Operational Resilience Governance Guide

v.2 July 2023

Introduction

Operational disruption may be as simple as an equipment breakdown, a bad release or as extreme as a pandemic such as we have seen with COVID-19. These events may create the same consequence; the disruption of a firm's ability to deliver services to its consumers. Operational resilience is essentially the ability of firms and a sector as a whole to prevent, adapt to, respond to, and recover and learn from, operational disruptions.

The expectation on boards and senior leaders in relation to operational resilience is to set the tone from the top, championing resilience, foster a strong culture of resilience, and demonstrate that they understand their consumers and the market harm that an event could cause. These expectations are also driven by regulators' view that without the active engagement of boards and senior leaders, firms cannot meet their resilience goals.

This Best Practice Guidance documentation has been produced by the TISA Operational Resilience Governance Working Group. The Group consist of representatives from a wide range of firm types. Each section was written by one or more members of the group and reviewed by all members of the group, to provide a balanced view of each key area of the requirements. The document focuses on areas a firms Board may find useful when looking at operational resilience governance, though there can be no one size fits all solution. The document focuses on six key areas:

1. **Accountability,** how does operational resilience fit across the three lines of defence
2. **Roles and responsibilities,** Senior Management ownership and the responsibility of those managing Important Business Services
3. **Committee structure,** where does operations resilience fit into the existing forums
4. **Management reporting,** monitoring, and measuring resilience across the firm
5. **Communication,** management of internal and external stakeholders
6. **Embedding resilience,** how does operational resilience align to existing control frameworks with the firm

Governance framework

The UK regulators have clearly mandated that operational resilience is a Board-level concern. In order for the Board to provide effective oversight of operational resilience, firms need to have the right structures in place to support the review, challenge and escalation of operational resilience issues, to ultimately inform resilience decision-making.

In the short term, governance for firms will likely be focussed on how firms have addressed the regulatory requirements and identified their list of important business services (IBS), and set impact tolerances etc., and the sign-off process for the self-assessment document. However, longer term firms need to ensure they have in place structures that support the ongoing management of operational resilience, including the refresh of the self-assessment and the underlying data.

There are some key principles that firms should take into account when designing an effective governance framework to support operational resilience:

- **Accountability:** Clear accountability must be defined across the three lines of defence for operational resilience, with 1st-line ownership of operational resilience outcomes supported by 2nd-line oversight and challenge and 3rd-line independent assurance.

- **Roles and responsibilities:** Specific responsibilities for the Board and senior management should be articulated, to ensure clear reporting lines for decision-making. Whilst ultimate accountability for implementing operational resilience policies and reporting to the Board may sit with the SMF24, multiple individuals across the firm will be responsible for supporting delivery of operational resilience e.g. individuals responsible for specific Pillars (technology, people etc.) and individuals responsible for a specific IBS. Responsibilities for these individuals also need to be clearly articulated. This is discussed in further detail in the next section of this guide.

- **Committee structure:** In order to integrate operational resilience into existing governance structures, there needs to be sufficient capacity within existing forums to allow for due consideration of operational resilience matters. Consideration also needs to be given as to the membership and remit of these forums, to ensure there is the right representation in decision-making committees and that there is clarity over where decisions are escalated. For example, IBS owners need to own their IBSs and associated impact tolerance(s), so need to have a voice in discussions that will impact the resilience of those services.

Governance framework

- **Management reporting:** Both the Board and senior management will require appropriate reporting to support them in fulfilling their roles and responsibilities relating to operational resilience. Some of this will rely on leveraging existing data and metrics but applying a resilience lens to this, whilst others will require creation or collation of new data points. The key questions that the data needs to support are as follows:

    a. **Individual IBS resilience** – how resilient are individual IBSs and how close is the organisation to breaching the impact tolerance for an IBS?
    b. **Vulnerability concentrations** – looking across our IBSs, where are the key vulnerabilities that pose the biggest risk to the organisation's resilience?
    c. **Resilience investment** – where, and how much, do we need to invest to improve our resilience? What is the cost/benefit analysis associated with this?
    d. **Managing resilience issues** – when resilience issues arise, are we able to identify, manage and escalate them, including tracking actions taken on the back of these issues and the impact of them?
    e. **Strategic change** – how are changes in the organisation impacting our current or future resilience profile?

- **Embedding resilience:** Operational resilience needs to be embedded into business decision-making rather than operating as a silo. That means integrating operational resilience considerations into processes (and related committees) around change management, supplier management, enterprise risk management etc., so that there is collective buy-in and accountability for resilience across the organisation. The practicalities of how this works for Outsourcing and Change Management are described in further detail in this document.

- **Importance of documenting a governance framework:** A firms' governance framework for operational resilience should be documented and available to relevant team members. Firms can reap the benefits of a documented governance framework as it produces a written record of how everyone should work, appropriate processes to follow when there is a chain of personnel, relevant training on said process, thus developing a clearer picture on how best to support resilience. An accurate and well-documented governance process is the best indication that a firm has adopted one. Documented governance processes can be shown to the regulators and auditors to display a complete view of their governance

Roles and responsibilities

As set out in the previous section of this guide, the regulators have deliberately pushed operational resilience to the top of the agenda for Boards. This has been achieved both through direct language in policy and through engagement with Non-Executive Directors and holders of Senior Manager Function (SMF) roles during interviews, bilateral meetings and industry events. Many TISA member firms have seen movement towards the 'equal footing' that the regulators emphasised between financial and operational resilience from the Board down.

The UK regulators explicitly outline that the Board is responsible for providing effective oversight of operational resilience work, driving improvements (particularly where the firm is outside tolerance), explaining the reasoning for any judgements to remain outside tolerance to the regulator, and considering operational resilience when making strategic decisions and . The UK regulators also require the Board to explicitly:

- Approve a firm's important business services and associated impact tolerances
- Approve the resource mapping exercise
- Approve and regularly review the self-assessment document, **at least annually**. There should be a formal timetable to review.

In order to achieve this, the Board is required to possess sufficient knowledge, skills and experience to provide constructive challenge to senior management, as well as to have appropriate management information on operational resilience. As a result, many firms have undertaken Board engagement and training sessions in order to bring members up to speed on the regulatory requirements and help facilitate and evidence sufficient Board challenge.

All of these considerations apply also whenever there is a significant Change to the business, e.g. new business lines, change of major outsource partner, new data centres or any other significant change. Any major project should therefore incorporate operational resilience impacts.

Firms are also giving significant focus going forward to developing the monitoring and reporting capabilities to support the Board in their role. This is further discussed later in this guide.

Whilst the Board responsibilities are significant when it comes to operational resilience, for many firms the more challenging area of focus has been adapting Executive and Management roles and responsibilities to support the Board in their role, and to deliver both better outcomes and effective governance of operational resilience. There is no template approach, which requires each member firm to consider their organisational culture, operating model and existing governance framework and adapt it as they see fit, in line with the first principle of the Basel Committee's papers on operational resilience.

Roles and responsibilities

It is also important that any change is sustainable, hence key staff across the organisation should be made aware of their roles (from 'Board room to the boiler room') and how they contribute to the firm's resilience objectives. However, at the senior management level there are some key themes that might be considered when reviewing roles and responsibilities:

SMF 24 (or equivalent): Accountable for the firm-wide approach to achieving operational resilience.

It is important to note that the SMF 24 (Chief Operations Function) is only a requirement for firms operating under the Enhanced Senior Managers and Certification Regime (SM&CR). However, the importance of clearly-defined leadership and sponsorship of the resilience framework remains, regardless of the designation of a SMF 24 or otherwise.

Firms without a formally designated SMF 24 typically assign responsibility to operations and/or technology executives who might hold the Chief Operations Function in an Enhanced firm.

This senior leader might be expected to:

- Own the framework and supporting standards or methodologies used to manage and monitor resilience across the firm.
- Establish and chair a resilience steering group (or consider resilience as part of the agenda of an existing committee) to bring together the other stakeholders described below with the risk, control and audit community.
- Represent the resilience framework throughout governance including at relevant Boards or Board Committees.
- Be the ultimate decision-maker for resilience challenges and manage (healthy) tension between Important Business Service Owners (see below) and those Pillar leads (see below) responsible for supporting people, processes, technology, suppliers, facilities and information.
- Ensure the customer is kept up to date, with the appropriate communications, at the right time, using the right method and the right messaging.

Depending on the extent of the Risk function's involvement in setting the firm's direction on resilience, the SMF 4 (Chief Risk) could also have a formal role in co-chairing relevant committees in support of their first-line peers. Larger groups may also see a role for an Operations-focused SMF 7 (Group Entity Senior Manager) who may co-ordinate multiple legal entity SMF 24s or equivalents.

Roles and responsibilities

Pillar Owner(s): Responsible for managing the resilience of supporting processes and/or dependencies

All firms have many of the key building blocks required to manage and monitor the resilience of their organisations – it is part of doing business and managing operational risk. There will often already be senior leaders responsible for the resilience of supporting:

- People
- Processes
- Technology
- Third Parties (including suppliers)
- Facilities
- Information (including data and security)

These leaders are required to maintain service through business as usual as well as disruption. Often, these individuals only need to be engaged in the resilience framework and provided with a steer on the resources that have been identified as supporting IBSs to incorporate into their existing criticality framework(s). Once engaged they might be expected to:

- Support the delivery and maintenance of the IBS framework and wider resilience approach.
- Provide skilled and experienced staff to support resilience activities such as incident management, scenario testing and prioritisation of remediation activities.
- Deliver investments into the resilience of IBS including those actions required to remain within Impact Tolerance by March 2025.
- Provide relevant risk and performance data or metrics to enable oversight of service resilience and wider firm resilience.
- Assess the impact to the consumer – this is a key expectation of Consumer Duty, where firms will be expected to understand the demographic of their customer base, and therefore the impact of any resilience incident.

Specific requirements around third party risk management, and the incorporation of resilience into existing frameworks and processes, are further discussed later in this guide.

Roles and responsibilities

Important Business Service Owner(s): Responsible for the outcome that a business service delivers

One major stumbling block that many firms have identified is that Important Business Services (IBSs) are not typically delivered by one team, function or in some cases geography. It is generally accepted that a single individual needs to be accountable for the end-to-end IBS, and this has been recognised by the FCA and the PRA when they engage with firms and ask them 'who owns this this IBS?' Such individuals are often senior first-line business leaders and may even be designated as SMF 6 (Head of Key Business Area) or be delegates of such an individual.

This individual might be expected to:

- Approve the designation of the service as Important, agree associated Impact Tolerances and key artefacts e.g. Scenario Testing outcomes.
- Prioritise investments into the resilience of a service including those actions required to remain within Impact Tolerance by March 2025.
- Oversee the maintenance of the IB Service's documentation including revisions when material changes occur to how the service is delivered
- Engage with Pillar Owners to manage budgetary, risk management, delivery or role/responsibility challenges as they arise.

Whilst the IBS owner might delegate parts of their role, they will often remain personally accountable throughout the wider governance framework.

TISA

Resilience decision making

Resilience vulnerabilities may be identified through the IBS mapping, resource assessment or scenario testing exercises. These may relate to a single IBS or be systemic vulnerabilities of greater severity.

Firms will need to determine what remediation actions are necessary to address these vulnerabilities, in order to enable their IBSs to remain within their impact tolerance(s) in the event of a disruption.

Firms will need to weigh up the costs associated with any such remediation. Discussions should be initiated on prioritisation between both IBS owners and pillar owners, as some resilience vulnerabilities will have a greater impact than others on the ability to provide the important business services to customers and, in the event of an outage, to remain within the Impact Tolerance. It is important to consider the impact to consumers in this prioritisation exercise. Meanwhile, other vulnerabilities may not have as great an impact on a single IBS, but the impact may be pervasive across multiple IBSs.

High priority findings should be escalated to the Board, particularly where funding decisions are required. Investment prioritisation can then be discussed and actioned. This should particularly include escalation of any decisions to not remediate a vulnerability, alongside the rationale for this decision.

Firms should ensure strong oversight of remediation activity, including:

- Maintenance of a log of all remediation actions to resolve resilience vulnerabilities
- Allocation of a suitable pillar owner and IBS owner for each remediation action, to ensure accountability
- Monitoring of progress of actions against delivery dates, and escalation of issues or delays

Where actions are tracked through separate programmes of work, the operational resilience team should be engaged with the change team, and track delivery against action dates.

Resilience transition and monitoring

As the business is moving through the transition phase up to 2025 firms should be reviewing their vulnerabilities and carrying out stress tests with evolving complexity. The stress tests should incorporate severe but plausible scenarios and the resulting identified vulnerabilities should then be addressed by the firm in their operational resilience plan.

Self assessments should be regularly refreshed to show the progress made, operating models should evolve and progress in the remediation of vulnerabilities should be documented.

Your self-assessment should look different in 2025.

Key to supporting resilience decision making is ensuring that firms have in place the right mechanisms to monitor and measure resilience. We talk at a high level on slide 4 about what the key questions are that data needs to support, but what does that mean in practice?

Firms will have a wealth of data already across both first and second line that can be leveraged for the purposes of monitoring resilience. The challenge is being able to extract, collate and make sense of that data. This will include data that speaks to the inherent vulnerability of resources (e.g. data on the financial viability of third party suppliers or on whether BC or DR plans exist and have been tested) as well as more dynamic data on the performance of resources (e.g. data on operational risk events/incidents, instances of CPU capacity exceeding certain thresholds or on the number of application errors or malware attack attempts, and data on customer withdrawals or complaints).

This data will likely sit across multiple teams and functions across Operations, Technology, Risk, Front Office etc. As such, firms will need to consider what their data and technology strategy looks like going forward, to help support them with this monitoring. Ensuring consistent taxonomies so that processes, systems and teams etc. are all denoted in the same way across different systems and different datasets is a key first step to ensuring data alignment across the different systems that data may sit across.

Not all data points will be equal and so judgement will be needed to determine how these data points get aggregated, what they mean collectively for the resilience of an important business service, how this gets reported on, and what issues need to be escalated for discussion or decision making. This is where the IBS owner will play a key role, in bringing this view together and providing a holistic overview of an IBS. The pillar leads will also play a key role to help tease out vulnerabilities or issues that may be impacting multiple important business services.

Communications

As per SYSC15A.8 and PRIN2.1.1R Principle 7, firms must maintain an internal and external communication strategy to act quickly to reduce the anticipated harm caused by operational disruptions. Further, firms should be mindful of the communication needs of all customers (including vulnerable customers) and should consider how they would provide important warnings or advice quickly to consumers and other stakeholders where there is no direct line of communication – see proposed SYSC15A.8.2G. This communication strategy needs to be included in a firm's self assessment document.

There are several areas organisations should ensure they have addressed in developing their communication strategy:

External stakeholder management:

- Customers or clients need prompt and clear information when an incident occurs and during the resolution process. In order to achieve this, firms need to understand their customer or client base, how they engage with the firm, the outcomes that they are looking to achieve, and how these might differ across different customer or client types. This will drive the design of the communication strategy. One size may not necessarily fit all, and firms may want to consider more than one strategy for different customer or client types. This is as per the guidance and rules in relation to the "Consumer Understanding" aspect of Consumer Duty
- Whilst customers or clients are clearly a key focus for external communications, firms should also be mindful to consider other external communication that may be necessary, for instance communication with suppliers, shareholders or investors, market infrastructure providers, and the general public. The nature, frequency and format of communications needs to be tailored to these different stakeholder groups.

Regulator engagement: Regulators will expect to be informed on any issues they would reasonably expect to know about. Firms will need to inform regulators on any incident(s) as soon as possible. Organisations should therefore have a clear communication and escalation process in place. Regulators will also expect to see process mapping, tolerance setting and stress testing processes and documents. Identifying current or potential vulnerabilities is essential and again communicating these and how they are being managed to regulators is paramount.

Internal communications: In the event of an incident, or potential near miss, upward information flows should be swift and unimpeded to enable informed and rapid decision making. There should also be a downward dissemination of lessons learned and actions to address.

Firms should be able to utilise existing communication strategies from business continuity and resolution planning work, however these may need to be further fleshed out or enhanced. For instance, firms need to ensure that any existing communication strategy engages important business service owners and pillar owners.

Embedding resilience

Operational resilience links closely to a number of existing regulatory concepts. A key focus for firms therefore needs to be how operational resilience can be embedded into, or align with, other risk and control frameworks that support firms in adhering to these requirements, including:

- **Consumer Duty:** firms will need to consider the consumer during any operational resilience exercise or event. This will include understanding the demographic of customer base of the firm, in order to determine the impact any event may have; and then determine the communication strategy and need of the customer when an event occurs.
- **Business continuity and disaster recovery:** firms will want to consider how existing business continuity and disaster recovery plans align with operational resilience work, including ensuring that any RTOs for individual processes or systems are aligned with the impact tolerances for the important businesses they support and considering how impact tolerance testing and BC/DR testing can be aligned or integrated to increase efficiency but still ensure firms get the distinct outputs they need.
- **Incident management:** firms need to have a clear plan for identifying, managing, escalating and reporting any operational resilience incidents, particularly those that result in a breach of impact tolerance for one or more important business services. Firms may need to review and enhance existing incident management processes accordingly, including to ensure that all operational resilience incidents are captured by this, and ensure important business service owners are engaged as stakeholders in the process.
- **Outsourcing and third party risk management:** outsourcing and third party risk management processes may need to be enhanced to ensure firms understand where they are reliant on third parties to deliver important business services, to enhance processes for onboarding a new third party that will support an important business service, and to assess the resilience of third parties (upfront and on an ongoing basis).

Embedding resilience

Operational resilience links closely to a number of existing regulatory concepts. A key focus for firms therefore needs to be how operational resilience can be embedded into, or align with, other risk and control frameworks that support firms in adhering to these requirements, including:

- **Operational risk management:** in addition to clarifying how risk appetite and impact tolerance relate, firms will also want to consider how operational risk data can be easily leveraged for operational resilience purposes, including event or incident data as well as information from risk and control assessments. That may mean incorporating resilience into a firm's impact taxonomy (where it has one), and considering re-aligning risk and control assessments by process or end-to-end business, to enable easier mapping to important business services.
- **Change management:** change needs to be managed in a way that supports resilient outcomes. As such, business and IT change processes may need to be enhanced to suitably cover the resilience implications of change. Similarly, new product approval processes may need to be enhanced to ensure any new products, or significant changes to existing products, consider how this may change the IBS profile of a firm.
- **Recovery and resolution planning:** where firms have identified critical functions and operations, core business lines and critical resources as part of recovery and resolution planning, work may be needed to articulate how these align with, or differ from, the important business services and critical resources identified for operational resilience purposes. This will be particularly important for global firms, as they BCBS and US regulatory requirements have a wider focus on the resilience of critical operations (rather than important business services).

Outsourcing and third party risk management and change management in particular are explored in further detail in the following slides.

TISA

Embedding resilience

Outsourcing and third party risk management

Outsourcing has many benefits for firms, in their business models, but it does come with inherent risks. And these risks are exacerbated by the operational resilience requirements. Firms not only have to be concerned about their own potential operational failings and recovery plans, but those of third parties too. And often third parties who may not be fully inclined to align themselves to regulatory requirements.

For all firms using outsourced providers, the standard maxim remains – you can outsource the activity, but not the responsibility. There will always be the Principle 3 and SYSC 8 expectations that you will manage the outsourcing relationship effectively. These expectations include:

- Having a structured process to assess, onboard and monitor outsourced providers
- Having contracts in place, with clear rights to assess, and termination
- Being able to demonstrate that you understand the activities the outsourced provider is undertaking, and the risks

However, the operational resilience requirements add another layer to the inherent risks of outsourcing, and it is important that firms recognise this, and control against it. For the purposes of undertaking the operational resilience assessment (process mapping of resources, developing impact tolerances etc.), any outsourced services should be treated the same as insourced services, and assessed with the same level of rigor.

This clearly presents a challenge for firms if outsourced providers are unwilling to engage with the process and provide the required information. If this is the case, firms need to consider whether the outsourced service can be continued.

The first point for this engagement and assessment will always be with the 1st Line risk owners. But it is important for firms to bring in 2nd Line, and potentially also 3rd Line too. Historically there is always some degree of reticence with 2nd and 3rd Line functions engaging with outsourced providers. But firms need to consider the specific challenges of the operational resilience requirements, and draw in the specialisms of the control functions, as required.

2nd Line Risk, in particular should be considering operational resilience within their risk reporting and Risk & Control Self Assessment exercises. And when it comes to outsourcing relationships, taking a view as to whether the activities can still be undertaken, inside risk appetite.

Embedding resilience

Change management

High profile failures have focused regulatory and supervisory attention on the risks that change projects can pose to the operational resilience of firms. The volume, speed and complexity of change can present a significant challenge to many firms, and it can be during change programmes that disruptions or breaches can occur to a service.

Firms need to be able to innovate, keep the complexity of their business, products and associated systems manageable and ensure older systems are maintained and up to date. Firms must do this while minimising the likelihood of incidents, failures, and the disruption to customers. That means embedding operational resilience into business decision-making, including change management processes. Considering from the outset of a program what may go wrong and planning for avoidance, mitigation and recovery should a failure happen are all critical. It is good practice for firms to document the operational resilience considerations and specific guidelines, as part of the change management process.

Systems inevitably grow, but firms that have taken the steps to understand and update their IT portfolio and have in place clear processes to map their evolution, will deal with complicated but understandable systems rather than complex and obscure ones. They will likely spend fewer resources fixing recurring issues and can focus on extracting value from their pool of IT assets.

Change programme delivery is more often than not, separate from business as usual, and most interaction focuses on technology change management, service transition and training for the new systems. Embedding operational resilience into change management relies on earlier interaction with the first line, second line and third party suppliers, to make sure business owners and those managing the change understand the impact on the resilience of the firm's Important Business Services, their sub processes and other critical functions.

This isn't about focussing on service resilience at all costs, but firms need to understand how a change programme will impact regulatory and customer requirements, and whether it will result in any degradation in the resilience of one or more services.

Building contingency plans for new elements of architecture, as they are under development, will help firms to remain within their Impact Tolerances, supported by robust scenario testing. Whilst a mature testing model will include a variety of approaches to ensure a service can remain within the Impact Tolerance, it is however important to include more severe but plausible scenarios as part of testing in order to establish and understand the breaking point.

Please remember that the information contained within these statements is for informational purposes only and is not intended as a substitute for the need of each firm to understand its own requirements and determine its own procedures that are relevant to its business. The information contained is for general guidance only, is not exhaustive and may change from time to time.