 31000 standard provides principles and guidelines for effective risk management. Organizations like Coca-Cola and Siemens have implemented ISO 31000 to enhance risk maturity across their global operations. This standard helps establish a common risk language and systematic approach to risk management, fostering a risk-aware culture.

Examples in Action

Consider these real-world scenarios:

- A manufacturing company utilises a risk maturity model to identify potential supply chain disruptions. They discover a high risk of dependence on a single supplier. This insight prompts them to diversify their supplier base, mitigating the risk of production stoppages.
- A financial institution leverages a risk maturity model to assess its cybersecurity protocols. They discover gaps in employee awareness and data encryption practices. By addressing these vulnerabilities, they significantly reduce the risk of financial losses and reputational damage from cyberattacks.

Risk maturity models offer a structured pathway for organisations to strengthen their risk management capabilities and ultimately improve business performance. By assessing maturity levels, identifying improvement opportunities, and implementing targeted actions, organisations can enhance risk awareness, optimise resource allocation, improve decision-making, and build resilience. Successful implementation of risk maturity models requires commitment from leadership, integration with strategic objectives, and continuous improvement efforts. Organisations that embrace risk maturity models not only mitigate threats effectively but also seize opportunities with greater confidence in today's increasingly uncertain world.

5.2. Operational Resilience Maturity Dashboard

This section briefly outlines the most recent developments in the level of operational resilience maturity by a small number of large, regulated UK entities. The analysis is based on the OECD (2021) ERM maturity risk dashboard, which was developed initially for implementation by taxation authorities. However, the framework, being consistent with the ISO 31000 general guidance on the implementation of best practices in ERM systems, is therefore also compatible with the analysis of the maturity of operational resilience.

5.2.1. Outline of the Dashboard

The OECD (2021) risk management maturity model sets out five levels of maturity:

1. *Emerging*: this level is intended to represent those organisations that still have significant further progress they to make in developing operational resilience.
2. *Progressing*: this level is intended to represent those organisations which have made or are undertaking reforms in enterprise risk management as part of progressing towards the average level of established risk management.
3. *Established*: this level is intended to represent where most regulated entities might be expected to cluster.
4. *Leading*: this level is intended to represent the cutting edge of what is generally possible at the present time through actions taken.
5. *Aspirational*: the intention of this level is to look forward at what might be possible in the medium term as the use of new technology tools develops and as organisation move towards more seamless and real-time operational resilience.

The nine indicative attributes cover the following areas (which are set out in ISO 31000):

1. Overall risk management framework design
2. Corporate strategy
3. Governance
4. Risk culture
5. Risk identification
6. Risk analysis and evaluation
7. Risk treatment
8. Framework review and revision
9. Information, communication, and reporting

These indicative attributes are a selection of attributes that leading industry frameworks identify as important elements for implementing and sustaining enterprise risk management within any organisation. Additionally, the OSFIC (2023) identified 7 operational risk subject areas where operational resilience could be strengthened (see section 4.2.2). We therefore incorporated an additional indicative attribute into the operational resilience maturity dashboard which recorded an indicative one or zero as to whether the organization explicitly disclosed it addressed each of the following four subject areas:

1. Business continuity management
2. Crisis and change management
3. Technology and cyber risk management
4. Third party and data risk management

5.2.2. Construction of Operational Resilience Maturity Dashboard Index

An operational resilience maturity dashboard index was constructed based on research constructed content analysis an equally weighted scoring of whether the financial institutions disclosed relevant information in their annual report related to each of the five maturity levels associated with each of the nine dimensions of the OECD (2021) framework, as well as the OSFIC (2023) subject areas. For each of the nine dimensions, a score of 1 to 5 was associated with the level of disclosed alignment by the financial institution with each of the nine dimensions, as well as a score of 0 or 1 as to whether it disclosed information concerning each of the five subject area dimensions. These equally weighted scores were then each multiplied by 2 to arrive at a total maximum operational resilience maturity of 100%.

5.2.3. Implementing the Maturity Dashboard in practice

Data and Sample

The operational resilience maturity of the six largest UK listed financial institutions which are subject to the BofE, FCA and PRA (2021) guidelines in the were chosen for initial analysis, comprising the two largest banks, insurers and asset managers by total assets.⁸ The annual reports related to each of the three latest years after the issue of the guidelines (2021 - 2023) were then analysed.

⁸ The total asset size of the sample is approximately GBP 5.4 billion as of 31 December 2023.

Findings

Table 2 summarises the average maturity scores (ranging from 1 to 5) for the six UK financial institutions in each of the 10 categories, as well as their total average operational resilience maturity (%).

Table 2
Sample of Large UK Financial Institutions
Average operational resilience maturity disclosure scores 2021-2023

Category number	Description	Average score		
		2021	2022	2023
1	ERM policy and operational risk management framework	3.3	3.5	4.3
2	Corporate strategy and risk appetite	3.5	3.3	4.0
3	Corporate governance structure	2.5	2.7	2.8
4	Risk culture and context	1.8	2.0	2.5
5	Risk identification	2.2	2.3	2.5
6	Risk analysis and evaluation	1.0	1.0	1.3
7	Risk treatment	1.0	1.0	1.2
8	Monitoring, review and revision processes	2.5	2.2	1.8
9	Risk information communication and reporting	1.3	1.3	1.3
10	Operational risk management subject areas that enhance operational resilience	2.2	2.5	3.2
Total	Total operational resilience maturity %	42.7	43.7	50.0

The average operational resilience maturity score ranges vary considerably across the 10 major categories, with the highest average level for ERM policy and operational risk management framework, and the lowest for risk treatment, risk analysis and evaluation and risk information communication and reporting. Moreover, there has been significant improvements over time for only the first five categories of operational risk management, as well as the five operational risk management subject areas. The overall operational resilience maturity of the sample increased only slightly from 2021 to 2022 but increased to 50% in 2023. Overall, the results suggest that, at least for the sample of six largest UK financial institutions, there is only a progressing to established level of average operational resilience maturity. Figure 11 summarises the major trends across each of the three categories of UK financial institution over the period 2021 to 2023.

Figure 11
Average total operational resilience maturity for UK financial institutions by sector type

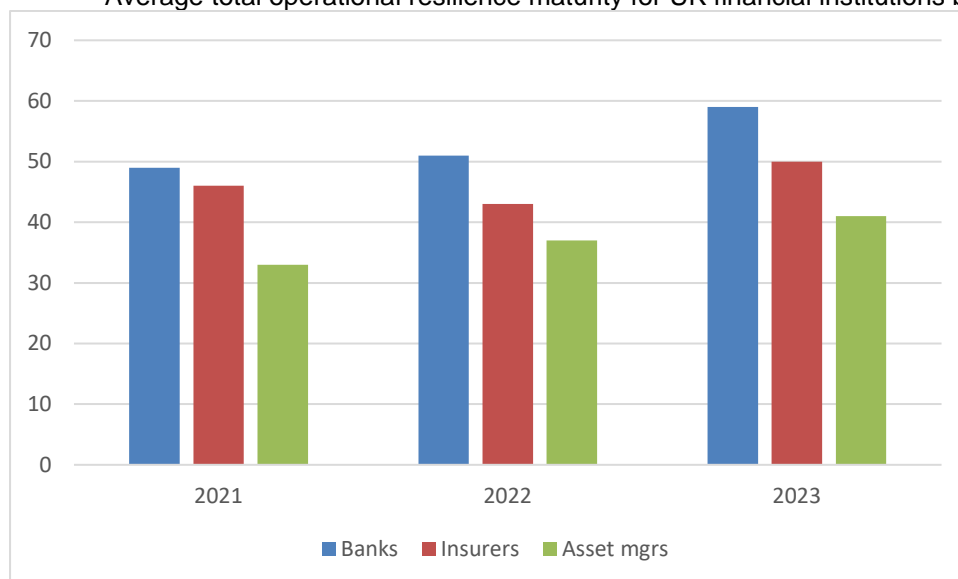


Figure 9 shows that the banks have a significantly higher level of total average operational resilience maturity than either the insurers or asset manager institutions. While each of these have gradually increased over the last three years, although the insurance industry failed to increase from 2021 to 2023.

5.2.4. Discussion of results

The results of the analysis suggest that, while the total overall operational resilience of the six largest UK financial institutions has gradually increased over time, there are significant variations across the dashboard, with implementation of overall ERM and operational risk management frameworks not being fully implemented with processes of monitoring, review and risk communication. Furthermore, there are considerable variations between types of financial institutions, with the two banks averaging established levels of operational resilience maturity while the two asset managers are still emerging and progressing stages of maturity. These results are of concern given the importance of these institutions to both the overall UK economy and to the confidence that the major players in the financial system are robust to operational resilience threats.

6. Actuarial Skills and Their Role in Operational Resilience

In this section, we explore the intersection of how these actuarial skills and their impact on the capability of UK regulated firms to assure their operational resilience.

Risks are mathematical distributions of diverse types. As businesses face increasingly complex and interconnected risks, actuaries play a vital role in enhancing operational resilience by being able to interpret these risks and model their impact. Actuaries use scenario analysis and stress testing to model extreme events. By simulating various operational disruptions, Actuaries have the capability to assess the organization's ability to withstand shocks by leveraging data analytics to capture loss events and quantify operational risks and thereby inform decision-making.

Key aspects of actuarial skills related to operational resilience are outlined below:

- *Risk Quantification:* Actuaries have the relevant technical capability and professional competency skills to quantify risks using statistical methods, probability theory, and mathematical modelling. They have the appropriate skills and competencies to assess the financial impact of operational disruptions and set risk tolerance levels.
- *Business Impact Analysis:* Actuaries possess the appropriate training and professional competencies to understand the interconnectedness of business processes. They have therefore the most relevant skills and competencies to analyze how disruptions affect critical services and prioritize recovery efforts.
- *Risk Communication:* Actuaries have therefore the most appropriate knowledge capabilities as to how best to communicate risk insights to senior executives and the board. They also have sufficient critical evaluation knowledge skills to independently advocate for risk management practices and challenge decision-making from a risk perspective.
- *Resilience Testing:* Actuaries have professional competencies to regularly participate in regulatory capital exercises. They have the appropriate professional technical training and competencies to undertake stress-test operational scenarios and evaluate the organization's resilience profile.
- *Collaboration:* Actuaries have the appropriate management capabilities and knowledge communication skills to facilitate and collaborate with cross-functional teams, including IT, finance, and risk management.

Actuaries therefore have the most appropriate and relevant professional capabilities to enable regulated financial organisations to ensure alignment of their risk strategies and resilience to ensure compliance with the upcoming UK regulatory operational resilience requirements.

7. Conclusion

This paper provides practical guidance to UKFIs in implementing the BofE, PRA and FCA (2021) guidance on implementing an effective and robust system of operational resilience. Our research is timely for several reasons. First, there is an absence of any guidance or implementation regulations that enable UKFIs to effectively deliver effective operational resilience that meets the expectations of the regulators, their primary and secondary stakeholders and UK society in general. Second, in contrast, there is considerably more guidance provided by regulatory authorities in other jurisdictions which provide valuable insights. Third, we identify and discuss several subject areas which enhance operational resilience and focus attention on the importance of solid information technology, robust tolerance setting processes and scenario testing and planning approaches. Fourth, we identify a new operational resilience scenario framework which can help UKFIs better understand the emerging risks and threats to operational resilience and how to assess and address these. Finally, we develop and test an operational resilience dashboard for a sample of large UKFIs. We find that the majority of these have yet to demonstrate fully competent and robust established or leading practices which are considered essential to demonstrate operational resilience. Operational resilience is the outcome of mitigating actions made by the risk management system of the firm. Although operational resilience has been traditionally managed through the Operational Risk Framework, many of the operational resilience risks have a financial impact. These financial impacts tend to be sudden and high impact risks, which need to be measured to be better understood for mitigating actions to be effective.

Given the lack of guidance provided by the BofE, PRA and FCA (2021) as to the form and content of the regulatory expectations of operational resilience, and relative to the more specific guidance provided by the OSFIC (2023), we recommend that a standard and mandatory level of disclosure be provided by UK financial institutions to provide greater public confidence in their ability to maintain levels of operational resilience maturity that ensure the overall viability and systemic security of the UK financial system. Appendix D provides an example of such disclosure, based on the voluntary disclosure by one of the larger financial institutions.

Our research is subject to several limitations. First, we have not considered fully the issues associated with third party risk management and their operational resilience implications, which are yet to be fully addressed by revised UK regulatory guidance. Second, we have not considered newly emerging risks such as climate change which have been recognised in the context of climate risk reporting but not yet fully integrated into operational resilience. Third, our discussion and analysis are limited to the latest available regulatory guidance and related practices and literature.

Acknowledgements

The authors like to include acknowledgements to those who have helped them in the development of their paper, David Trefusis, Fred Vosvenieks and Mairi Russell.

References

- Australian Prudential Regulation Authority (APRA) (2023). *CPS 230 Operational Risk Management Prudential Standard*. Sydney: APRA.
- (2024a). *CPG 230 Operational Risk Management Prudential Practice Guide*. Sydney: APRA.
- (2024b). *APRA Finalises Cross-Industry Guidance on Operational Resilience*. APRA Media Release 13 June 2024.
- Bank for International Settlements (2020). *FS Briefs: Covid19 and Operational Resilience: Addressing Financial Institutions' Operational Challenges in a Pandemic*. New York: BIS.
- Bank of England. (2022a). *Operational Resilience: Next Steps on the PRA's Supervisory Roadmap - Speech by David Bailey*. London: Bank of England.
- (2022b). *What Will Operational Resilience Look Like Going Forward? An Overview of the Supervisory Regulatory Position - Speech by Duncan Mackinnon*. London: Bank of England.
- (2022c). *Operational Resilience - Outcomes in Practice - Speech by Lyndon Nelson*. London: Bank of England.
- Bank of England, Financial Conduct Authority and Prudential Regulation Authority. (2018). *Discussion Paper Building the UK financial sector's operational resilience*.
- Bank of England DP01/18; Prudential Regulation Authority (PRA) DP01/18; Financial Conduct Authority (FCA) DP18/04. Bank of England: London.
- (2021). *Operational Resilience: Impact Tolerances for Important Business Services*. London: Bank of England, PRA and FCA.
- (2022). *DP3/22 - Operational resilience: Critical third parties to the UK financial sector*. London: Bank of England, PRA and FCA.
- (2023). *CP26/23 - Operational resilience: Critical third parties to the UK financial sector*. London: Bank of England, PRA and FCA.
- Basel Committee on Banking Supervision (2020). *Consultative Document, Principles for Operational Resilience*.
- (2021). Revisions to the principles for the sound management of operational risk.
- Bolte, J.P., D.W. Hulse, S.V. Gregory and C. Smith (2006). Modelling biocomplexity – actors, landscapes and alternative futures. *Environmental Modelling and Software* 22: 570-579.
- Chanon, R.D, (2021) Winter 2021 -Reflections on the European Risk Landscape, The Institute of Risk Management Magazine.
- CMMI Institute. (2023). *Capability Maturity Model Integration Version 3.0*.
- CNN (2024).
- Committee of Sponsoring Organizations of the Treadway Commission (COSO (2017). *Enterprise Risk Management - Integrating with Strategy and Performance*. Washington DC: COSO.
- Congressional Research Service (2008). *Report for Congress: High Altitude Electromagnetic Pulse (HEMP) and High-Power Microwave (HPM) Devices: Threat Assessments*. CRS: Washington DC.
- Cutter, [Susan L. \(2024\) Compound, Cascading, or Complex Disasters: What's in a Name? \(accessed May 28, 2024\)](#)
- Department of Homeland Security (US). (2010). *DHS Risk Lexicon, Regulatory Guidance*. September.
- Drew, A. (2022). Revolution: adopting operational resilience for risk management systems, *The Actuary (online)*, August
- European Commission (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission.
- European Union (2019). Regulation EU 2019/881 on ENISA and on Information and Communications Technology Cybersecurity Certification. Brussels:

- European Union. ----- (2022a). Directive EU 2022/255 on Measures for a high Common Level of Cybersecurity Across the Union.
- (2022b). Regulation EU 2022/2254 on Digital Operational Resilience for the Financial Sector.
- Financial Markets Authority (New Zealand) (2022). *Cyber Security and Operational Systems Resilience*. Auckland: FMA.
- Hababbeh, L. (2021), *Emerging Risk Landscape - Space Weather Risk*, Institute and Faculty of actuaries. (accessed June 13, 2024)
- (2022a). Complexity challenge: understanding complicated risks, *The Actuary Magazine*. (accessed June 13, 2024)
- (2022b). Unsteady states, *The Actuary Magazine*. (accessed June 13, 2024)
- (2023). Why can't we prevent bank runs? *The Actuary Magazine*. (accessed June 13, 2024)
- (2024). *An Operational Resilience Scenario Framework*. Mimeo.
- HM Government (2023). *National Risk Register - 2023 Edition*. London: HM Government.
- Hofstede, G. (2001). *Cultures Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*. London: Sage Publications.
- Hong Kong Monetary Authority (2022a). Supervisory Policy Manual Module OR-2 on Operational Resilience. Hong Kong: HKMA.
- (2022b). Module TM-G-2. Business Continuity Planning. Hong Kong: HKMA.
- International Association of Insurance Supervisors (2019). *Holistic Framework for Systemic Risk in the Insurance Sector*. IAIS. International Standards Organisation (ISO) (2018a).
- International Standards Organization (ISO). *ISO 27000 (2018): Information Technology and Security Techniques*. Geneva:ISO.
- (2018b). *ISO 31000: Risk Management Guidelines*. Geneva: ISO.
- (2019). *ISO 22301: Security and Resilience: Business Continuity Management Systems Requirements*. Geneva: ISO.
- (2024). *ISO 22301: Security and Resilience: Business Continuity Management Systems Requirements. Amendment 1: Climate Action Changes*. Geneva: ISO.
- [King, M. \(2020\), Interview with Lord Mervyn King: thinking beyond the box, The Actuary Magazine. \(accessed May 26, 2024\)](#)
- Grewal J, Hababbeh L, Acharyya M, et al. COVID-19 and the effectiveness of ERM frameworks. *British Actuarial Journal*.2022;27: e23.doi:10.1017/S135732172200017.
- McAndrews, J.J. and S. M. Potter (2002). Liquidity Effects of the Events of September 11, 2011, *Economic Policy Review - Federal Reserve e Bank of New York* (2): 59-79.
- National Institute of Standards and Technology (NIST) (2024). The NIST Cybersecurity Framework (CSF) 2.0, Washington DC: Department of Commerce. OECD (2021). *Enterprise Risk Management Maturity Model*. Paris: OECD.
- Office of the Superintendent of Financial Institutions Canada (OSFIC) (2023). *Operational Resilience and Operational Risk Management - Draft guideline*. Ottawa: OSFIC.
- Prudential Regulatory Authority. (2017). *SS21/15Statement of Policy: Internal Governance*. London:
- (2021a). *Operational Resilience. Statement of Policy*. London: Bank of England.
- (2021b). *Operational Resilience: Impact Tolerances for Important Business Services. Policy Statement PS6/21*. London: Bank of England.
- (2021c). *PRA Rulebook: CRR Firms, Solvency II Firms: Operational Resilience Instrument 2021*. ----- (2021d). *Outsourcing and Third-Party Risk Management. Policy Statement PS7/21*.
- . (2021e). *Outsourcing and Third-Party Risk Management. Supervisory Statement SS2/21*.
- . (2021f). *CBEST Threat Intelligence-Led Assessments*. London: PRA.

- (2022). *Operational Resilience: Impact Tolerances for Important Business Services*. Supervisory Statement SS1/21. London: Bank of England.
- Singapore Monetary Authority (SMA) (2022a). *Business Continuity Management Guidelines*. Singapore: SMA.
- (2022b). *MAS Strengthens Financial Institutions Business Continuity to address Evolving Threats*. Media Release 6 June.
- Taleb, N. (2007) *The Black Swan: The Impact of the Highly Improbable*. Random House, New York, NY.
- and Mark Blyth (2011), The Black Swan of Cairo. How Suppressing Volatility Makes the World Less Predictable and More Dangerous. *Foreign Affairs*. May/ JUNE 2011 (accessed May 28, 2024).
- The BP US Refineries Independent Safety Review Panel (The Baker Report 2007). The Report of the BP US Refineries Independent Safety Review Panel UK Finance. (2024).
- Walker, D. (2009). A Review of Corporate Governance in UK banks and Other Financial Industry Entities. London: Institute of Directors
- Westermann, G. (2005) The IT Risk Pyramid: Where to Start with Risk Management, Research *Briefing V1(D)* (Cambridge, MA: Sloan Centre for Information System Research).



Institute and Faculty of Actuaries

London

1-3 Staple Inn Hall · High Holborn · London · WC1V 7QJ

Tel: +44 (0) 20 7632 2100 · Fax: +44 (0) 20 7632 2111

Edinburgh

TBC

Oxford

1st Floor · Park Central · 40/41 Park End Street · Oxford · OX1 1JD

Tel: +44 (0) 1865 268 200 · Fax: +44 (0) 1865 268 211

Beijing

Level 14 · China World Office · No.1 Jianguomenwai Avenue · Chaoyang District · Beijing,
China 100004

Tel: + +86 (10) 6535 0248

Hong Kong

1803 Tower One · Lippo Centre · 89 Queensway · Hong Kong

Tel: +11 (0) 852 2147 9418

Singapore

5 Shenton Way · UIC Building · #10-01 · Singapore · 068808

Tel: +65 8778 1784

www.actuaries.org.uk

© 2024 Institute and Faculty of Actuaries