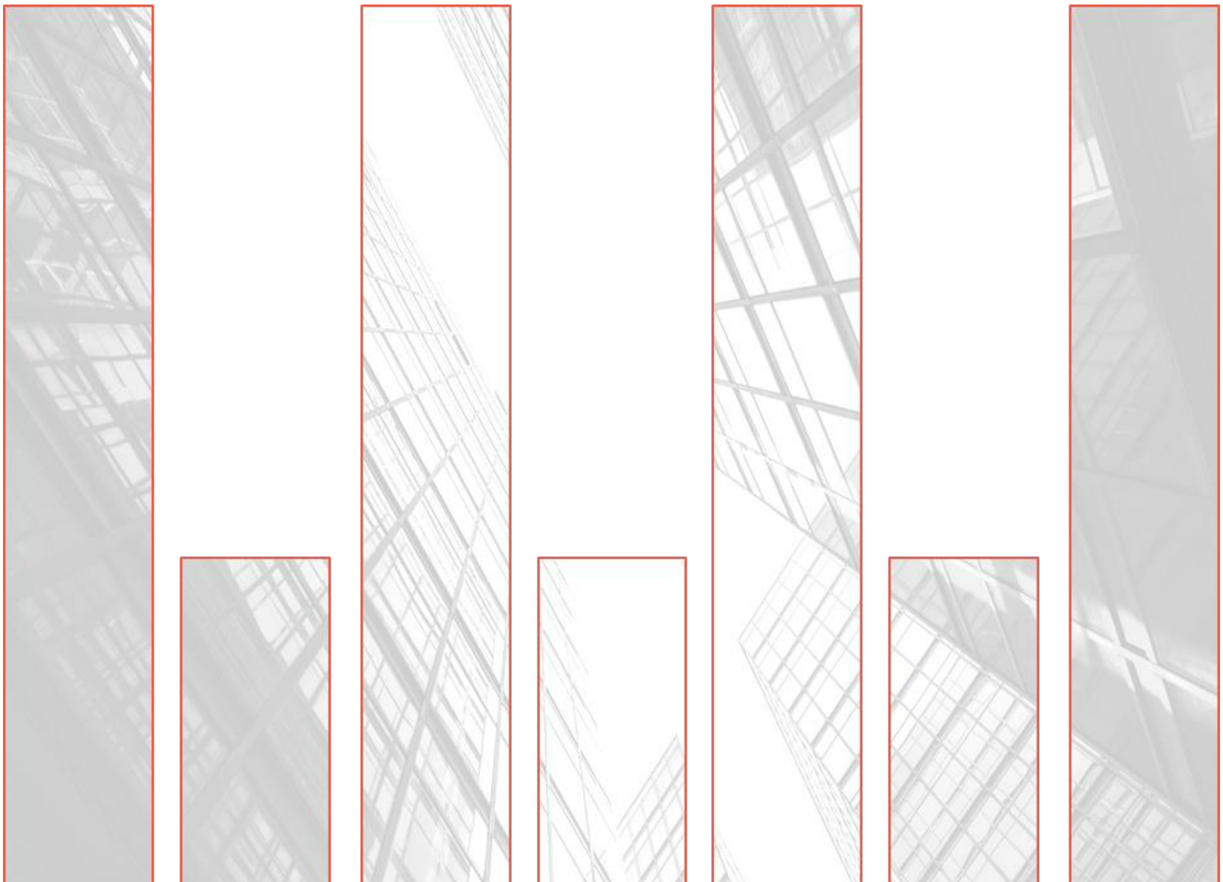
CMORG
CROSS MARKET OPERATIONAL
RESILIENCE GROUP

# Guidance for Firm Operational Resilience

VERSION 3 | APRIL 2025| TLP CLEAR



# Contents

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

# 1 Introduction to the Guidance for Firm Operational Resilience

The Operational Resilience Collaboration Group (ORCG) is a sub-group of the Cross Market Operational Resilience Group (CMORG) – the primary venue for collective action between the private sector and public authorities in the UK's financial sector. Established in 2019, the ORCG facilitates collaboration between financial institutions that have a common interest in operational resilience, focusing on shared problems that firms may not be able to address alone.

In response to the initial issuance of new policy requirements for operational resilience from the UK financial authorities in 2021, the ORCG had commissioned the development of guidance for its members to assist with interpretation and implementation of these policies. This guidance has since been updated, with the second version published in November 2023 and the third version (being the current iteration) published in April 2025.

## 1.1 Purpose of the Guidance

Following on from the development of the original guidance produced in 2021, this document provides an **update** to firms on the guidance to implementing operational resilience. This guidance is specific to the key requirements set out by:

- the Prudential Regulation Authority (PRA) in their Supervisory Statement SS1/21 'Operational resilience: Impact tolerances for important business services'; and
- the Financial Conduct Authority (FCA) in their Policy Statement PS21/3 'Building operational resilience'.

It also addresses the requirements for Financial Market Infrastructures (FMIs) as set out by the Bank of England (BoE) in their Supervisory Statement 'Operational Resilience: Recognised Payment System Operators and Specified Service Providers'.

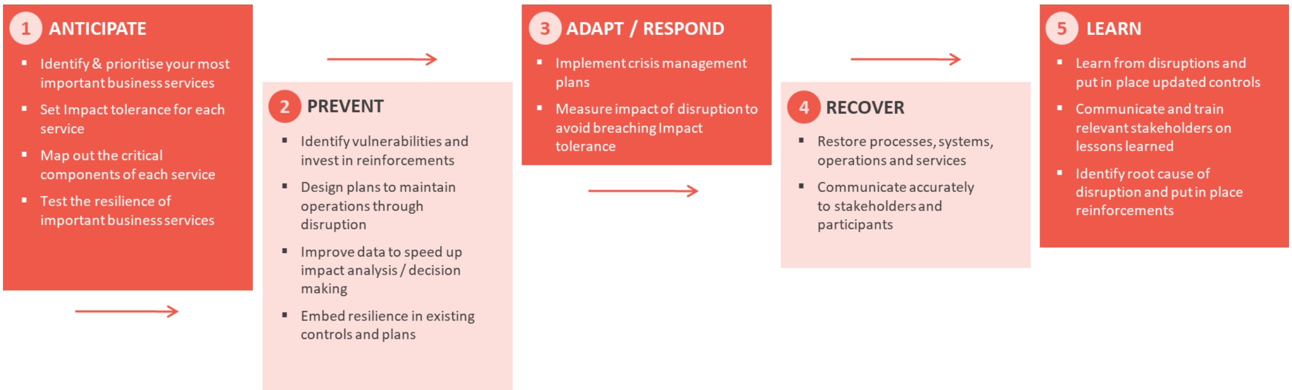
This guidance does not address the requirements of other international regulations related to operational resilience, nor the expectations of authorities in other jurisdictions.

The content should be considered high-level principles that can be used proportionately by a firm according to its size, scale and complexity. It is not intended to be prescriptive nor mandatory, but rather to support completion of individual firm documentation that aligns to their specific corporate governance requirements and templates.

## 1.2 Defining operational resilience

Operational resilience is an organisation's ability to anticipate, prevent, adapt, respond to, recover, and learn from internal or external disruption, continuing to provide Important Business Services (IBSs) to customers and clients, and minimise any impact on the wider financial system when, not if, disruption occurs.

*Figure 1. Lifecycle of an incident*



1 ANTICIPATE

- Identify & prioritise your most important business services
- Set Impact tolerance for each service
- Map out the critical components of each service
- Test the resilience of important business services

2 PREVENT

- Identify vulnerabilities and invest in reinforcements
- Design plans to maintain operations through disruption
- Improve data to speed up impact analysis / decision making
- Embed resilience in existing controls and plans

3 ADAPT / RESPOND

- Implement crisis management plans
- Measure impact of disruption to avoid breaching Impact tolerance

4 RECOVER

- Restore processes, systems, operations and services
- Communicate accurately to stakeholders and participants

5 LEARN

- Learn from disruptions and put in place updated controls
- Communicate and train relevant stakeholders on lessons learned
- Identify root cause of disruption and put in place reinforcements

## 1.3 Definitions

| Term | Definition |
|---|---|
| **Business Continuity Management (BCM)** | The capability of an organisation to continue the delivery of products and services within acceptable timeframes at a predefined capacity during disruption. |
| **Business service** | A 'business service' is a service that a firm provides to an external end user. Business services deliver a specific outcome or service to an identifiable user and should be distinguished from business lines, such as mortgages, which are a collection of services and activities. They will vary from firm to firm. |
| **Critical functions**[1] | Activities, services or operations (wherever carried out) the discontinuance of which is likely (a) to lead to the disruption of services that are essential to the economy of the United Kingdom, or (b) to disrupt financial stability in the United Kingdom, due to the size, market share, external and internal connectedness, complexity or cross-border activities of a bank or a group which includes a bank (with particular regard to the substitutability of those activities, services or operations). |
| **Financial stability** | The impact on the wider financial sector and UK economy, including:<br>• the potential to inhibit the functioning of the wider economy; in particular the economic functions listed in SS19/13 'Resolution planning';<br>• the potential to cause knock-on effects for counterparties, particularly those that provide financial market infrastructure or critical national infrastructure; and<br>• whether the service is covered by an impact tolerance set by the Bank's Financial Policy Committee. |
| **Important Business Services (IBS)**[2] | The services a firm provides (or which are provided by another person on behalf of the firm) which, if disrupted, could cause (1) intolerable levels of harm to any one of the firm's clients; or pose a risk to (2) the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets; (3) the firm's safety and soundness; (4) the financial stability of the UK; or (5) policyholder protection (in the case of insurers). |
| **Impact Tolerance (ITOL)**[3] | The maximum tolerable level of [unmitigated] disruption to an IBS, as measured by a length of time in addition to any other relevant metrics, reflecting the point at which any further disruption to the IBS could cause intolerable harm to any one or more of the firm's clients, policy holders or pose a risk to the soundness, stability or |

[1] Critical Functions: Banking Act 2009, Section 3 (1)

[2] Important business service - FCA Handbook

[3] Impact tolerance - FCA Handbook

| | |
|---|---|
| | resilience of the UK financial system or the orderly operation of the financial markets. |
| **Mapping** | The process of identifying and documenting the processes that underpin IBSs, and the resources that are critical to the delivery of these processes. |
| **Market integrity** | Where the outcome of disruption detrimentally affects:<br>i. Another organisation's ability to function normally;<br>ii. The consumers of other organisations; and<br>iii. Confidence in the financial system. |
| **Processes** | A structured set of activities required to produce a specific output such as an IBS. Processes may be considered a resilience pillar, but it may also be useful to see processes as being enabled by underlying resources. |
| **Policyholder protection** | In the case of insurers, an appropriate degree of policyholder protection – the impact on policyholders affected by a disruption to the service, including consideration of:<br>i. the type of product, type of policyholder, and their current or future interests.<br>ii. the significance to the policyholder of the risk insured.<br>iii. the availability of substitute products that would offer a policyholder a similar level of protection; and<br>iv. the potential for significant adverse effects on policyholders if cover were to be withdrawn or policies not honoured. |
| **Resources** | The assets or dependencies that are essential to the delivery of IBSs. These include the people, technology, data (information), facilities and third parties required to deliver IBSs. |
| **Safety and soundness**[4] | Firms having resilience against failure, now and in the future, and avoiding harm resulting from disruption to the continuity of the financial services they provide. |
| **Scenario testing**[5] | Assess the ability to remain within the ITOL for each of its IBSs in the event of a Severe but Plausible (Extreme but Plausible for FMIs) disruption of its operations. |
| **Severe but Plausible (SBP) Scenarios (or Extreme but Plausible for FMIs)** | Scenarios that would result in a high impact and significant disruption and, whilst having a low likelihood, still has a credible chance of occurrence. |
| **Vulnerability assessment** | Identification of vulnerabilities and/or weaknesses in the delivery of an IBS within ITOL through assessment of how the failure of a resource or process could impact the IBS. |

[4] The PRA's approach to banking supervision (bankofengland.co.uk)

[5] SYSC 15A.5 Scenario testing - FCA Handbook

# 2 Important Business Services

## 2.1 Overview

### Section Objectives

- To assist firms in implementing and maturing their approach to identifying their IBSs.

### Regulatory Context

The UK authorities require firms to identify their IBSs considering the risk their disruption poses (for FCA regulated firms) to consumers and market integrity, and (for PRA regulated firms) to the firm's safety and soundness, financial stability and, in the case of insurers, policy holder protection. Firms are expected to have a relatively short list of external-facing services, proportionate to the size of their business (i.e. larger firms will likely identify a larger number of IBSs than smaller firms), for which the firm has chosen to build high levels of operational resilience in anticipation of operational disruption, and against which the firm's Board and senior management can make prioritisation and investment decisions. Firms are expected to review their IBSs annually at minimum, or sooner if a significant change occurs.

The Financial Policy Committee (FPC) has also set out its expectation that relevant firms (i.e. those designated as Other Systemically Important Institutions (O-SIIs)) and FMIs should consider the vital services that are important to financial stability when identifying their IBSs. Vital services include: (1) payments, clearing and settlement of transactions; (2) deposit taking and lending; and (3) insurance and activities which support the functioning of markets. More broadly, firms and FMIs should factor in the potential impacts on the wider financial system from weaknesses in their own operational resilience and actions they might take in response to incidents as they take steps to build their resilience. These impacts can be transmitted across the financial system through the following transmission channels:

- **Operational contagion.** Occurs when an initial operational disruption causes further operational disruption elsewhere in the financial system or in the real economy. An operational outage affecting the services of a firm or FMI could leave them unable to transact with other firms or participate in financial markets. This will have knock-on impacts to the ability of the disrupted firm's or FMI's counterparties to undertake their own activities. Operational contagion could also spread beyond the financial sector and lead to disruption in the real economy if households and businesses are prevented from transacting.

- **Financial contagion.** Occurs when operational disruption leads to financial impacts. This could happen if an operational disruption impacts liquidity flows.

- **Loss of confidence.** Can be a key point of transmission across the financial system. Operational disruption can lead to a loss of confidence if the incident causes a firm's or FMI's counterparties or customers to revise their view of the riskiness of the institution, or the institution's ability to manage its risks and the risks to its business model. The possibility that an unaffected firm or FMI could be vulnerable to the same operational disruption, or cyber-attack, that impacted another firm or FMI could trigger a loss of confidence across the financial system. This could lead to run behaviour at otherwise healthy firms or mean that firms reduce their risk appetite and become reluctant to extend liquidity or credit. Even if an individual institution is not considered systemic, if a risk is perceived to be common among similar institutions, the collective impact could pose a systemic risk.

## Guiding Principles

**P.1 A business service must have a clearly identifiable user external to the firm which allows for the identification of both distinct services and "instances" of such services where needed.**

- This is to ensure an understanding of the specific intolerable harm caused to the external end-user (direct and indirect) if the business service was disrupted.
- End users may include retail customers, business customers, other legal entities, trustees, market participants, the supervisory authorities, or other members of a regulated entity's group.

**P.2 Internal services that are fundamental to the provision of the business service should also be captured through mapping and tested.**

- It is important to understand the context of failure from an external perspective. Internal shared services may underpin many external facing business services and therefore should be included within the context of the business service as many times as required.

**P.3 Business services can be distinguished from supporting services or capabilities if they could be considered as providing value to an external end-user on a stand-alone basis. Additionally, if a service has no external end-user value on its own, then it is part of another business service.**

- If a service cannot be offered to an external end-user without having to consume another service at the same time, then the articulation may be too low level. This avoids introducing internal or shared services to the top-level business service list, but also prevents activities, or stages within a business service such as 'Know Your Customer / Client' (KYC) being called out separately.

**P.4 Business services should be described in a way that is agnostic of the means of accessing the business service.**

- Business service requirements should remain constant. However, the channel used to access those business services will change depending upon market trends. Firms with single-channel business services will have different requirements for those business services which can be delivered through multiple channels. By focusing on a specific channel, the validity of multi-channel resilience may not be challenged sufficiently (e.g., access to cash vs. branch cash withdrawal).

**P.5 For a business service to be valid, the firm must be responsible for the provision of the service delivery or have outsourced it to another party on behalf of the firm. If there are any activities in which the firm acts only as an introducer, broker, or intermediary, regardless of the branding of the service, then the activity does not need to be included as a business service. This will reflect the contractual relationship between customer and providing entity.**

- This will avoid a firm taking accountability for a service wholly owned by another entity. It could be that the service in question forms a business service for another firm (e.g., an insurance provider's product offered through a retail bank).

**P.6 A business service should provide a standalone and singular outcome to the external end user.**

- To assess if a business service is 'important', a harm assessment relating to the disruption of that service needs to be established. If two or more outcomes relate to the business service then the calibration and profiling of the harm assessment becomes overly complex / burdensome, and likely impractical.

**P.7 The granularity of contractual relationships should be considered when defining business services.**

- Contractual relationship can be used to define engagement models that exist between the firm and its external third parties. Business services also model this engagement, and so the contractual landscape is a useful reference point for establishing the granularity of business services. Typically, a business service will not relate to two or more contractual relationships.

**P.8 There should be a proportionate number of Important Group Business Services (IGBS).**

- To ensure a group level view of operational resilience, IGBSs should also be identified for PRA-regulated firms subject to capital requirement regulations (CRR). This covers services in other entities within the group which could transmit risk directly to the safety and soundness of the firm.

## 2.2 Phased approach for identification of Important Business Services

| Stage | Activities | Output |
|---|---|---|
| **1. Information Gathering** | • Obtain existing list of Critical Functions / Critical Economic Functions and Core Business Lines – if available / applicable.<br>• Where these do not exist, use existing product / service catalogues or relevant product / service taxonomy. | • Set of critical functions and/or product / service catalogues to drive business service selections. |
| **2. Identify Business Services** | • Using the information gathered from stage 1 along with the industry principles, engage with appropriate stakeholders to identify business services.<br>• Discuss selections at industry level, if possible, to ensure consistency and appropriate levelling. | • Long list of business services. |
| **3. Determine Importance** | • Define criteria for assessing importance of the service based on the intolerable harm to consumers and/or risk to market integrity, financial stability, safety and soundness and, if applicable, policy holder protection.<br>• Leverage the industry principles; criteria used should be firm specific.<br>• Use assessment criteria to identify IBSs.<br>• Define group IBSs where these exist[6].<br>• Obtain internal sign off from relevant stakeholders on the understanding that the selections made are subject to change. | • Short list of IBSs with demonstrable supporting evidence and rationale for the selections made. |

[6] To establish the IGBSs, the following conceptual steps are suggested:

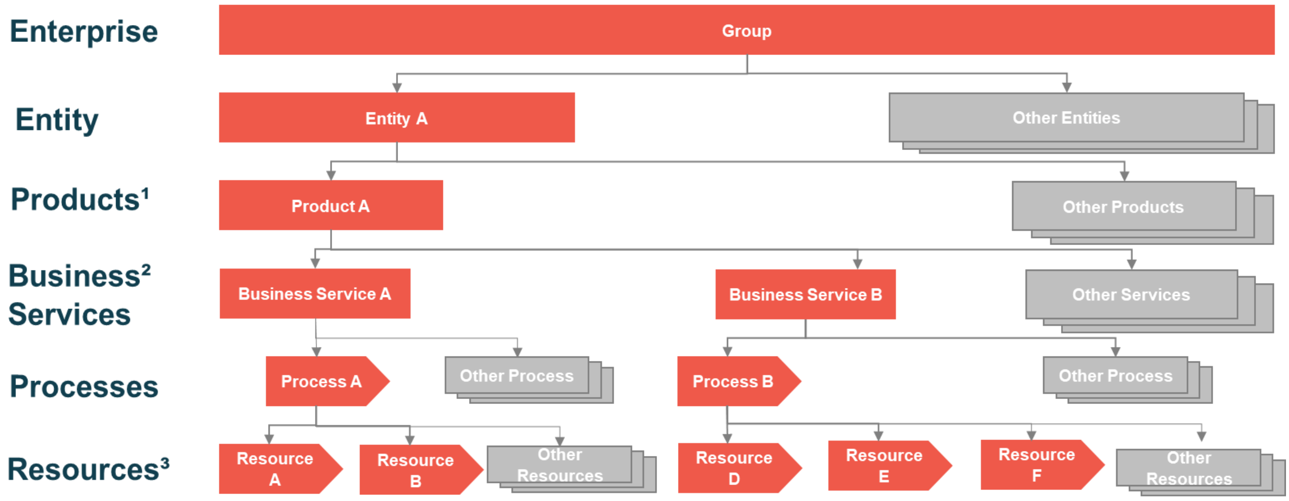
- For the institution's CRR entity / entities authorised by the PRA, establish the applicable UK Holding Company if such exists.
- If a UK Holding Company exists, all the firms that provide Business Services under that Holding Company must be established.
- For each of these firms, excluding the CRR(s), the external services offered need to be assessed to determine if they - the service - could either, 1. Impact the safety and soundness of the CRR firm(s) or 2. Impact UK Financial stability.
- If a service can impact 1. or 2. above, then it is an IGBS.

| | | |
|---|---|---|
| **4. Assign Ownership** | - Define IBS (and IGBS) ownership model / owners. | - Business service owners and ownership model / responsibilities matrix. |
| **5. Govern and Iterate** | - Ongoing governance and assessment of operational resilience including Board approval and related senior management oversight.<br>- Selections are subject to change based on changes to guidance / principles, changes to business models, outputs from process mapping / changes to dependencies, setting ITOLs, scenario testing, self-assessment, etc. | - Governance activities defined and embedded in the firm to support of the approval of the self-assessment which includes, inter alia, IBS, ITOL, and lessons learned documentation. |

## 2.3 Visualising the service relationship with processes and resources

Firms are expected to develop their own methodology and assumptions for identifying IBSs. that best fits their business. **Figure 2** provides one illustrative example of the basic relationship between products provided to external users and related services, processes and resources. There are other illustrative examples not shown here, including ones which could show business services across entities and/or products.

*Figure 2. Service Relationship*



1. For simplicity, certain nodes within this schematic have been consolidated; these are shown in grey.
2. A product, provided to a consumer / client / counterparty, will generally consist of constituent business services with some being defined as 'important' and others not due to their ability to cause intolerable harm to: consumers, market integrity, the firm's safety and soundness, policyholder protection, or financial stability of the UK financial system.
3. It is possible and acceptable that a specific business service could support multiple products (e.g., "client balance enquiry" could support multiple product offerings).
4. A resource can support multiple processes.

## 2.4 Defining Important Business Services

### Assessing whether a business service is 'important'

There is no single correct answer to what is important – firms must be able to justify the criteria, metrics, and thresholds for determining importance and be prepared to continuously iterate and refine their selection. Defining a maximum period for the disruption of the business service is one mechanism that firms can use to ensure focus on the business services that are most important although there should be evidential justification for such an approach. It should be noted the related harm assessment should not be restricted to such a period, as harm can often lag the disruption event. The approach adopted should be consistent across the firm.

Firms must consider a proportionate response – ensuring that they consider their significance to customers and markets. Flexibility and iteration are required as the understanding of services increases and the customer base, markets, and firms themselves change. The IBS taxonomy should be proportionate to the size, scale and complexity of the firm.

For a business service to be identified as an IBS, it is expected, if disrupted, to cause material detriment to:

- **Consumers.** Where the outcome of disruption passes significant inconvenience and harm and reaches an intolerable threshold, and is detrimental to one or more of the following:
    i. Physically or emotionally: disrupts access to basic needs (e.g., food, utilities, transport, shelter);
    ii. Financially: loss of income / earnings, charges incurred, loss of opportunity, settlement of debt, disruption of supply; and
    iii. Impact to vulnerable consumers.

- **Market Integrity.** Where the outcome of disruption detrimentally affects:
    i. Another organisation's ability to function normally;
    ii. The consumers of other organisations; and
    iii. Confidence in the financial system.

- **Firm Safety and Soundness.** Where the outcome of a disruption could lead to an impact on the safety and soundness of the firm including:
    i. Impact to capital or liquidity;
    ii. Inability to manage financial risks effectively;
    iii. Run on the financial institution;
    iv. Extreme regulatory censure or legal action (e.g., financial institution to lose its financial institution licence or receive material financial penalty);
    v. Firm reputational impacts; and
    vi. Sensitivity of the data - confidentiality, integrity, or availability.

- **Policyholder Protection.** In the case of insurers (as defined as being a relevant Solvency II firm), an appropriate degree of policyholder protection – the impact on policyholders affected by a disruption to the service, including consideration of:
    i. the type of product, type of policyholder, and their current or future interests;

ii. the significance to the policyholder of the risk insured;

iii. the availability of substitute products that offer a policyholder a similar level of protection; and

iv. the potential for significant adverse effects on policyholders if cover were to be withdrawn or policies not honoured.

- **Financial Stability.** Where the outcome of a disruption could lead to a systemic outcome that affects economic stability in a country or region, including:

  i. General loss of confidence in the financial system and the potential to inhibit the functioning of the wider financial sector and economy; and

  ii. Potential to cause knock-on effects for counterparties, particularly those that provide financial market infrastructure (FMI) or critical national infrastructure (CNI).

## Service substitutability

Substitutability of service should not be used in isolation to determine whether a business service is, or is not, an IBS, instead substitutability needs to be considered in a wider context, as defined by the FCA and PRA.

### FCA

The factors that a firm should consider when identifying its IBSs in relation to intolerable harm to consumer or market participants are set out in FCA SYSC 15A.2.4[7]. There are thirteen factors set out, and the ability of clients to obtain the service from other providers (substitutability, availability, and accessibility) is one factor of consideration. Firms should note that specifically:

- SYSC 15A.2.4 sets out the factors that a firm should consider when identifying its IBS. An IBS should not be excluded by just considering one factor of substitutability. No one factor in the 13 set out in SYSC 15A 2.4 has greater weight than another, therefore substitutability does not outweigh other factors on its own when identifying an IBS.
- A service should be considered an IBS if a disruption to it could cause intolerable levels of harm to its customers, even if the service is substitutable.
- Firms should consider a particular service as an IBS if they cannot be easily substituted in the market.

### PRA

The factors that firms should consider when identifying their IBSs including where a disruption of the service threatens policyholder protection, the safety and soundness of individual firms, or financial stability, are set out in SS1/21[8], paragraph 2.5.

- In the case of policyholder protection, the availability of substitute products that would offer a policyholder a similar level of protection is one factor of consideration. Firms should consider all the factors set out in SS1/21 paragraph 2.5 (c).
- In the case of firm safety and soundness or financial stability, substitutability cannot be used to justify exclusion of an IBS or as a consideration when setting ITOLs. PS6/21[9] makes it clear that if a firm's

[7] SYSC 15A.2 Operational resilience requirements - FCA Handbook

[8] SS1/21 Operational resilience: Impact tolerances for important business services | Bank of England

[9] PS6/21 | CP29/19 | DP1/18 Operational Resilience: Impact tolerances for important business services | Bank of England

provision of a service is not substitutable, this may increase the criticality of this service to financial stability. However, this does not imply that substitutability can justify exclusion of an IBS.

- Firms should not assume that other providers will step in to provide an IBS when identifying IBSs and setting ITOLs. The PRA expects firms to consider the impacts of disruption before they are mitigated.
- Identifying a lack of substitutability from other market providers will be an important consideration for those firms required to consider financial stability, when identifying IBSs and setting ITOLs.

Firms should consider substitution as an effective mitigation strategy as part of scenario testing. Specifically, where firms have the capability to provide similar service using alternative means or channels:

- Where substitution is available, these procedures should be evaluated as effective mitigation to remain within ITOL during SBP scenario testing. If a firm can prove effective substitutability during testing, it will help to make them more resilient; and
- Firms should also consider developing and testing alternative mitigating actions where substitution may not be possible, such as disruptions to critical third parties (CTPs) or FMI, or where other market participants are likely to be disrupted simultaneously.

## 2.5 Governance, accountability and management of an Important Business Service

The PRA expects Capital Requirements Regulation (CRR) consolidation entities (in the case of UK banking groups) or an insurer (in the case of UK insurance groups) to identify a proportionate number of IBSs and Important Group Business Services (IGBSs) and respective ITOLs at the level of the group. IGBSs are business services that if disrupted, pose a risk to:

- (For CRR consolidation entities) the safety and soundness of any CRR firm in the CRR consolidation entity's consolidation group or, where relevant, UK financial stability;
- (For insurers) the firm's safety and soundness, policyholder protection or, where relevant, UK financial stability; or
- Taking a group level view of operational resilience ensures that risks arising in parts of the group that are not subject to the individual requirements are considered.

IBSs should each have an accountable owner, at a senior level, within the organisation.

- The accountable business area is responsible for the resilience of their services and must have a holistic view of end-to-end resilience capabilities and risks, so that the IBSs can remain within their ITOL. Additionally, depending on the size, scale and complexity of the firm, individuals within Operations and Technology should be defined as accountable at the IBS level.

Organisations must be clear on the responsibility and accountability for mapping, testing, and addressing identified vulnerabilities and self-assessment of each IBS.

- Complex, siloed delivery models can lead to gaps in understanding the resilience of business services. Understanding the detail of who is accountable and responsible for ensuring business services are resilient reduces the likelihood of gaps. Nominating a single accountable owner may be an optimal way of meeting this principle.

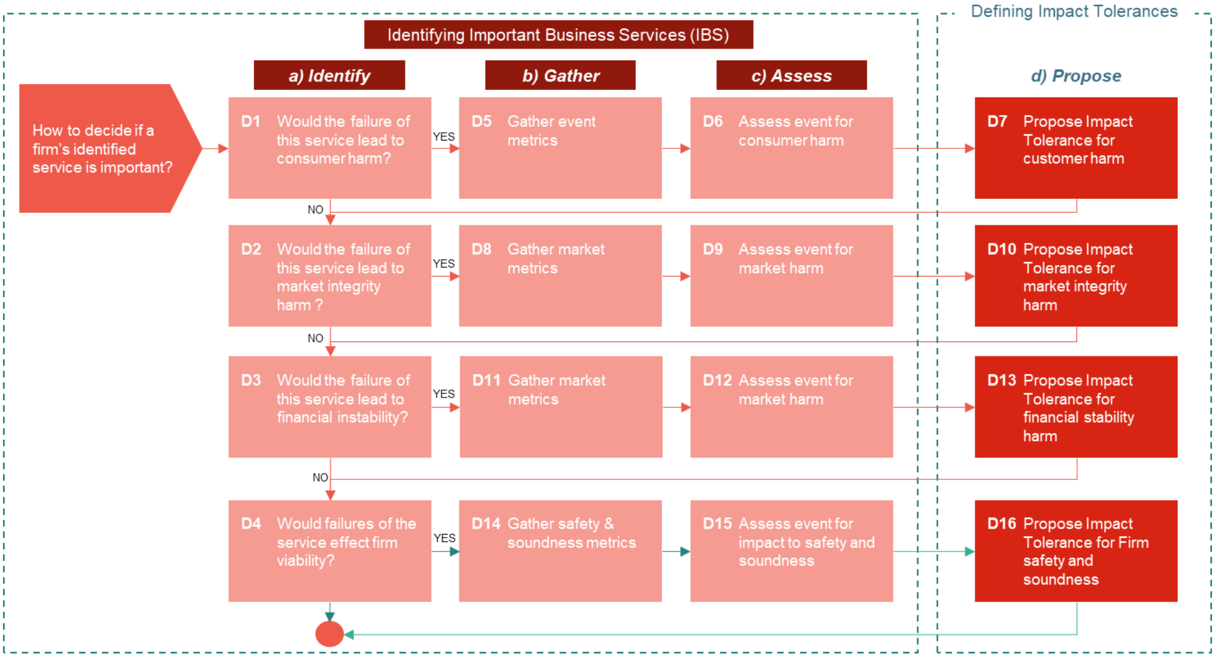
An organisation's IBSs should be reviewed at a minimum on an annual basis, or as soon as practical, upon identification of a material change that has occurred, and approved by the organisation's Board or governing forum. Material change should be clearly defined by the firm using quantitative and qualitative metrics.

- Firms, markets, and the operating environment (including threats) are constantly evolving. This means that the importance of existing services may alter (higher or lower), or new services may be introduced.
- When there are changes to one or more of the firm's IBSs, firms should consider the implications on other elements of the operational resilience framework and processes and take steps to resolve these in a timescale proportionate to the firm. This includes any remapping, review of any scenario testing plans, whether existing vulnerabilities and remediation plans remain appropriate, etc.

## 2.6 Decision workflow for identifying Important Business Services

To support the financial services industry in identifying IBSs, a decision tree (as shown in **Figure 3**) has been constructed to support firms defining which business services are 'important'. A business service should not be excluded from being defined as important by considering one factor alone and should be determined without reference to response or recovery capabilities.

*Figure 3. Identifying an IBS*


Identifying Important Business Services (IBS)
Defining Impact Tolerances
a) Identify
b) Gather
c) Assess
d) Propose
How to decide if a firm's identified service is important?
D1 Would the failure of this service lead to consumer harm?
YES
D5 Gather event metrics
D6 Assess event for consumer harm
D7 Propose Impact Tolerance for customer harm
NO
D2 Would the failure of this service lead to market integrity harm ?
YES
D8 Gather market metrics
D9 Assess event for market harm
D10 Propose Impact Tolerance for market integrity harm
NO
D3 Would the failure of this service lead to financial instability?
YES
D11 Gather market metrics
D12 Assess event for market harm
D13 Propose Impact Tolerance for financial stability harm
NO
D4 Would failures of the service effect firm viability?
YES
D14 Gather safety & soundness metrics
D15 Assess event for impact to safety and soundness
D16 Propose Impact Tolerance for Firm safety and soundness

### Decision 1 (Consumer Harm): Would the failure of the service lead to consumer harm?

Where the outcome of disruption is detrimental to one or more of the following:

- Physically or emotionally: disrupts access to basic needs e.g., food, utilities, transport, shelter.
- Financially: significant loss of income / earnings, charges incurred, loss of opportunity, settlement of debt, disruption of supply that is irreparable.
- Vulnerable customer: impact to those vulnerable consumers (firm to define what a vulnerable consumer is and understand how the worsening of circumstances impacts them).
- Non-receipt of margins or collateral may trigger positions to be unwound, affecting a client's position, profit and loss, capital and liquidity position.

### Decision 2 (Market Integrity): Would the failure of this service lead to market integrity harm?

Where the outcome of disruption detrimentally affects:

- The effectiveness and reliability of the financial market (e.g., potential to cause market "deadlock").

- Another organisation's ability to function normally.
- General loss of confidence in the financial system.
- Impairment of cash correspondents' payment services.
- Inability to settle with clearing entities impacting market-making consumers' ability to transact and manage risk.
- Disruption affects counterparties' intra-day liquidity and ability to pay, thereby incurring significant charges or borrowing costs.

### Decision 3 (Financial Stability): Would the failure of this service lead to financial instability?

Where the outcome of a disruption could lead to an impact on the financial stability of the UK, including:

- The potential to inhibit the functioning of the wider economy, particularly the economic functions listed in SS19/13 Resolution planning.
- The potential to cause knock-on effects (e.g., contagion, amplification effect) for counterparties, particularly those that provide FMI or CNI.
- The potential to cause a loss of confidence in the UK financial system and trigger behavioural choices not to transact in the UK financial system or other atypical behaviour such as runs or disruptive flights to safety.
- The extent to which O-SII firms and FMIs provide vital services that are important to financial stability.
- The potential to impact on the wider financial system through one of the following transmission channels: (1) operational resilience contagion; (2) financial contagion; and (3) a loss of confidence.

### Decision 4 (Firm Safety and Soundness): Would failures of the firm affect firm viability?

Where the outcome of a disruption could lead to an impact on the safety and soundness of the firm, including:

- Impact to capital or liquidity.
- Run on the financial institution.
- Extreme regulatory censure or legal action (e.g., financial institution to lose its financial institution licence or receive material financial penalty).
- Extreme firm reputational impacts or loss of confidence in firm (e.g., adverse media coverage, analyst commentary, negative impact on share price).
- Loss of confidentiality, integrity, or availability of data.
- Disrupting the delivery of other IBSs within the firm's business, product lines or entities.

### Decision 5 (Consumer Harm): Gather event metrics

In the event of disruption to an IBS, consider the potential impact:

- High volume / low value.
- High value / low volume.
- What number of your consumers carry out this activity daily / hourly (average across a year to identify worst case scenario which considers known peak periods); how many of those are vulnerable (known).

- Peak Time Analysis that determines when the service experiences higher than usual demands – e.g. tax year end.
- What is the proportion of your consumers who carry out this event hourly / daily?
- Do you have any historical incident, or consumer complaint information that supports an assessment of consumer behaviour during disruption?
- Are you the only provider in market?
- Is the consumer 'tied in' at any point in the process?
- Is there any personal, sensitive, or commercial data involved?

### Decision 8 (Market Integrity): Gather market metrics

- Are you a major provider in the UK market? (using market share MI if available)
- Are you a systemically important financial institution (SIFI) in the UK (e.g., an Otherwise Systemically Important Institution (O-SII) or a Domestic Systemically Important Bank (D-SIB))?
- Do you provide a vital service to the UK financial system? (Provision of payment and settlement services; intermediating between savers and borrowers; or insuring against and dispersing risk)?
- Would other organisations be able to bear the increased load in the short and long term?
- Would failure cause a general loss of confidence in the financial institution system?

### Decision 11 (Financial Stability): Gather market metrics

Gather market metrics:

- Are you a major provider in the market?
- Would other organisations be able to bear the increased load in the short and long term?
- The size and nature of risks associated with the business service

### Decision 14 (Firm Safety and Soundness): Gather safety and soundness metrics

Gather safety and soundness metrics:

- Capital and liquidity information from recovery and resolution planning / ICAAP scenarios.
- Regulatory fines that would be incurred.
- Legal recourse for prolonged service disruption.
- Reputational impact (scorecards, brand tracking, review aggregation metrics).

### Decision 6/9/12/15: Assess event impacts

Review the gathered metrics (D5/8/11/14) against time periods to support understanding when intolerable harm begins to occur.

### Decision 7/10/13/16: Propose ITOLs (see Section 3)

Assume failure happens at peak volumes, assess effect on consumers (D5), market integrity (D8), financial stability (D11) and firm (D14). Agree ITOL for IBS (this will always be a judgement based on metrics and an understanding of consumer behaviour).

# 3 Impact Tolerances

## 3.1 Overview

### Section Objectives

- To assist firms in implementing and maturing their approach to setting ITOLs for each of their IBSs.

### Regulatory Context

The UK authorities require firms set an ITOL for each of their IBSs (against each of the FCA and PRA regulatory objectives), measured by a length of time in addition to any other relevant metrics, and at the point at which any further disruption to the IBS would pose a risk (for FCA regulated firms) to consumers and market integrity, and (for PRA regulated firms) to the firm's safety and soundness, financial stability and, in the case of insurers, policy holder protection. ITOLs should be set on the assumption that a disruption will occur and should apply at peak times as well as in normal circumstances.

The UK authorities require firms to use a time-based metric for all ITOLs, using these in conjunction with other metrics where appropriate (e.g., with a volume and/or value metric).

### Guiding Principles

P.1 **Firms should articulate their ITOLs in a clear, unambiguous, and easily consumable way; describing the maximum tolerable level of disruption in terms of various metrics including, as a minimum, a period of time (either a duration such as 24 hours, or a point in time such as 2pm the next business day after disruption).**

P.2 **For each IBS, firms should provide clear rationale for when intolerable consumer harm is reached, or a risk to market integrity, the firm's safety and soundness, financial stability and, in the case of insurers, policy holder protection would materialise.**

P.3 **For each regulatory objective, the firm should identify all the different types of impacts that could arise if the IBS is disrupted (e.g., value or number of transactions disrupted, lost revenue, and number of vulnerable customers affected).**

P.4 **Thresholds for intolerable harm should be set for each type of impact. Related data (empirical and theoretic) is then employed to assess how quickly intolerable harm manifests for each impact type. The ITOL time metric should not exceed the shortest of these durations.**

P.5 **Where a firm has opted not to consider a regulatory objective when setting an ITOL, they should be able to provide assurance that sustained disruption to the IBS will not impact that objective.**

P.6 **Assumptions used to define the ITOL statement should be transparent in the review / approval process.**

P.7 **ITOLs should not be confused with Recovery Time Objectives (RTO); the former is set in the context of intolerable harm whereas the latter is set according to the risk appetite of the firm. Given RTOs are objectives, they should be set before the ITOL to ensure the goal is to recover before breaching the ITOL.**

P.8 **Impact tolerances differ from risk appetite in that they assume a particular risk has crystallised instead of focusing on the likelihood and impact of operational risks occurring.**

P.9 **The disruption analysis is cause-agnostic but should be set at the worst possible time / context in terms of impact.**

P.10 **When assessing harm, the level of harm can accumulate at different rates for the firm, consumers and market. Consideration should be given to the ways in which they are interconnected (e.g., customers being impacted will inevitably have an impact on the firm's safety and soundness).**

## 3.2 Setting an Impact Tolerance

### Overview

ITOLs are set at the point at which any further disruption to an IBS would pose a risk (for FCA regulated firms) to consumers and market integrity, and (for PRA regulated firms) to the firm's safety and soundness, financial stability and, in the case of insurers, policy holder protection (collectively the "Regulatory Objectives"). ITOLs should be measurable in a way that supports the ability of a firm to test its capability to remain within the ITOL thresholds in SBP scenarios.

ITOLs are used in the event of a disruption to an IBS and are used to ensure that the firm does not exceed the tolerance defined in the ITOL and result in intolerable harm against any of the Regulatory Objectives. This is achieved by either complete recovery of the service or utilisation of mitigating action (e.g., workarounds, service substitution). They are also used to drive investment in detective, preventative, response, and recovery strategies.

## 3.3 Impact Tolerance metrics

Firms should identify the appropriate thresholds for causing harm or the potential to threaten the harm criteria. Metrics that describe the accumulation of harm can be used to derive the time-based metric. These are specific to the IBS and can consider characteristics of the service they describe. Such metrics can include things such as:

- types of consumers
- values and volumes of transactions or consumers
- types of transactions
- criticality of transactions
- impact or dependency for other IBSs
- estimated losses

Once the thresholds are understood, consideration of worst-case scenario should be thought through to understand how harm would accumulate up to and beyond the threshold. The time-based metric can be derived from this (e.g., from a firm perspective, if the threshold for financial loss is £200m, and in the worst case the firm would lose £50m a day if the IBS was disrupted, the time-base threshold would be four business days).

## 3.4 The difference between risk appetite and impact tolerances

As detailed in the PRA's Statement of Policy 'Operational resilience'; "Impact tolerances differ from risk appetites in that they assume a particular risk has crystallised, instead of focusing on the likelihood and impact of operational risks occurring. Firms that are able to remain within their ITOLs increase their capability to survive SBP disruptions, but risk appetites are likely to be exceeded in these scenarios" (see **Figure 4**).

*Figure 4. The relationship between risk appetite and ITOL*

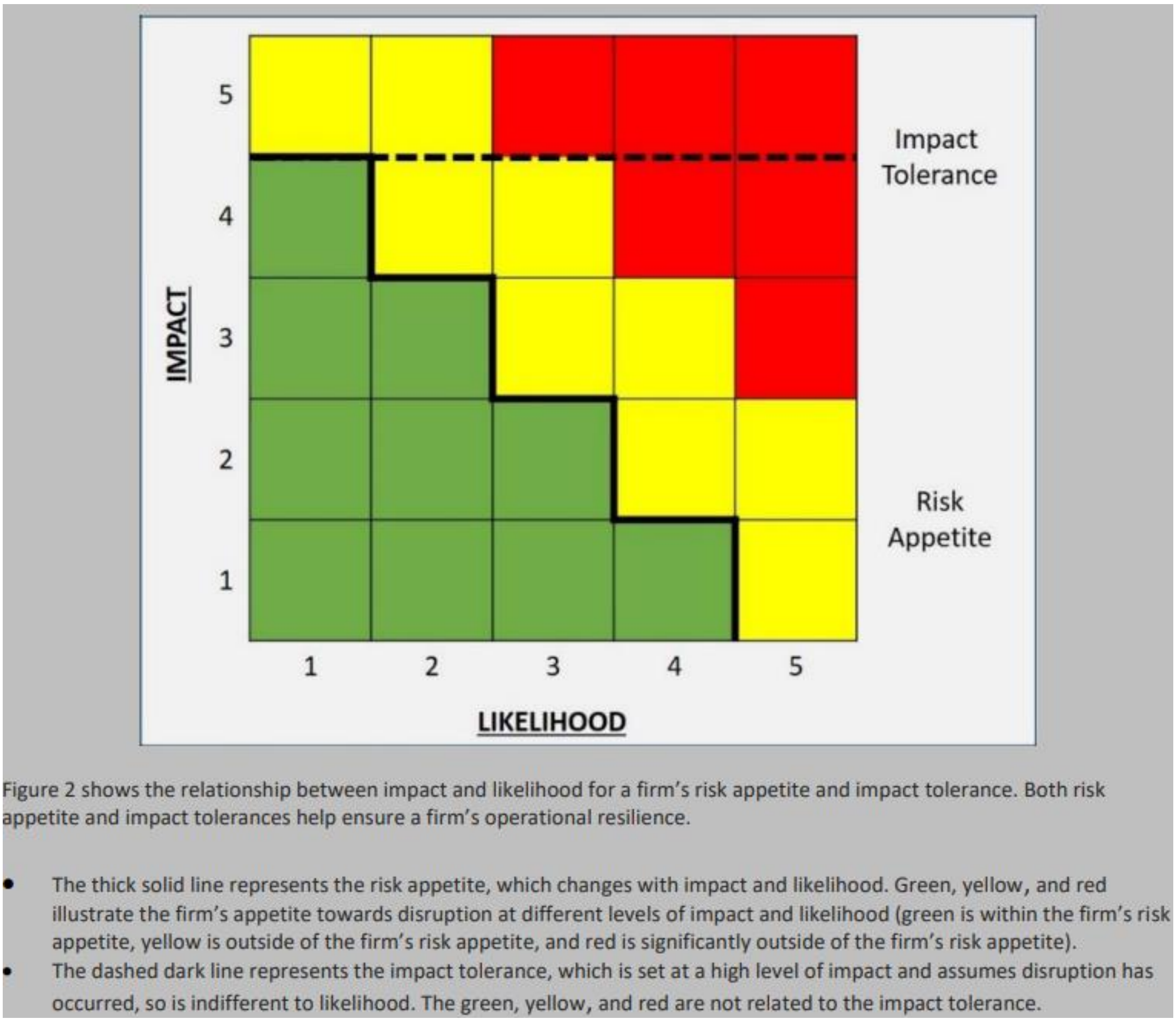


Figure 2 shows the relationship between impact and likelihood for a firm's risk appetite and impact tolerance. Both risk appetite and impact tolerances help ensure a firm's operational resilience.

- The thick solid line represents the risk appetite, which changes with impact and likelihood. Green, yellow, and red illustrate the firm's appetite towards disruption at different levels of impact and likelihood (green is within the firm's risk appetite, yellow is outside of the firm's risk appetite, and red is significantly outside of the firm's risk appetite).
- The dashed dark line represents the impact tolerance, which is set at a high level of impact and assumes disruption has occurred, so is indifferent to likelihood. The green, yellow, and red are not related to the impact tolerance.

## 3.5 Impact Tolerance statement

An ITOL statement can be used to support an ITOL and ensure the specifics of intolerable harm are clearly defined in a statement for an IBS. This should be a living and breathing statement, formally reviewed and approved at least annually, or as soon as practical, upon the identification of a material change to the IBS, the firm, or its environment. Material change should be clearly defined by the firm using quantitative and qualitative metrics.

### Principles for setting Impact Tolerance statements

P.1 **The ITOL indicates a certain period, or point in time, a particular IBS should not be disrupted beyond, plus any other relevant non-timed based metrics. The ITOL statement is defined to clearly outline the specific conditions aligned to the harm factors / regulatory objectives**

P.2 **The ITOL statement consists of one or two sentences that offer a clear and simple explanation of what the ITOL is per IBS.**

P.3 **An ITOL statement is defined per harm factors (i.e., financial market integrity, consumer harm, firm safety and soundness, or stability of the UK financial system) if there are different tolerances, but with the shortest time metric ITOL being the leading indicator.**

**P.4 The ITOL statement is scenario agnostic and does not factor in potential mitigating actions, including substitutability in the firm or market.**

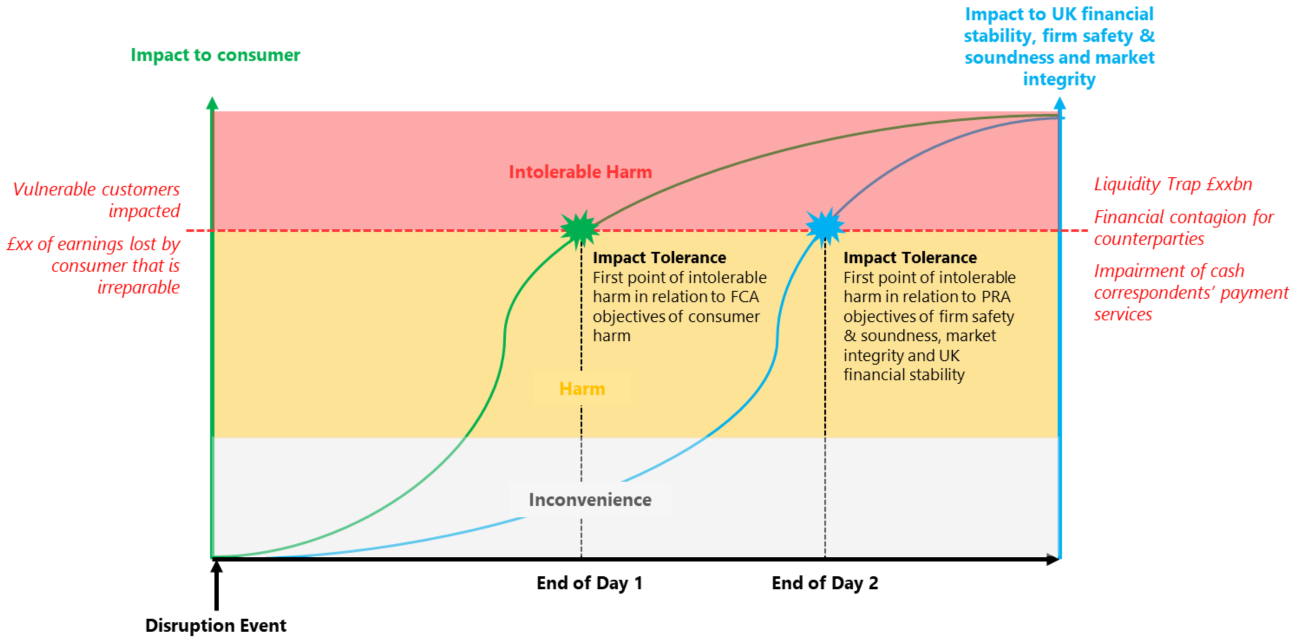
**P.5 The ITOL considers the worst possible time for a disruption when setting the tolerance and it accounts for a demand fluctuation for the IBS within the market.**

**P.6 An ITOL statement should be established according to quantifiable metrics that characterise intolerable harm across the themes of consumers, market integrity, safety and soundness / policyholder protection, and financial stability. The duration of an ITOL is set at the point where intolerable harm first occurs and based on the gross impact of an IBS disruption. Dual regulated firms should identify separate ITOLs for their IBS where the delivery of that service is relevant to both PRA and FCA objectives.**

## 3.6 Impact Tolerance examples

**Figure 5** shows how a disruption event can unfold over time for impact types relating to a) consumer harm and b) financial stability.

*Figure 5. Identifying where intolerable harm unfolds*


Impact to consumer
Impact to UK financial stability, firm safety & soundness and market integrity
Vulnerable customers impacted
£xx of earnings lost by consumer that is irreparable
Intolerable Harm
Impact Tolerance
First point of intolerable harm in relation to FCA objectives of consumer harm
Impact Tolerance
First point of intolerable harm in relation to PRA objectives of firm safety & soundness, market integrity and UK financial stability
Liquidity Trap £xxbn
Financial contagion for counterparties
Impairment of cash correspondents' payment services
Harm
Inconvenience
End of Day 1
End of Day 2
Disruption Event

# 4 Mapping

## 4.1 Overview

### Section Objectives

- To assist firms in implementing and maturing their approach to the identification and documentation of the necessary resources (people, processes, technology, facilities, and information) required to deliver each of their IBS. This identification process is referred to as 'mapping'.

### Regulatory Context

The UK authorities require firms to identify and document, through 'mapping', the necessary people, processes, technology, facilities, and information (the 'resources') required to deliver each of their IBSs. For this, firms are expected to complete mapping to a level of detail necessary for them to identify vulnerabilities and test their ability to remain within ITOLs. Mapping must be updated annually at a minimum, or following significant changes to the firm's business, IBSs, or associated ITOLs.

The UK authorities require firms to complete mapping irrespective of whether the resources are being provided wholly or in part by a third party (which may be an intragroup or external provider). Where a firm relies on a third party for the delivery of an IBS, the UK authorities expect them to understand how their outsourcing and third-party dependencies support their IBSs, with an expectation on firms to obtain assurance (as set out in SS2/21 'Outsourcing and third party risk management') from their third parties through the lifecycle of an outsourcing or other third-party arrangement. This includes any reliance placed on sub-outsourcing arrangements in the provision of the firm's IBSs.

The following guidance has been provided by the FCA (PS21/3) for each of the resource types:

- **People –** People that support the provision of the IBS. Firms need to understand which people are responsible for processes, technology and implementing and monitoring controls. As well as understanding overall senior management accountability, this could include individuals responsible for specific capabilities, the size and strength of their teams, training / education and wider organisational people challenges such as HR controls, employee attrition, hiring practices and key personnel succession planning.
- **Processes –** A process is a structured set of activities designed to produce a specific output. The ability to define what processes are responsible for delivering outputs in an organisation is a key element of an organisation's approach to technology.
- **Technology –** Underlying systems and architecture to support the provision of the service.
- **Facilities –** Office locations, printing facilities, mailing, credit card production / statements / client communications.
- **Information –** Any data, feeds or material that is required by a firm to deliver a service.

### Guiding Principles

P.1 **Firms must identify and document the necessary people, processes, technology, facilities and information (the 'resources') required to deliver each of their IBSs. This includes any relationships with third parties which could impact the firm's ability to remain within their ITOLs.**

**P.2 Firms should develop their own methodology and assumptions for mapping that best fit their business, whilst ensuring that a consistent approach is taken to mapping across all IBSs and resource types.**

**P.3 Mapping should be completed to a level of detail necessary for firms to identify vulnerabilities and test their ability to remain within ITOL. In doing so, firms should identify the resources that are critical to delivering an IBS, ascertain whether they are fit for purpose, and consider what would happen if resources were to become unavailable.**

**P.4 Mapping should be accessible and usable for the firm and documented in a way that is proportionate to the firm's size, scale, and complexity.**

**P.5 Firms should update their mapping annually at a minimum, or following significant changes to the firm's business, IBSs or associated ITOLs.**

**P.6 Mapping should mature over time to enable the firm to fully understand all the dependencies and interconnectivity required to deliver their IBSs.**

**P.7 Firms should complete their mapping using 'golden sources' (master data sources), as far as possible.**

**Where a firm relies on a third party for the delivery of an IBS:**

**P.8 Mapping must be completed irrespective of whether the resources are provided wholly or in part by a third party (which may be an intragroup or external provider). If a third-party provider supplying an IBS to a firm fails to remain within ITOL, that failure is the ultimate responsibility of the firm.**

**P.9 Mapping should be completed to a level of granularity which enables the firm to understand potential vulnerabilities, whether they sit with the third party or beyond (including any reliance placed on sub-outsourcing arrangements). Detailed mapping of third- and nth-party relationships should allow firms to quickly understand exposure and take mitigating actions to manage the impact in the event of disruption. Mapping of nth parties should therefore be considered, unless other assurance mechanisms are effective and more proportionate.**

## 4.2 Mapping the resources required to deliver Important Business Services

### Mapping resources

| Stage | Activities | Output |
|---|---|---|
| **1. Scoping** | • Once IBSs have been identified and ITOLs set, use the IBS maps to identify the critical activities that underpin them.<br>• Map the processes required to deliver the critical activities, drawing from existing mapping where possible. | • Process maps for critical activities. |
| **2. Mapping** | • Identify the resources that deliver and support IBSs. | • For each IBS, list the resources that support it, linked to the processes identified in stage 1. |

| | | |
|---|---|---|
| | • The above resources fall into the resilience pillars, but further granularity may be desirable depending on a firm's complexity.<br>• Assess the criticality of each resource at each step (e.g., could the unavailability of the resource yield a breach of ITOL?). | |

Mapping starts by identifying the end-to-end processes that are critical for the delivery of an IBS. As per Principle 7, firms must draw information from master systems and existing tools, where possible (these will be useful in establishing the link between processes and resources). When extracting this information, it may be useful to ask if a resource is critical to the delivery, protection, or recovery of an IBS, even though this is not required by the authorities. Once this initial analysis is undertaken, manual analysis will then require establishing which resources are critical to IBSs, and whether any other critical resources have been missed out by the initial analysis. These activities may be led by operational resilience specialists but will require input and ratification from subject matter experts (SMEs) and the relevant business areas.

### Assessing criticality of mapped resources to delivery of the IBS

A very simple, high-level map may be created as per the template shown below. This type of map would help highlight resources that are critical to multiple IBSs, IBSs without certain pillars mapped to them (which is not necessarily a problem e.g., a cloud-based service might run without any facilities mapped), and IBSs without recovery resources mapped to them.

| Pillar | Resource | Classification | IBS1 | IBS2 | IBS3 |
|---|---|---|---|---|---|
| **People** | Team A | Delivery | ✓ | ✓ | |
| **People** | Team B | Delivery | | | ✓ |
| **Facilities** | Building 1 | Delivery | ✓ | ✓ | ✓ |
| **Facilities** | Building 2 | Delivery | ✓ | | |
| **Third Parties** | Third Party A | Delivery | ✓ | ✓ | |
| **Third Parties** | Third Party B | Recovery | ✓ | | |
| **Technology** | App 1 | Delivery | ✓ | ✓ | ✓ |
| **Technology** | App 2 | Delivery | | ✓ | |
| **Technology** | App 3 | Recovery | ✓ | | ✓ |
| **Technology** | App 4 | Recovery | ✓ | ✓ | ✓ |

### Creating IBS maps

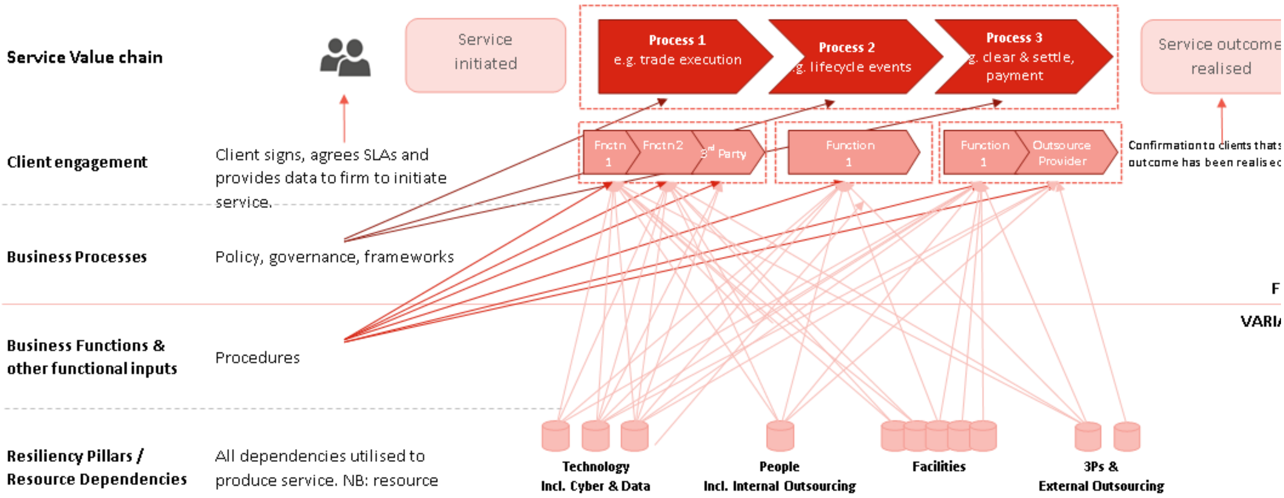
More comprehensive IBS maps can be created to demonstrate the range of resource dependencies and relationships. It may be useful to share these maps with support areas, (e.g., technology) so that they can map infrastructure in support of the business dependencies that are managed by them. This is to ensure prioritised recovery of critical resources in the face of material disruption. This is important, because the recovery order of critical systems that underpin an IBS is key to meeting tolerance thresholds. The map may also be used to demonstrate supporting activities that feed into the delivery of the service and ensure the resource dependencies for that activity are likewise mapped.

Depending on the size and complexity of a firm, a range of mapping solutions is available, from individual, manually produced process maps (e.g., using Visio) that include dependencies, resources, and controls, to app-based versions that connect dependencies and resources. Another option is to use pictorial diagrams for the high-level chain of activities linked in a relationship database of all resource dependencies.

Variable aspects of delivering the service tend to be business functions, procedures, individual resources, and other dependencies that are more prone to change, and therefore lend themselves to being mapped in a relationship database. Firms with group structures or multiple-regulated legal entities may also want to include these entities and/or cost centres to their mapping.

Due to the potential complexity of mapping, the actual mapping of *all* the resources and dependencies for an IBS, as shown in the theoretical example below, is easier to manage using an appropriate tool, such as a database-driven application. If the tool has robust reporting and visualisation capability, this also aids the analysis and provision of mapping information to other areas, such as technology, which can then ensure appropriate prioritisation for the recovery of processes. Linking to other information such as cost centres, legal entities, and locations, can assist with modelling as part of vulnerabilities analysis and scenario testing.

*Figure 6. Mapping example*


Service Value chain
Service initiated
Process 1 e.g. trade execution
Process 2 .g. lifecycle events
Process 3 g. clear & settle, payment
Service outcome realised
Client engagement
Client signs, agrees SLAs and provides data to firm to initiate service.
Fnctn 1
Fnctn2
3rd Party
Function 1
Function 1
Outsource Provider
Confirmation to clients that outcome has been realised
Business Processes
Policy, governance, frameworks
F
VARI
Business Functions & other functional inputs
Procedures
Resiliency Pillars / Resource Dependencies
All dependencies utilised to produce service. NB: resource
Technology Incl. Cyber & Data
People Incl. Internal Outsourcing
Facilities
3Ps & External Outsourcing

## 4.3 Special considerations for mapping information / data

### Defining information

Information occurs in many forms. In the context of operational resilience, information includes all forms of structured and unstructured data critical to the provision of an IBS. Information may relate to a business process or to technology processes and services that underpin it. Further, information may be held by the firm or by third parties on behalf of the firm, and it may be point-in-time or continually updated during the provision of a service.

The difference between structured and unstructured information may be summarised as follows:

- **Structured information** is stored electronically and resides in fixed fields within a record or file. It includes data contained in applications, databases, warehouses, and data feeds. Typically, data critical to the provision of an IBS is held as structured information, as this supports a structured approach to controls, reviews, and audit.

- **Unstructured information** does not have a predefined data model or is not organised in a predefined manner. It may be stored physically or digitally, and includes data held on share drives, user tools, spreadsheets, documents such as contracts and operating procedures, emails, social media, chats, flat files, transactional messages, reports, graphics, digital images, microfiche, video recordings, and paper files. Typically, unstructured data is transient in nature and is seldom critical to the provision of IBSs.

The principles and approach outlined in this section focus primarily on structured information, thus excluding broader, less tangible aspects of information such as knowledge and skills, some of which may be best captured under the people pillar. The terms 'data' will be used to refer to structured information in this section, while 'information' will be used generically to encompass both structured and unstructured information.

### Principles for information mapping

In addition to the general resource mapping principles, the following principles have been formulated to aid information mapping (but no specific principles for the other pillars are covered by this Guidance) because of the added complexity of data / information.

P.1 **When considering what may be classed as critical data, firms should consider consumer, market / economic and firm harm caused by loss of confidentiality, integrity, and availability of that data. Whilst loss of availability and integrity are commonly used considerations as they may lead to service outages, confidentiality may also cause harm or lead to market instability.**

P.2 **Priority may be given to mapping structured data, but consideration should be given to unstructured data which may be critical to the operation or recovery of a service. The rationale for not including or including unstructured data should be included.**

P.3 **Initial mapping of data to IBS may focus on identifying the physical data stores, most commonly via the IT application. As a starting point, it may be reasonable to assume that when a critical data store is identified, all data within it is critical.**

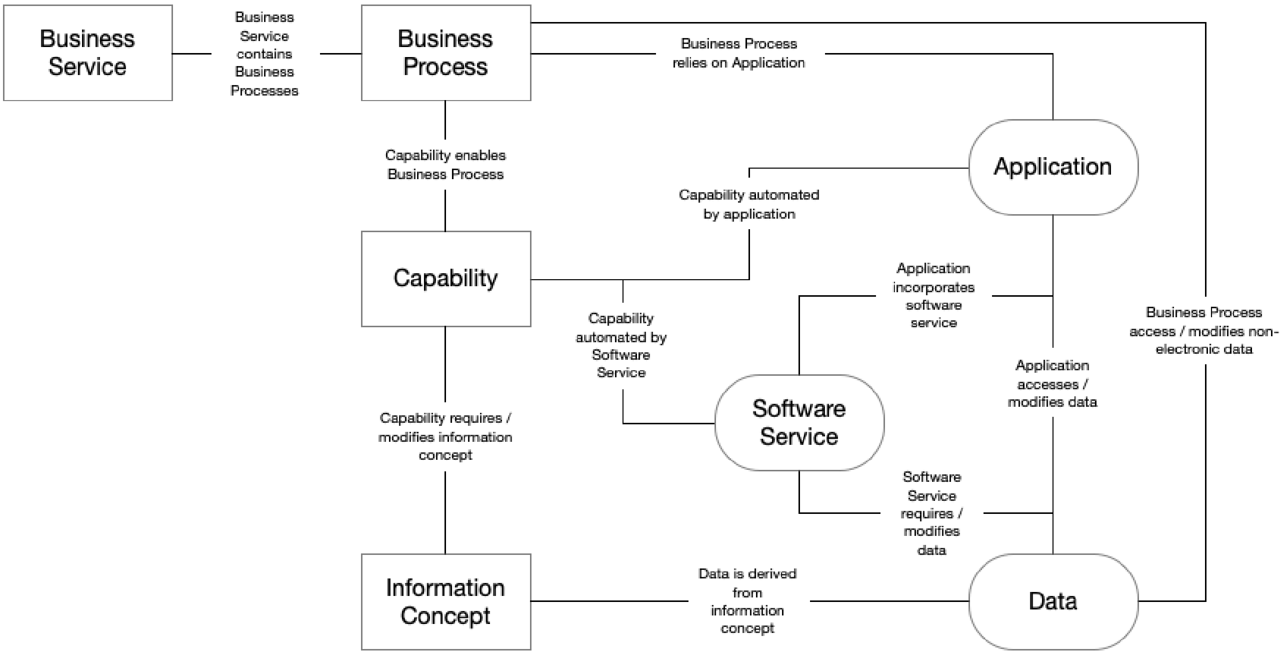
P.4 **When critical data is identified, ensure the resources (people, facilities, third parties, technology) required to maintain the data have also been identified.**

P.5 **When critical data is identified, it should be assessed initially to ensure that obvious vulnerabilities are identified (methods such as Failure Mode Effect Analysis (FMEA) or Single Point of Failure (SPOF) may be considered) to ensure adequate confidentiality, integrity, and availability in relation to the defined ITOLs for the business service.**

## Business services – Simplified data model

The model in **Figure 7** has been adapted from The Open Group Architecture Framework (TOGAF) and Business Architecture Body of Knowledge (Bizbok) to illustrate how applications can be aligned to processes and used to identify data stores.

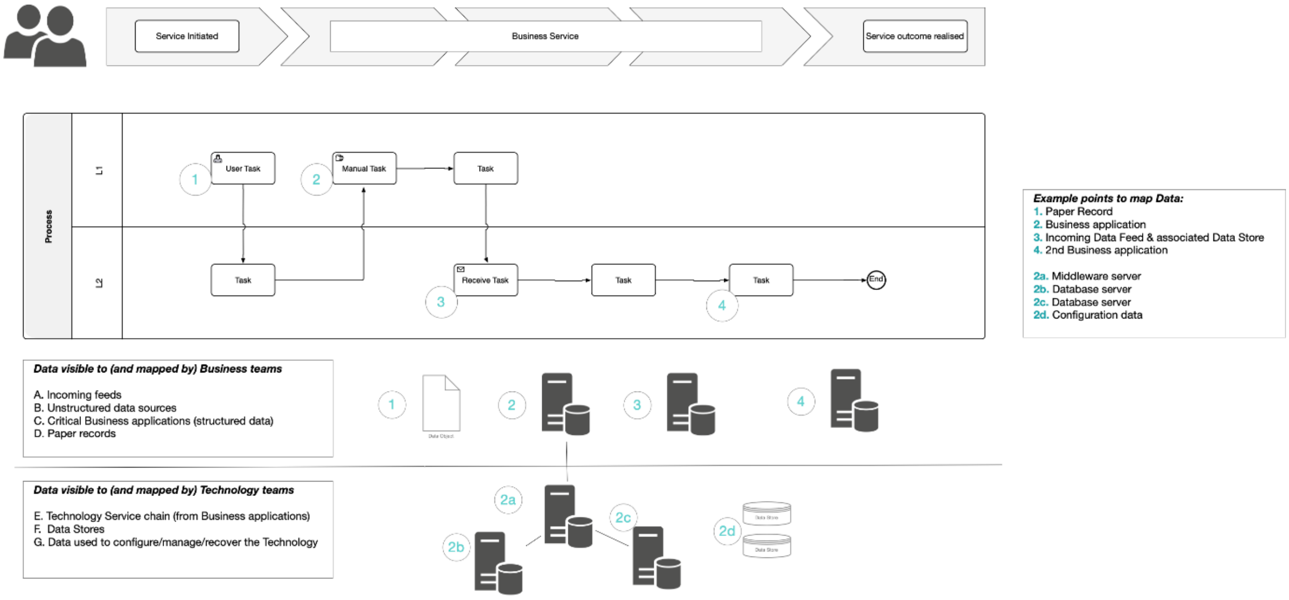
*Figure 7. Business data model*


Business Service
Business Service contains Business Processes
Business Process
Business Process relies on Application
Capability enables Business Process
Application
Capability automated by application
Capability
Application incorporates software service
Capability automated by Software Service
Business Process access / modifies non-electronic data
Application accesses / modifies data
Software Service
Capability requires / modifies information concept
Software Service requires / modifies data
Information Concept
Data is derived from information concept
Data

## Information mapping example

The process diagram in **Figure 8** is an example of data mapping against a business service.

*Figure 8. Information mapping process diagram*


Service Initiated
Business Service
Service outcome realised
Process
L1
L2
User Task
Manual Task
Task
Task
Receive Task
Task
Task
End
1
2
3
4
Example points to map Data:
1. Paper Record
2. Business application
3. Incoming Data Feed & associated Data Store
4. 2nd Business application
2a. Middleware server
2b. Database server
2c. Database server
2d. Configuration data
Data visible to (and mapped by) Business teams
A. Incoming feeds
B. Unstructured data sources
C. Critical Business applications (structured data)
D. Paper records
Data Object
Data visible to (and mapped by) Technology teams
E. Technology Service chain (from Business applications)
F. Data Stores
G. Data used to configure/manage/recover the Technology
2a
2b
2c
2d
Data Store
Data Store

# 5 Scenario testing

## 5.1 Overview

### Section Objectives

- To assist firms in implementing and maturing their approach to scenario testing.

### Regulatory Context

The UK authorities require that firms regularly test their ability to remain within ITOL in SBP disruption scenarios (across an appropriate range of adverse circumstances, varying in nature, severity, and duration, that are aligned to the firm's risks and vulnerabilities), with a focus response and recovery arrangements.

Over time, firms are expected to sophisticate their scenario testing as they develop operational resilience for each IBS, achieved by:

- Testing against increasingly complex SBP scenarios (e.g., by increasing the number or type of resources unavailable for delivering the IBS or extending the period for which a particular resource is unavailable), proportionate to the firm and the degree of operational resilience each IBS has.
- Maturing the format and type of testing used to understand the resilience of the organisation, evolving from judgement, desk-based scenario tests, to a wider range of testing that provides empirical data including, but not limited to:
    - Penetration tests
    - Disaster recovery / fail over tests
    - Simulations
    - Lessons learned from real scenarios

### Guiding Principles

P.1 **Firms must regularly test their ability to remain within ITOLs in SBP disruption scenarios, focusing on their recovery response arrangements.**

P.2 **Firms should identify the SBP scenarios they use for testing (e.g., documenting these in a 'scenario library'). When setting these scenarios, firms should consider (1) previous incidents or near misses within the organisation, across the financial sector, and in other sectors and jurisdictions; (2) new and emerging risks and threats identified through horizon scanning, and the proximity of impact.**

P.3 **Firms must develop and maintain a testing plan which takes account of, but not limited to, the following factors:**

- **the type of scenario test.**
- **the scenarios which the firm expected to be able to remain within ITOLs and which ones they may not.**
- **the frequency of the testing.**
- **the number of IBSs tested.**
- **the availability and integrity of resources.**

- **how their environment is changing and whether this will give rise to different vulnerabilities.**
- **how the firm would communicate with internal and external stakeholders effectively to reduce the harm caused by operational disruptions.**

**P.4 The identified scenarios and testing plans should be reviewed annually at a minimum or following significant changes to the firm's risks and vulnerabilities.**

**P.5 Firms should sophisticate their testing plans as they develop operational resilience for each IBS including:**

- **Testing against more SBP scenarios (e.g., by increasing the number or type of resources unavailable for delivering the IBS or extending the period for which a particular service is unavailable).**
- **Maturing the format and type of testing (e.g., evolving from judgement, desk-based scenario tests, to a wider range of testing that provides empirical data).**

**P.6 Firms should ensure that they are testing the full range of response and recovery activities they would undertake in the event of a disruption. Where full recovery of the resources that support an IBS is not possible, firms should consider a broader range of other response actions which could be taken to remain within ITOL (e.g., substitutability, use of alternative channels, tactical remediation processes, alternative operational / manual workaround procedures, customer treatment strategies, communications strategy and plans, etc.).**

**Where a firm relies on a third party for the delivery of an IBS:**

**P.7 Firms should acknowledge any response and recovery activities which are contingent on or limited by third parties. This should be supported by rationale of the level of assurance over, and any assumptions relating to the actions taken by, third parties and direct market participants.**

**P.8 Firms should have assurance that material third party arrangements enable them to remain within ITOL. Consideration should be given to the following:**

- **Material third party contractual arrangements to include necessary measures to enable firm to gain assurance of third-party resilience, including access to premises, the third party's own testing outcomes and incident data.**
- **Third parties directly participate in testing where practicable, sharing relevant data and demonstrating resilience capabilities with the firm.**
- **Assessing the resilience of third-party arrangements in line with its own assets under the firm's own control.**
- **Firm considers all elements of response and recovery from a scenario that are in its control, even where there is a primary reliance on the third party for full recovery (e.g., firm responsible for data integrity and quality following cyber incident).**
- **Testing should include a firm's ability to resume delivery of IBS within ITOL when the material third party service becomes unavailable.**

## 5.2 The purpose of scenario testing

### Overview

Scenario testing provides assurance that a firm's detect, response and recovery plans and capabilities are effective to enable a firm to remain within ITOL in SBP scenarios. The testing enables firms to identify vulnerabilities or gaps in their detect, response and recovery plans to take action to remediate. It also provides opportunities to improve the resilience of its IBSs.

Scenario testing helps to answer these questions:

- For the scenario being tested, do current response and recovery capabilities demonstrate that the harm and risk factors underpinning ITOLs (considering both FCA and PRA objectives as appropriate) are effectively mitigated before intolerable harm is reached?
- What opportunities are there to improve resilience through improved planning and documentation, what mitigants can be deployed, leveraging alternate systems internally or through setting up arrangements with other firms? Where could firms collaborate to improve systemic resilience?
- Are there gaps in the capabilities required to recover service(s) within tolerance(s) that need to be highlighted to management? Are there solutions already available within a firm to enable recovery within ITOL or is investment required to develop a new capability?

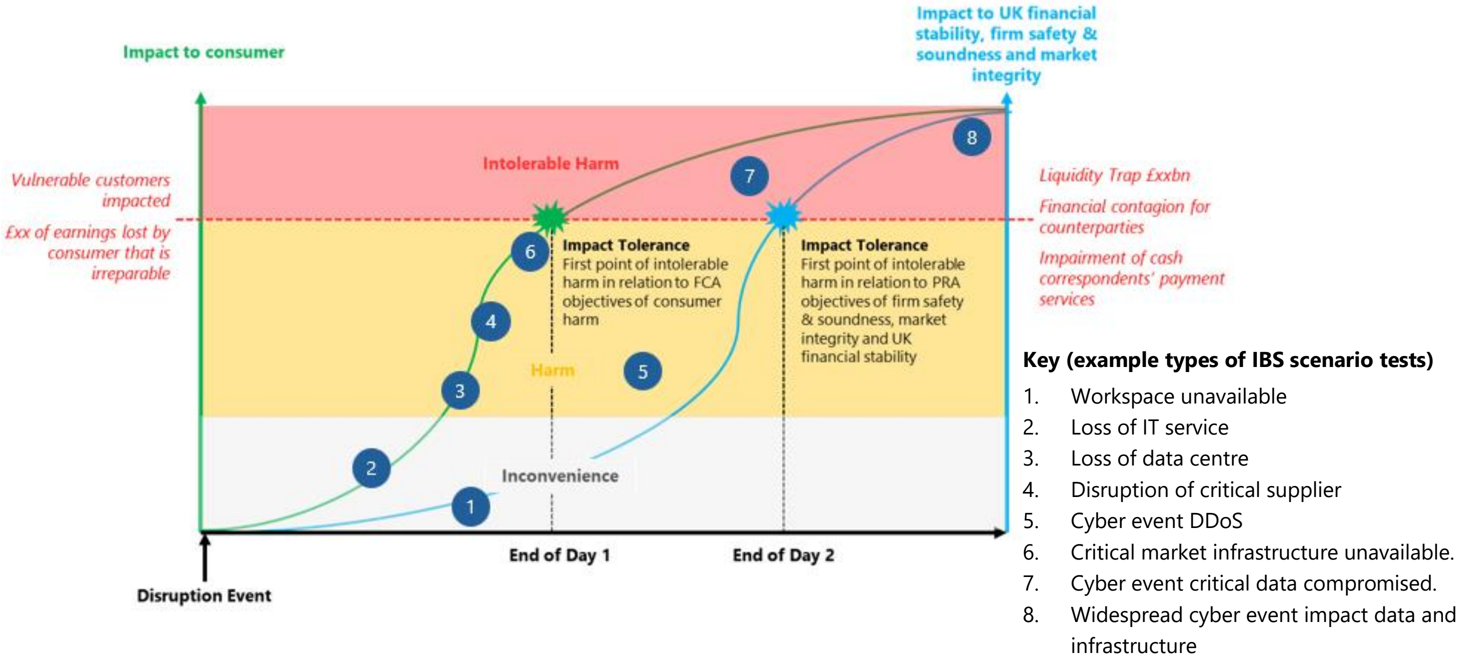
### Assessing scenario test results against ITOLs

It is expected that scenarios will breach ITOL if the event goes unmitigated and that even with mitigation, some scenarios will breach ITOL.

For scenarios where firms are unable to meet ITOL it should be determined if scenarios are too extreme to mitigate, or if remedial action is required. Rather than looking at scenario tests in isolation, a broad range of tests across multiple resource pillars should be considered, to highlight which scenarios firms are able to manage within tolerance and those which they aren't.

**Figure 9** shows how disruption events unfold and assessing the associated impact to a) consumer harm and market integrity and b) safety and soundness, and financial stability.

*Figure 9. Examples of IBS scenarios*


Impact to consumer
Impact to UK financial stability, firm safety & soundness and market integrity
Vulnerable customers impacted
£xx of earnings lost by consumer that is irreparable
Intolerable Harm
Liquidity Trap £xxbn
Financial contagion for counterparties
Impairment of cash correspondents' payment services
Impact Tolerance
First point of intolerable harm in relation to FCA objectives of consumer harm
Impact Tolerance
First point of intolerable harm in relation to PRA objectives of firm safety & soundness, market integrity and UK financial stability
Harm
Inconvenience
1
2
3
4
5
6
7
8
End of Day 1
End of Day 2
Disruption Event

**Key (example types of IBS scenario tests)**

1. Workspace unavailable
2. Loss of IT service
3. Loss of data centre
4. Disruption of critical supplier
5. Cyber event DDoS
6. Critical market infrastructure unavailable.
7. Cyber event critical data compromised.
8. Widespread cyber event impact data and infrastructure

**Figure 9** illustrates how test results can be mapped against the ITOL of an IBS. The test scenarios would be named more explicitly within a firm, including names of relevant critical suppliers, data centres etc.

It should not be assumed that the results plotted (inside or outside of tolerance) imply a complete recovery of service. The results highlight whether breaching an ITOL can be avoided using mitigating actions, i.e., restoring a degraded service. Full restoration of normal service may occur over a longer period of time.

## 5.3 Developing and maintaining a scenario testing plan

### Scope

- Testing should be deliberately demanding but proportionate to the firm's maturity (crawl, walk, run).
- Disruption doesn't happen in isolation. Testing should consider enterprise-wide scenarios as well as impact to individual IBSs. This may also include idiosyncratic scenarios.
- The design of the scenario test should acknowledge the potential wider impact of a scenario, including impacts to other firms and the markets in which the firm operates.
- Each test should cover a different scenario from the last; multiple iterations of the same event have a diminishing return and risk complacency. Format and participants of testing should vary.
- Each test should involve either a primary decision maker(s) or their delegate(s) to build depth within functions.
- Firms should consider scenarios that impact service unavailability and data integrity.

### Priorities

- Internal risk registers and known vulnerabilities should inform testing priorities.
- Although known vulnerabilities will influence priorities, testing should occur across all resource pillars to build a complete view of capabilities and to ensure testing expertise is developed in all areas. Additionally, there may be little value in prioritising a known vulnerability if steps are being taken to mitigate and close any gaps.

### Frequency

- There is an expectation that all IBSs will be evaluated against a range of scenarios, and gaps remediated, during the implementation window defined by the authorities. This will provide an indication of the volume of testing required by each firm.
- Scenario testing should reflect the degree of change to operations i.e., scenario testing should keep pace with change to validate that ITOL can still be met in an evolving environment and to ensure the expected levels of resilience are in place or are being maintained.
- Firms should respond to significant changes in the threat landscape, and flex testing and/or risk assessments, as necessary.
- Scenario testing should be considered following any improvements made in response to a previous test.
- One scenario test could be used to evaluate multiple IBSs (and more than one scenario could be included in a single test).
- Scenario tests can test multiple regulatory criteria i.e., test intolerable harm and policyholder protection. Where one ITOL is more stringent than another, firms must demonstrate that they have considered both

tolerances within their scenario design and execution. Just because you may meet the tolerance threshold of one criterion, doesn't mean by default you have met another.

### Risks

Whilst striving for high levels of assurance, firms must manage the potential for disruption caused by testing, particularly in live environments. Risks to production / business as usual (BAU) must be clearly articulated and accepted in advance, and any risks should not outweigh the benefit of testing.

The potentially daunting extent of scenario testing can be reduced by considering:

- How existing testing can be leveraged, or modified, to meet the requirements of scenario testing (e.g., DORA (Digital Operational Resilience Act) / ICAAP (Internal Capital Adequacy Assessment Process) etc.).
- Capabilities that are evaluated in anger (e.g., COVID-19 and unavailability of buildings) can be used to provide assurance.
- Leveraging assumed capabilities and extrapolating recovery times (e.g., using testing from a similar system, or generic recovery capabilities). However, this may provide lower levels of assurance.

### Example scenario inputs and sources for consideration

To ensure impact scenarios are adequately plausible, chosen scenarios should consider actual events that have occurred, as well as being forward looking, factoring in threats and risks from the horizon. The list below highlights some external data sources that should be considered when considering plausibility of scenarios due for testing. The CMORG Dynamic Scenario Library should also be used as a detailed source of scenarios that can be used and adapted by firms to consider and use as part of their scenario testing plans.

- CMORG Dynamic Scenario Library
- National Risk Register (NRR)
- Global Risk Register (GRR)
- Business Continuity Institute (annual horizon scan)
- ORX Scenarios database
- ORIC International
- Insurance company models and insights
- Internal, firm specific risk registers
- Regulatory publications (e.g., ICO/FCA/PRA)
- Cybersecurity Information Sharing Partnership (CISP)
- World Economic Forum (WEF)
- National Cyber Security Centre (NCSC)
- Securities Industry and Financial Markets Association (SIFMA)
- CMORG Strategic Risk Register (SRR)

## 5.4 The approach to scenario testing

### Defining the scenario

In defining a scenario, firms should identify an appropriate range of adverse circumstances varying in nature, severity, and duration, proportionate to their size and complexity.

Scenarios that are developed and prioritised for testing should reflect the firm's assessment of its risks and vulnerabilities that its IBS are exposed to.

### Considerations when defining the scenario - Approach

The factors that firms should consider include the following:

- The scenario should set out the cause of the disruption. The cause will enable specific response and recovery actions and help to identify issues that need to be remediated. It will also enable the firm to determine how it will detect the disruption and identify specific controls and procedures that it will be reliant on. Simply stating that one or multiple resources is unavailable for a period is less helpful in determining the effectiveness of response and recovery actions.
- Risk coverage of scenarios. Firms should consider crystallisation of data integrity and/or availability risks, as well as scenarios that recognise that all IBSs could potentially be impacted by SBP disruption including simultaneous disruptions.
- Calibrating the scale of disruption by considering the impact of the scenario through:
  i. A significant disruption impacting multiple resources and/or multiple IBSs.
  ii. Systemic disruption impacting multiple firms or parts of the UK financial system.
  iii. Sequence of events, or parallel events occurring amplifying the impact of the disruption.

### Generate SBP scenario

- Firms should define a methodical approach to defining scenarios which provides a clear rationale for why certain scenarios are prioritised.
- The approach should include a mechanism for calibrating what is SBP for the firm and be tailored to the IBS being tested. The factors in relation to severity and plausibility are covered in the next sections.
- Scenarios need to be internally relevant (applicable to a firm's operating circumstances), proportionate to the size and scale of the firm and have a clear trigger and articulation of impact and scope.
- The SMEs that understand the key dependencies and vulnerabilities of the IBSs should be involved in scenario development (e.g., involving technology and cyber experts will be necessary to ensure that cyber scenarios are relevant, as well as SBP).
- The outputs of mapping may highlight areas of risk or concern that would benefit from inclusion in the scenario.
- Clarity around which elements of the IBS the scenario is pertinent to, and whether other dependencies might also be impacted should be taken into account.
- Where vulnerabilities have been identified outside of testing, or are in the process being addressed, scenario testing may be less valuable.
- Complete review and challenge with relevant internal teams (e.g., relevant SMEs and Second / Third Line of Defence).

## Plausibility

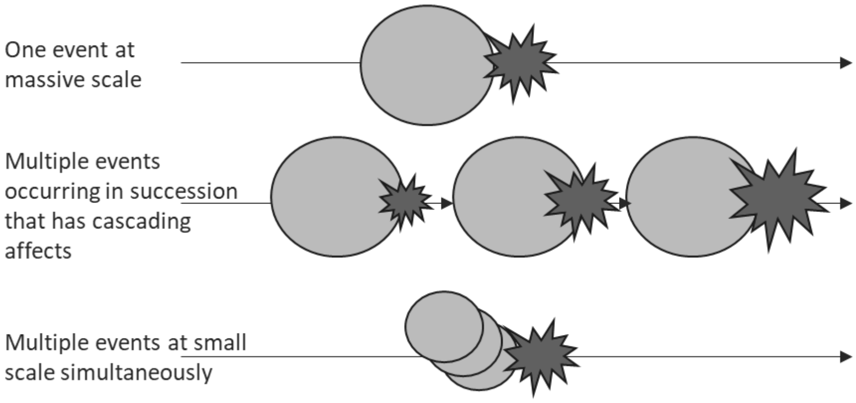
- A scenario can be defined as plausible if it is conceptually consistent with what is known to have occurred in the past (i.e., it has some basis in prior knowledge).
- It should be possible to link scenarios back to threat intelligence and open-source risk registers – plausible threats should be known / monitored.
- High plausibility is reached through the following:
  - There are multiple different sources of corroboration.
  - The explanation of the concept or event is low complexity.
  - There is minimal conjecture.
- Risk coverage of scenarios – firms should assume that risks will crystallise. This should include data integrity and availability, as well as scenarios that include both integrity and availability elements. The coverage model should recognise that all IBSs could potentially be impacted by SBP disruption including simultaneous disruptions.
- Firms should consider a variety of sources such as previous incidents or near misses experienced internally or observed externally, horizon risks, such as the evolving cyber threat, technological developments, and business model changes.
- The cause of disruption should reflect, but not be limited by, an assessment of identified risks and vulnerabilities such as sophisticated cyber-attacks, failure of third parties that are material to remaining within tolerance, and failure of IT infrastructure or controls / processes. The 'Scenario Themes' can be used to highlight the different types of disruption and provide details of previous incidents to support scenario creation.
- The cause of disruption and how that might reflect in the severity of the scenario should be considered, (e.g., the capability of a threat actor is likely to affect the potential outcome of a cyber event because a nation state will have significant resources, and different motivations, when compared to a less sophisticated actor with a purely financial motive).

## Severity

There are a broad range of considerations for defining the severity of the scenario:

- The surface area of disruption. Is it one or more dependency type impacted (e.g., firm and third party impacted by the same cyber vulnerability)? How many dependencies are impacted (e.g., is it a single database or has a data integrity issue cascaded through interconnected systems)? How many IBSs could be disrupted simultaneously by the loss of the same dependency (e.g., a shared supplier, or a data centre)?
- The scenario narrative should be explicit about the way the disruption manifests, particularly for cyber events where a capable threat actor may have a range of options for causing disruption.
- Scenarios should consider the worst possible timing of the disruption (e.g., a weekend / evening disruption vs a busy trading day).
- Graduating and compounding impacts. Could multiple events occur sequentially that ramp up the impact over time, or could parallel events occur? Scenario injects may be used to push a scenario to a point where it would not be possible to remain with tolerance – consideration should then be given to whether the disruption has become too severe to plan for or is beyond plausible.
- For systemic firms specifically, consideration should be given to the length of disruption and whether the scenario story looks at the impacts to other firms, and how disruption impacts corporates and markets because of interconnectedness.

*Figure 10. Compounding impacts of an event*


One event at massive scale
Multiple events occurring in succession that has cascading affects
Multiple events at small scale simultaneously

## Tailored

- Use the results of end-to-end resource / dependency mapping completed against IBSs to build the scenario around concentrations, shortfalls in BAU delivery or known risks / vulnerabilities.
- Consider those dependencies whose failure would have greatest impact on service delivery.
- Use external past events as a reference or start point if the organisation involved is sufficiently comparable in terms of scale and complexity.
- Be cautious with using internal past events (or open regulatory / audit findings) as a scenario; they can too easily be dismissed as fixed or being fixed.

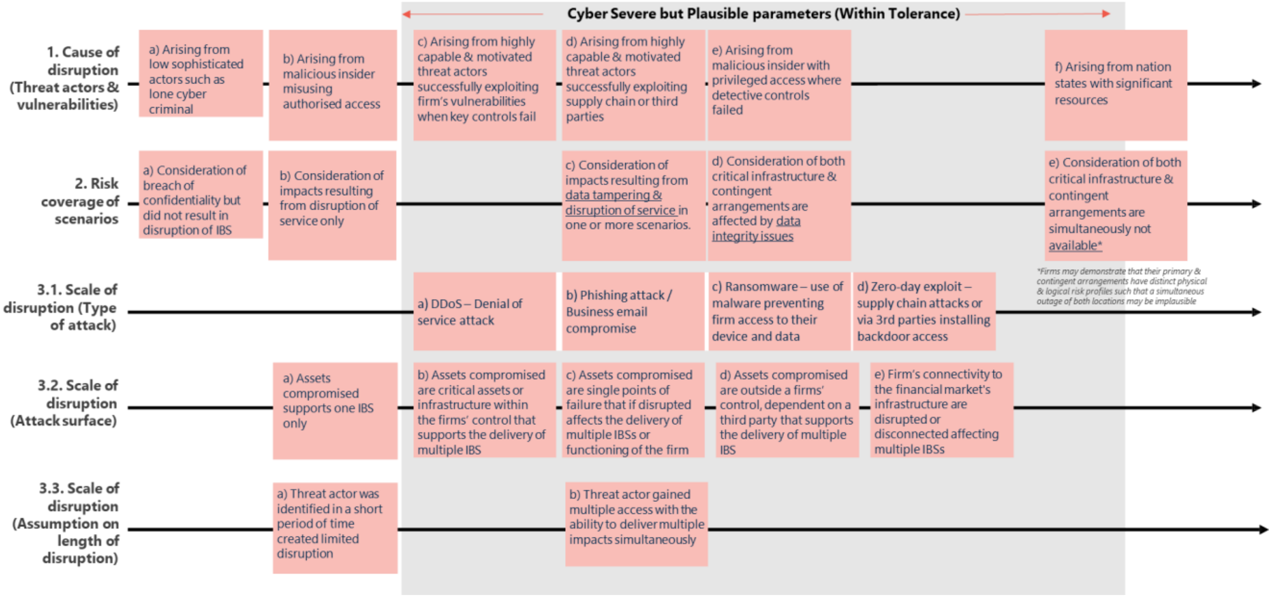
## Assumptions

- Key scenario assumptions should be appropriately justified and documented, informed by internal and external incidents to ensure that they remain plausible. Care must be taken to avoid bias and an over-reliance on recent experience.
- When defining assumptions, it can be useful to consider the key drivers of potential impact. These can include: (1) type and volume of customer accounts impacted; (2) anticipated timing of any system outage; (3) the cause (e.g. fire, flood) and extent of any physical damage; (4) the extent to which other firms / wider sector participants are impacted.
- The CMORG Dynamic Scenario Library provides a useful resource of categorised and individually described scenarios and assumptions to be considered / developed by firms.

## Example of calibration of a cyber scenario

**Figure 11** is illustrative only and the relevance or accuracy will be dependent on a range of firm specific factors (e.g., some firms only have a small handful of IBSs so the calibration of SBP will differ between firms). Please note the example below is calibrated in relation to systemically important firms.

*Figure 51. Calibration of cyber scenarios*


Cyber Severe but Plausible parameters (Within Tolerance)
1. Cause of disruption (Threat actors & vulnerabilities)
a) Arising from low sophisticated actors such as lone cyber criminal
b) Arising from malicious insider misusing authorised access
c) Arising from highly capable & motivated threat actors successfully exploiting firm's vulnerabilities when key controls fail
d) Arising from highly capable & motivated threat actors successfully exploiting supply chain or third parties
e) Arising from malicious insider with privileged access where detective controls failed
f) Arising from nation states with significant resources
2. Risk coverage of scenarios
a) Consideration of breach of confidentiality but did not result in disruption of IBS
b) Consideration of impacts resulting from disruption of service only
c) Consideration of impacts resulting from data tampering & disruption of service in one or more scenarios.
d) Consideration of both critical infrastructure & contingent arrangements are affected by data integrity issues
e) Consideration of both critical infrastructure & contingent arrangements are simultaneously not available*
*Firms may demonstrate that their primary & contingent arrangements have distinct physical & logical risk profiles such that a simultaneous outage of both locations may be implausible
3.1. Scale of disruption (Type of attack)
a) DDoS – Denial of service attack
b) Phishing attack / Business email compromise
c) Ransomware – use of malware preventing firm access to their device and data
d) Zero-day exploit – supply chain attacks or via 3rd parties installing backdoor access
3.2. Scale of disruption (Attack surface)
a) Assets compromised supports one IBS only
b) Assets compromised are critical assets or infrastructure within the firms' control that supports the delivery of multiple IBS
c) Assets compromised are single points of failure that if disrupted affects the delivery of multiple IBSs or functioning of the firm
d) Assets compromised are outside a firms' control, dependent on a third party that supports the delivery of multiple IBS
e) Firm's connectivity to the financial market's infrastructure are disrupted or disconnected affecting multiple IBSs
3.3. Scale of disruption (Assumption on length of disruption)
a) Threat actor was identified in a short period of time created limited disruption
b) Threat actor gained multiple access with the ability to deliver multiple impacts simultaneously

## 5.5 Test ability to remain within Impact Tolerance

Testing is likely to include table-top (discussion-based), simulations and live proving elements. Exercises will be enhanced if the groundwork is done in advance where possible (e.g., known or assumed recovery times for technology dependencies is captured ahead of table-top exercises).

Firms should aim to gain the highest possible level of assurance whilst not exposing the firm to unacceptable risks. The focus is on understanding and, where possible, demonstrating whether current capabilities are effective at remaining within ITOLs. Evidence should be gathered to support the conclusions that are based on testing.

Gathering the information to complete the 'test' doesn't need to occur in a single exercise, as there may be a lot of data to collect, particularly if testing a new scenario. Similarly, the 'test' does not need to be completed in one session but can be completed over multiple sessions and in a way which is supportive of the scenario test and test type.

### Example test types for scenario testing plan

Firms may use a combination of different types, or methods of testing, but the objective is to provide sufficient assurance that response and recovery capabilities exist and are effective in ensuring the firm is able to operate within ITOL for a specific scenario, and if not, what can be done.

In addition to the level of assurance achieved through the test type, firms can increase sophistication and realism through considering the surface area of the disruption. Factors include how multiple instances of the same types of dependencies might be impacted; how a disruption might impact multiple dependency types; or how a disruption would impact multiple IBS either immediately or over time.

Both the scenario and testing format will drive the information gathering requirements.

*Table 1: Test Types*

| Test Type | Characteristics | Level of Maturity in Operational Resilience | Planning Time and Effort | How does it support Testing to Remain within ITOL? |
|---|---|---|---|---|
| **Drill** | • Tests specific function or process<br>• Usually requires physical action<br>• Typically, a 'pass / fail' outcome | Low | Limited | Provides data that contributes to an understanding of the time to respond and recover (e.g., time to cascade a message, evacuate a building or setup an IVR in an outage). |
| **Structured Scenario Exercise (SSE)** | • Facilitated<br>• Scenario based<br>• Driven through predetermined questions | Low to medium | Low | Provides an opportunity to walkthrough the steps and timeline for response and recovery. Minimum prerequisite for reviewing and validating existing plans or plans in draft. |
| **Table-Top / Desktop Exercise / Assessment** | • Discussion based<br>• No time constraints<br>• Used as a tool to build competence<br>• Elements of ambiguity to trigger creativity in participants | Low to medium | Medium | Provides an opportunity to walk through the scenario, steps and timeline for response and recovery. Elements of ambiguity and stressing of assumptions should stimulate thinking on existing workarounds, contingencies, alternatives and substitutions. |
| **Simulation / War Game** | • Designed to depict an actual or assumed real-life situation<br>• Competitive / contested environment<br>• Use of technology / techniques to engage participants and create stress | Medium to high | Extensive | Provides an opportunity to rehearse the steps and timeline for response and recovery in as close to real life as possible. |
| **Live Systems or Operational Testing** | • Real time<br>• Test / Production / Recovery environment | Low to high (depends on complexity of firm) | Extensive | Provides data on timeline of restoration of IT infrastructure, systems, and applications. Identifies any issues in recovery and rehearses supporting plans. Provides data on ability to recover to Work Area Recovery sites / similar. |
| **No Notice** | • Unannounced | High | High | Provides additional credibility in evidence of response and recovery timeline. |
| **Operational Incidents** | • Although not a test, real incidents can be leveraged to confirm the effectiveness of resilience measures | N/A | N/A | Explicit validation of capabilities and confirmation of whether ITOL is met or breached. |

*All test types can involve third parties (e.g., outsourced service providers, cloud hosting platform providers). Involving third parties is likely to increase the planning time and effort.*

## Information gathering considerations

- Which individuals would be expected to participate in this type of response and therefore may be needed during the test?
- When identifying the data requirements, the following should be considered / obtained:
  - ITOL metrics used to define intolerable harm / risks to firm safety and soundness etc.
- Operational data at different periods including:
  - Demand and volumes (e.g., number of new claims via phone or online and significant demand variations in time / day / month).
  - Operational hours.
  - People capacity and locations.
- Knowledge of the processes and resources / dependencies that make up the IBS.

- The SLAs and known capabilities of third parties and FMIs including contingencies, and evidence obtained during third party testing and assurance activities.
- Knowledge of what contingency plans already exist, what options there are for relevant resource pillars including workarounds and alternates.
- Known risks and vulnerabilities.
- Duration of key technical activities such as time taken to failover IT systems, relocate staff to alternate working locations or recover data from backup solutions if Production and DR data is compromised. Knowing existing component recovery time will save time during the exercise and allow participants to focus on the unique aspects of the scenario such as alternate systems and workarounds.

### Running the test - Introduction

For each scenario, firms should test the effectiveness of the firm's ability to respond and recover and to confirm whether they are able to remain within ITOL. Actions to remain within ITOL may include:

- Response actions such as mitigations, including the delivery of IBS through alternative means or channels, or taking steps to ensure intolerable harm is not breached. Appropriate response actions may provide more time for firms to take recovery actions.
- Recovery actions to restore and resume the delivery of IBS and clear any backlogs.

### Running the test – Key elements of response and recovery

- Failure / disruption is assumed – ensure participants are aware not to challenge the scenario, firms are dealing with inevitability. Testing should focus on detection, containment, mitigation, response, and recovery actions.
- Service disruption commences at the point of failure for a service that is available 24/7. When a service is not provided 24/7, service disruption commences at the point of failure if such failure occurs during the business day or, if the failure occurs out of hours, the start of the next business day. This ensures that the operational disruption being tested is tracked against the scenario and ultimately testing whether the ITOLs were breached or met.
- As duration of recovery is important to assessing the outcome, testing should consider activities that impact the timeline such as the time required for data analysis during an incident, decision making etc. Previous testing and incidents can be leveraged.
- Setting out how the disruption will be detected and what controls or processes that firms will be reliant on so that appropriate response and escalation will be triggered. Include indicative timeline based on experience / known incidents? How would this differ during a disruption to 3rd party / FMI?
- What are the immediate response steps that would be taken? (in some circumstances taking the systems and therefore the business service off-line might be the safest and most effective immediate response to the event).
- What are the communication requirements (internal and external audiences) for the scenario envisioned, including who would provide updates to crisis structures?
- Containment actions: where relevant, what actions will firms take to contain or limit the amplification of the impact, within the organisation and external to other customers, third parties or FMIs. This includes factors that may lead to a firm to take action to disconnect from a third party and FMI or customers to its systems. What are the post-incident service recovery actions including reconnection criteria.

- Articulating the impact, leveraging defined ITOL metrics to enable targeted response and mitigating actions.
- How effective are mitigating actions in reducing impact / harm to consumers, the firm, and the wider sector? Is there a solution that might mitigate impact for some of the impacted consumers, even if not all? How sustainable are these mitigations, and will they extend the point at which ITOL would be breached? Are there options for a partial resumption of service (e.g., manual payments), or the delivery of an alternative service, which would mitigate impact? Are there alternative channels that can be used, and do they have the capacity to handle increased volume? How effective are third party / FMI mitigations?
- Are the mitigations in place effective for all harm factors (e.g., a mitigation for consumer harm may not be effective to mitigate risks to financial stability)?
- What relevant response and recovery plans and playbooks are in place, and how long does the recovery take? Which activities can be completed in parallel and where are there hard dependencies?
- Particularly for extended disruptions, who would support the response and recovery (e.g., CISO, operations, technology, business functions) and how might the resource profile change over time?
- For data-related scenarios what is the data recovery strategy, including effective execution of data reconciliation to ensure data integrity so that services can be resumed safely?
- Considering other ITOL metrics (in addition to the time-based metric) does the test demonstrate that the threshold of "harm" to customers, the firm and the stability of the financial system is not breached?
- Does the test confirm the assumptions made in the ITOL statement (e.g., the point at which intolerable harm would occur), or could intolerable harm materialise more quickly or slowly than expected?

## 5.6 Assessing test outcomes

### Assessing the outcome

SME judgement on the effectiveness of capabilities and recovery times is important and should be supported with evidence/data to provide greater assurance. The conclusions on remaining within ITOLs should be supported by qualitative and quantitative data and evidence, where possible, including due diligence on third party scenario specific recovery capabilities. Evidence could include:

- Metrics on recovery time, either from internal testing, or data obtained from third parties testing programme.
- Effectiveness of mitigating procedures such as how critical transactions are processed via alternate mechanisms, and backlogs cleared following service resumption. These should be aligned to the harm and risk factors underpinning ITOLs.
- Evidence of the firm's capability to recover data or service (could be from the scenario test itself, other testing, or an incident) - a mixture is useful (previous evidence, or part of the test).

Where firms have made assumptions on recovery, firms should make sure these are justified, documented, and challenged for reasonableness.

Where firms are unable to remain within ITOLs:

- The scenario should be reviewed to reassess plausibility and severity.

- Consider whether the scenario is relevant to other IBS, and how conclusions can be expanded as a result.
- Review whether detective controls and third party contracts / SLAs need to be revised.
- Consider the sustainable and effective mitigation responses to contain the impact and minimise intolerable harm.
- Document the justification and rationale where there is no recovery plan.
- The post-test review process should consider the following:
  - A list of key risks, vulnerabilities and gaps by resource pillar should be documented. Newly identified risks should be assessed and logged in the appropriate system of record. The definition of remediation actions required to manage the risks identified should be considered alongside other remedial actions to maximise value of investment.
  - Options to reduce impact to customers, clients, the firm, and markets.
  - How time to recover might be decreased – considering all possible options.
  - How responses and mitigations can prolong the point at which intolerable harm occurs.
  - The effectiveness of detection, containment, response, and recovery actions, and whether changes are required (e.g., new / revised response plans).
  - Whether there are any control gaps that need to be raised.
  - Are there any changes to the ITOL required (metrics or duration).
  - The point in time that the service(s) was restored or partially restored (degraded). When would the first end user receive the identifiable outcome of the service?

# 6 Vulnerabilities, Lessons Learned and Remediation

## 6.1 Overview

### Section Objectives

- To assist firms in implementing and enhancing their approach to the identification, prioritisation, remediation, monitoring and reporting of vulnerabilities that threaten their ability to deliver IBSs within ITOLs.

### Regulatory context

The UK authorities expect firms to regularly assess vulnerabilities identified (e.g. through mapping, results from controls testing, scenario testing, operational incidents within the firm or those with wider sector impact), prioritising those that have the greatest potential to impact consumer harm, their own safety and soundness or, where relevant, financial stability. Where firms identify vulnerabilities that threaten their ability to deliver IBSs within ITOLs, the UK authorities expect firms to take prompt action by developing and implementing effective remediation plans (including tactical remediation processes, alternative optional workaround procedures, strategic investments to effectively address vulnerabilities, and communication strategies for both internal and external stakeholders).

These remediation plans should include a timing for the necessary improvements, with the UK authorities expecting that these be approved, fully funded, and appropriately governed to ensure delivery, with evidence at closure. Where appropriate, these should be validated through scenario testing to verify that the vulnerability has been resolved. Where a firm's plans to build resilience are reliant on longer term change programmes, the authorities expect there to be effective mitigating action in place to meet their requirements while these programmes complete, and for firm's Boards to be satisfied that these are effective in mitigating the risk of harm to customers, the firm, and the market.

### Guiding Principles

P.1 **Firms should identify vulnerabilities and areas for improvement, using these to support the design of suitable test scenarios that, without mitigation, have the potential to cause an ITOL breach, to highlight the key areas for improvements and investment required, and to ultimately drive improvements in a firm's resilience posture.**

P.2 **When identifying, prioritising and remediating vulnerabilities, firms should aim for consistency and repeatability. This may be achieved by measuring resources in each resilience pillar (technology, third party, information, facilities, people) against a set of common resilience indicators. Although resilience indicators are not mandated by the authorities, they help to provide a data-led view of the firm's resilience.**

P.3 **The aim of resilience indicators is to determine whether mapped resources are fit for purpose. These indicators, jointly with high-level metrics and insights, inform current state and provide an input into resilience improvements through strategic investment prioritisation and localised control improvements.**

P.4 **When designing resilience indicators, firms should consider what is already being measured and consider its usefulness when viewed through a resilience lens, asking whether it provides any insight into the resilience of delivering the IBSs.**

**P.5 Vulnerabilities should be identified and prioritised based on the impact of an operational disruption when resources are not available, and whether IBSs can remain within ITOLs.**

**P.6 Assessments of the firm's resilience posture should be conducted on a regular basis (frequency to be defined by each individual firm) to understand how this changes over time, and following significant changes, e.g., to mapping.**

**P.7 It is imperative to assume failure, a principle that concurs with an understanding of operational resilience as an outcome. Thus, firms must work towards operational resilience continually to prevent disruption. Such work involves assessing as well as improving mapped assets and processes resilience, in effort to continue delivering IBSs and return to normal promptly following disruption. Vulnerability remediation is therefore best seen as a continuous cycle which drives learning and improved maturity.**

## 6.2 Vulnerability Remediation Lifecycle – Embedding and Taking Action

### Overview

This guidance defines a **resilience vulnerability** as '*any weakness or dependency that threatens the ability of a firm to deliver an IBS within its ITOL in the event of a SBP scenario. These vulnerabilities may be internal or external to the firm.*'

Vulnerabilities can manifest in resources, controls or processes as gaps (either incomplete or entirely missing), weaknesses (inadequate quality), susceptibilities (can be affected by something else) or flaws (defects or imperfections). Vulnerabilities, in an external context, should be considered in relation to (i) external dependencies which a firm may have, such as material outsourcing arrangements; (ii) on an inter-firm basis as part end-to-end service chain delivery, or (iii) within the financial system itself.

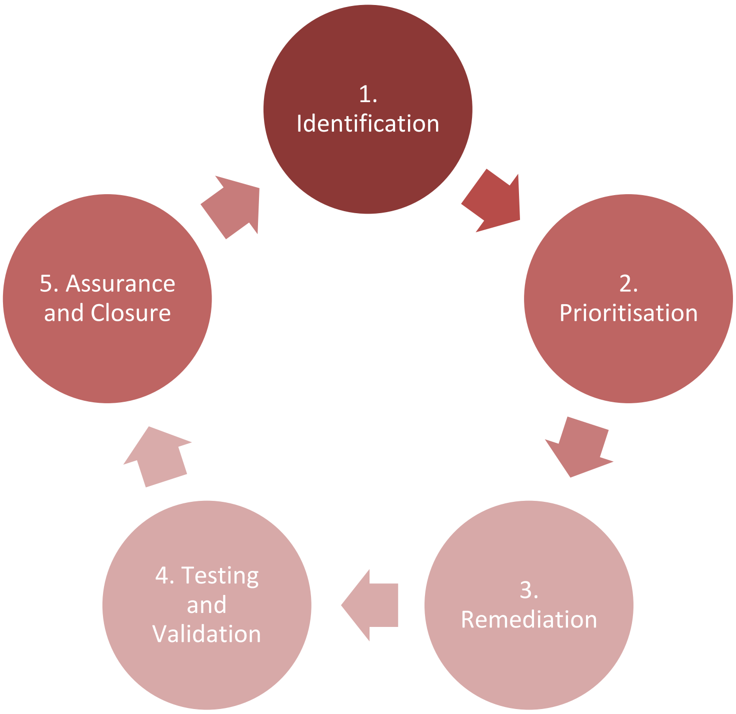
The experience learned from the 2024 CrowdStrike outage, as reported by the FCA[10], provided some positive comments on how well the industry responded. Demonstrating that whilst the new operational resilience processes of firms were effective there is more that the industry can and should be doing. In the context of vulnerability management, the FCA stated that "firms may benefit from reviewing third party risk management frameworks regularly, and after significant events / incidents, to improve the effectiveness of third-party risk controls". This highlights an area of focus for external vulnerability identification, and the lifecycle needs to include these requirements.

This guidance provides practices for the end-to-end management of vulnerabilities throughout their lifecycle, from identification, prioritisation, approval of remediation proposals and the monitoring of remediation progress and resulting reduction in risk.

Firms should regularly undertake assessments of the operational risks, threat landscape, and vulnerabilities relevant to its IBSs, using these to inform scenario testing plans and the design of disruption scenarios. Where vulnerabilities are identified and a firm is unable to operate within its ITOL, action must be taken to remediate these and with clear justifications for their completion time.

[10] CrowdStrike lessons for operational resilience (fca.org.uk)

*Figure 12. Vulnerability Remediation Lifecycle*



## 6.3 Identification

The first step a firm should take in their management of vulnerabilities is to set out how to identify vulnerabilities.

### Example sources for identifying vulnerabilities

Sources for identification of vulnerabilities can be based on concepts that a firm may already be using for other purposes. The list below is a non-exhaustive list of sources which can be used to identify vulnerabilities:

- **Incidents.** These may provide a source of identifying vulnerabilities during a stressed situation which may otherwise not be identified. It is important when looking at incidents that the findings are looked at generally rather than just in relation to that specific incident. Additionally, external events and incidents should always be reviewed to identify if there were any potential lessons identified that may have led to a vulnerability.
- **Mapping.** The identification of things such as single or critical points of failure, or a lack of substitutable alternatives may highlight vulnerabilities within service processes that require further assessment and remediation.
- **Risk and Control Assessments (RCAs).** The output from firms' RCAs may form part of the identified vulnerabilities. Deficiencies in the control environment may indicate potential vulnerabilities within a business service or process.
- **Risk Indicators and Appetite Actions.** Firms may look to use risk and resilience indicators (see Table 1 below) to identify where processes are outside of risk appetite and therefore where there may be vulnerabilities. Additionally, where issues are raised, these may also be vulnerabilities, should the have the potential to cause ITOL.
- **Scenario Testing.** The use of scenario testing can identify vulnerabilities which may cause the potential for intolerable harm.

## Reporting identified vulnerabilities

Firms should ensure they have a consistent and timely approach to the reporting and escalation of vulnerabilities, with clear governance structures and reporting lines. Reporting structure should be set out and approved, with the relevant individuals empowered to make strategic decisions such as remediation investment should it be required. Through this, the firm's governing body members should have a clear understanding of vulnerabilities found, and a clear understanding of the firm's position and roadmap to resilience. This information should be documented in the firm's self-assessment.

## Example resilience indicators

Resilience indicators may be split into two categories:

- **Lagging Indicators:** Backward looking risk and performance metrics that highlight current issues and risks with systems and processes.
- **Leading Indicators:** Forward looking measures that indicate potential future concerns or threats that should be planned for.

Although resilience indicators are useful for discovering vulnerabilities, there are also alternative approaches such as using control assessments to avoid duplication of effort and demands on the firm. The examples in the following table are not exhaustive but demonstrate the types of information that are likely to already be measured by the business and support areas. Resilience indicators are not intended to be prescriptive and will depend on a firm's size and complexity.

*Table 2: Lagging and leading indicators*

| Resource pillar | Resource type | Performance indicators (lagging) | Conformance indicators (leading) |
|---|---|---|---|
| **People** | • Primary teams<br>• Alternate teams<br>• Decision Maker<br>• SME | • Updated, known and accessible incident management and continuity / recovery procedures / documents.<br>• Business Continuity plans for each area signed off and exercised.<br>• Absence statistics for key roles<br>• Suitably Qualified and Experienced Persons (SQEP)<br>• Work area recovery<br>• Availability of key people<br>• Responsiveness of Op Res response system | • Staff turnover (FTE and contracted)<br>• Performance management<br>• Engagement and retention<br>• Knowledge management<br>• Succession plans<br>• Insider threat<br>• Cross-skilling<br>• Availability of contingent staff / assets<br>• Education and training of risks, mitigation and contingencies |
| **Facilities** | • Office sites<br>• Contact centres<br>• Data centres | • Key utility outages<br>• Generator design (e.g., backup power source)<br>• Network provision<br>• Air conditioning provision for data centres<br>• Physical security<br>• Fire safety | • Location risk / Natural disaster (flood, fires etc.)<br>• Statutory compliance |
| **Technology** | • Systems / applications<br>• Desktop builds<br>• Supporting infrastructure<br>• EUCs | • Patching coverage rate<br>• Frequency and severity of outages<br>• Mean Time to Resolution (of service outages)<br>• System availability<br>• System downtime<br>• Network spikes and utilisation bursts<br>• Network performance<br>• Service Level Agreement (SLA) conformance<br>• Business services without a defined SLA<br>• Service provider SLA conformance | • End of Service Life and support period<br>• System capacity<br>• Network availability<br>• Network bandwidth<br>• Monitoring<br>• Errors where root cause unidentified<br>• ITDR<br>• Data recovery<br>• Data privacy<br>• Critical data not digitised<br>• Technical debt (functional) |

| | | | |
|---|---|---|---|
| | | • Systems running without maintenance support<br>• Volume of changes (e.g., unplanned changes)<br>• Backup and restore procedures<br>• Incidents<br>• Malware scanning and security conformance | • Penetration testing<br>• Vulnerability scanning<br>• Access management<br>• Open security dispensations<br>• Obsolescence |
| **Processes** | • Key stages<br>• Actions | • Nonperforming processes (Audit)<br>• KPIs and/or KRIs as relevant to the service for trend analysis and to correlate IBS impact from incidents | |
| **Third parties** | • Material Suppliers<br>• Material Outsourcer<br>• Material Fourth parties – Sub Outsourcing | • Test of exit arrangements<br>• Control testing<br>• BC / DR Plans complete and accurate | • Switching impact<br>• Concentration risk<br>• Location risk<br>• Financial health |

## 6.4 Prioritisation

Once a firm identifies a vulnerability, it should consider performing an assessment on the vulnerability as soon as practical. This is done to determine the materiality of the vulnerability against the firm's IBS taxonomy. The output of this assessment may provide a view of potential impact of the vulnerability against meeting regulatory objectives and indicative prioritisation.

When prioritising vulnerabilities for remediation, firms may wish to use their own existing best practice guidance and methodologies, but as a starting point the following details could be used to inform these:

### Categorisation

Vulnerabilities may be seen as falling into two primary categories, micro and macro across three subcategories:

**Micro Vulnerability (firm level)**

1. **Corporate or enterprise-wide vulnerabilities.** These are vulnerabilities that affect most or almost all IBSs. Risks to these may be owned, reported and tracked by the relevant functional area (e.g., technology or physical security).

2. **IBS critical dependencies vulnerabilities.** These form a mix of conformance and performance metrics derived from managing areas and compliance areas, such as business continuity standards conformance. They come with the metrics of the managing area (e.g., for technology applications, the availability threshold may be >99.5%; for facilities, UPS switches tested monthly).

**Macro Vulnerability (system level)**

3. Macro vulnerabilities come about because of underlying externalities in the financial system, such as the structure of the financial system and the collective behaviour, or dependencies of, individual institutions and other participants within it. This could arise as a result of 'interconnectedness' of markets and participants in the financial system, meaning operational disruptions in one firm or FMI can have knock-on impacts on others. While operational incidents are most likely to originate in one specific part of the financial system, structural features and the collective behaviour or dependencies of firms, FMIs and other participants could amplify operational shocks in ways that can impact financial stability.

## Materiality and Impact Analysis

Firms may then consider the materiality of a vulnerability. This can be done in accordance with the categorisation of the vulnerability. Firms should consider assessing the vulnerability against a number of impact categories. These may include:

- **Impact on IBS.** Whether the vulnerability affects critical resources that are essential for business operations to deliver the IBS.
- **Prevalence.** Using the categorisation, how many IBSs could be impacted and at what level (micro or macro)?
- **Service Disruption.** Evaluate the potential for service disruption and the duration of downtime. Would this represent an ITOL breach scenario? Or cause a complete standstill to an IBS?
- **Data Sensitivity.** Determine if the vulnerability could lead to the loss, corruption or unauthorised access to sensitive or confidential data.
- **Compliance Requirements.** Identify any additional regulatory requirements that might be impacted by the vulnerability.
- **Legal Consequences.** Assess the potential for legal actions or fines resulting from a data breach or non-compliance.
- **Financial Impact.** Calculate the direct costs associated with mitigating the vulnerability, such as patching or system upgrades.
- **Indirect Costs.** Consider indirect costs like loss of business, reputational damage, and customer trust.
- **Threat Landscape.** Evaluate the current threat landscape and the likelihood that the vulnerability will be exploited.
- **Attack Vectors.** Identify the attack vectors that could be used to exploit the vulnerability.
- **Past Incidents.** Review historical data on similar vulnerabilities (internal and external).
- **Investor Concerns.** Assess how investors and stakeholders might perceive the vulnerability and its potential impact on the organisation.
- **End User.** Evaluate the potential impact on end users of the service. In particular if the end users of the service include vulnerable customers.
- **Risk Matrices.** Firms may wish to utilise existing risk matrices to support these assessments, factoring in likelihood and impact guidance.

## Risks

Once the materiality and impact assessment has been completed, firms may then wish to risk assess the vulnerability. This could be aligned to a firm's existing risk management framework and recorded in the firm's enterprise risk management tool. Risk owners may be identified aligned to the nature of the vulnerability and forecasting dates should be entered to support tracking and governance.

It is important to remember that when risk assessing a vulnerability, this does not include the assessment of likelihood. Vulnerabilities are limitations within a firm's estate that have materialised.

### Prioritisation

The firm could now opt to further refine identified vulnerabilities through a lens of prioritisation. This prioritisation could reflect the urgency to rectify the vulnerability against the risk to firm's IBS taxonomy. This could consider the following factors:

- **Prevalence.** How many IBSs does the vulnerability impact?
- **ITOL Breach.** Has the vulnerability resulted in an ITOL breach in the past?
- **Recovery / continuity plans.** Do these exist to provide service continuity to mitigate vulnerability impact?
- **Impact.** What is the potential impact of this vulnerability? (Utilising the output of the impact assessment).

Firms may want to implement a scoring matrix that outputs a prioritisation score for vulnerabilities based on the above characteristics. This will provide a prioritisation view, ensuring that the vulnerabilities that have the potential to cause the most harm are prioritised for remediation.

## 6.5 Remediation

Once a vulnerability has been prioritised, a firm will then proceed to remediate it, taking prompt action where the vulnerability threatens their ability to deliver IBSs within ITOL.

### Governance and Reporting

The vulnerability may be documented and taken to the next available appropriate governance forum(s) for socialisation and awareness. This may be aligned to the nature of the vulnerability – i.e., technology-based vulnerability should be taken to technology governance forums. If a vulnerability has been assessed as being a top priority or urgent, firms may consider invoking governance outside of usual cadence to reflect this urgency to address it.

The vulnerability and its remediation can then be scrutinised by the relevant governance forums, resulting in either acceptance of non-approval. Assuming approval, firms then could stand up the planning phase of remediation.

If the governance forum does not provide approval of the vulnerability, the firm may look to rectify the concerns as a priority (i.e., addressing additional information requests) and take back to the governance forum as soon as possible. If governance results in the vulnerability being descoped, the firm should document this as part of the governance process.

### Planning

Firms should consider producing a remediation plan, typically these plans include:

- **Executive Sponsorship.** This could be the accountable SMF24 or IBS owner.
- **Ownership.** Owner of the remediation plan, responsible individual.
- **Investment requirements.** See below section.
- **Target date.** Dates that plan will be delivered by.
- **Mitigation.** What steps can the firm take to mitigate the impact of the vulnerability whilst the remediation work is being conducted.

- **Milestones and Tasks.** Project outline of key milestones and associated tasks required to remediate.
- **Resources.** What roles, knowledge and skills are required to deliver the remediation.
- **Sustainability.** The vulnerability solution should be designed to be sustainable – i.e., the solution is not an interim solution, it is a permanent solution that addresses the vulnerability from reoccurring.

Firms may want to rely on a combination of internal and external resources to support execution of remediation plans.

### Investment

Not applicable for all vulnerabilities, however, some vulnerabilities may require the firm to secure investment to fund the remediation work. Firms may wish to utilise existing internal funding channels and governance. Business cases could be produced, including the planning activities. This business case should outline the benefits to the firm and how this support it in meeting its regulatory objectives and mitigates the cost of disruption.

IBS owners and other accountable owners typically champion the funding requirements to ensure they are secured as required. These existing governance and investment channels should include operational remediation as part of their highest category of prioritisation.

Firms may wish to invoke alternative channels by exception for urgent vulnerability remediation investment requirements, escalating as required upward to the Board.

If remediation funding cannot be secured, firms should consider escalating through appropriate channels for Board awareness and notifying relevant regulatory bodies. Additionally, firms may opt to take the proposal back to the committee for funding as soon as practical and, as an interim measure, prioritise the development of recovery / continuity plans to mitigate the vulnerability impact.

### Implementation

The vulnerability remediation plan is typically then implemented and delivered. The remediation plan may be tracked and monitored and taken to relevant internal governance fora, up to and including the Board, for updates on progress against milestones. It is good practice for firms to track and capture risks, findings and lessons learned from the implementation of the plan.

## 6.6 Testing and Validation

### Testing

Once implemented, firm should aim to test the effectiveness of remediation actions in mitigating the vulnerabilities. This could be aligned to the nature of the vulnerability and undertaken by suitable skilled individuals (e.g., if the vulnerability relates to data backups, firms should run a database restore to demonstrate effectiveness).

In addition to traditional testing above, firms may also prioritise operational resilience testing scenarios to test the vulnerability fix to determine if the solution enables the firm to remain within the ITOLs. Where practical, testing is typically repeated as soon as possible, through a range of scenarios, to ensure that the implemented solution is robust.

### Continuous monitoring

The fix to the vulnerability could be continuously monitored, with appropriate controls in place to ensure that the solution is fit for purpose and performs to acceptable standards – i.e., through cloud monitoring service to ensure platforms meet availability key performance indicators (KPIs).

### Risk mitigation

Risks aligned to the vulnerability remediation work and identified through response planning could be documented, assessed and managed through the firm's traditional risk management framework and enterprise risk management tools. This approach supports the robustness of the vulnerability remediation solution.

## 6.7 Assurance and Closure

### Purpose and Definition

IBS Owners, senior management, authorities and other stakeholders place reliance upon the work of others for the successful remediation of vulnerabilities. Whilst robust practices should be in place to test and validate the remedial actions, a final step in the lifecycle is required to provide assurance and formal closure over whether the risks to the IBS have been reduced as planned.

Confidence diminishes when there is uncertainty over the integrity of those activities, caused for a number of reasons (e.g., external events, change practices have a poor reputation from past failures), hence the importance of formal closure. Dependent upon the vulnerability and the remediation, Assurance may be considered not to be necessary, but closure is required for all vulnerability remediation programmes.

### Assurance

Assurance can take different forms:

- Day to day management of the vulnerability remediation.
- An assessment of the broader control and change management framework.
- An internal review by 2LOD or 3LOD.
- An external review by an independent assurance provider.

Each of these types of assurance can be deployed and will be dependent upon the nature of the vulnerability and the remediation (e.g., size, complexity, materiality).

Assurance is distinct from validation with the latter being focused on the testing and monitoring of the remedial actions compared to the former, which is an independent review and challenged, performed independently of the remediation team.

Key steps for success are:

- **Scope**. Coverage can focus on part or all of the lifecycle, dependent upon where the concerns or risks have been identified.
- **Criteria.** Assessment should be made against set criteria or measurements. This is key for ensuring the recipient of the review findings to understand the evaluation and how conclusions have been reached. Criteria will be dependent upon the subject matter under review. It will need to include materiality factors

to indicate which criteria are more important than others. They may already be established or need to be established for a specific engagement.

- **Evidence.** Evidence of the fundings needs to be gathered, it needs to be appropriate and suitable. This evidence will support the assessment against the set criteria. Appropriate evidence reduces the risk of material misstatement / incorrect conclusions.
- **Reporting.** The report will need to have the following:
    - Scope
    - Approach
    - Timing
    - Criteria
    - Assessment against criteria
    - Evidence
    - Findings
    - Funding / investment assessment
    - Conclusions

### Closure

Closure is the formal sign off, approving that no further work is required, and the vulnerability has been appropriately treated. Only when assurance (if required) has been successfully completed, can there be formal closure of the programme of work.

Closure should be supported by a report summarising and justifying why the vulnerability can be concluded and closed. The report would typically include details of the vulnerability, the approved remediation plan, confirmation of activities undertaken with relevant evidence, the outcomes, and be signed off by:

- 1LOD team responsible for the work.
- 2LOD team responsible for the risk.
- The IBS owner.

Presentation may be required at relevant risk committees or at a minimum to be noted as part of the periodic update on IBS provided at the relevant risk committees.

# 7 Embedding

## 7.1 Overview

This section aims to guide firms in incorporating operational resilience into their organisational framework. This approach aligns with the industry's movement towards integrating operational resilience into the daily operations of the firm.

The objectives and principles below aim to facilitate a consistency of approach that can be adopted across the industry.

### Section Objectives

- To assist firms in incorporating operational resilience into their organisational framework.
- To provide best practice guidance for embedding operational resilience into BAU activities.

### Regulatory context

The UK authorities have been explicit that operational resilience is not a 'once and done activity', or something that should be seen as 'tick-box regulatory compliance' but should instead be a way of working that is embedded into the overall culture of the firm. The most effective operational resilience frameworks have been observed as those which are embedded within a firm's overall enterprise-wide risk frameworks, achieved through the following:

- Management reporting and accountability aligned to IBSs.
- Alignment of approaches in the development of ICAAP and SBP scenarios.
- Integrating IBSs and ITOLs to existing operational risk, cyber, IT and third-party risk management policies, procedures and practices.
- Enhanced governance structures and risk committees to consider operational resilience.
- Using existing risk management frameworks to identify and address new vulnerabilities that could breach ITOLs.

In addition, effective operational resilience frameworks have also been observed as those which are embedded into firms' change management and strategic planning frameworks, with operational resilience being a core consideration for firms when assessing transformation and change risks. To achieve this, firms are expected to develop their resilience strategy (e.g., by strategically incorporating "resilience by design" principles when considering new IT solutions, architecture platforms, and making procurement or outsourcing decisions) and consider design solutions and governance to ensure new investments are resilient through defined standards and policies.

### Guiding Principles

**P.1 Firms should integrate operational resilience requirements into their existing governance and risk frameworks.**

**P.2 Firms should strive to build a culture of operational resilience.**

## 7.2 Integrating resilience into governance and risk frameworks

Integrating operational resilience into governance and risk frameworks supports the embedding of resilience into the firm's strategic decision-making and risk management, and supports the firm to prepare for, respond to, and recover from disruptions whilst maintaining IBSs.

The most effective operational resilience frameworks are embedded within firms' overall governance and enterprise-wide risk frameworks. Where possible, existing non-financial risk and enterprise-wide risk frameworks should be leveraged to integrate operational resilience considerations into holistic business-as-usual activities and risk management practices.

### Governance and Oversight Structure

- Firms should have a defined governance structure that assigns appropriate internal accountability to Board members, senior management / executive committees and key risk functions, and that can support regulatory submissions as and when required by the authorities.
- The Board sets the strategic direction for operational resilience across the firm and is responsible for making prioritisation and investment decisions to meet the operational resilience requirements.
- The regulation requires a firm's Board to approve the operational resilience self-assessment at least annually.
- Under the authorities' Senior Management Regime (SMR), every Senior Management Function (SMF) must have a 'Statement of Responsibilities' (SoR) that clearly states the function's responsibilities and accountabilities. The Chief Operations function (SMF24) is responsible for the internal operations and technology of the firm, which includes responsibility for the firm's operational resilience, and which is commonly fulfilled through a central team / function.
- Firms should leverage existing governance structures, to include appropriate Operational Resilience Committees / Steering Forums that have a defined escalation path to the Board. This will enable operational resilience information and updates to be reported efficiently and support with integration into corporate strategy.
- Utilising a Three Lines of Defence model:
    - The First line of Defence (1LOD) own resilience planning and execution at the functional / department level and is responsible for complying with the Operational Resilience requirements.
    - The Second Line of Defence (2LOD) is made up of the Risk / Control / Compliance teams that provide independent oversight of alignment with regulatory requirements and internal policies.
    - The Third Line of Defence (3LOD) is the audit function that provides independent assessment directly to the Board.

### Operational Resilience Reporting

- Board-level reporting at a minimum, should include reporting on recovery capabilities, resilience metrics, incidents and risk appetite.
- Firms should develop meaningful, and actionable metrics and consider a mix of leading metrics that are predictive and help to identify and anticipate risks and vulnerabilities, as well as lagging metrics that are outcomes focussed and help to validate the effectiveness of mitigation measures in place.

- Firms should consider metrics that link to ITOLs and risk thresholds (e.g., Recovery Time Objectives (RTOs), the maximum acceptable amount of time for restoring technology after an unplanned disruption) and Recovery Point Objectives, (RPOs - the maximum amount of data loss (measured by time) that is tolerable to a firm after an unplanned disruption)).
- When designing operational resilience metrics, firms should consider how they could:
  - Align metrics with business objectives and regulatory requirements.
  - Regularly review and update resilience metrics based on evolving risks.
  - Ensure data used for metrics is accurate, reliable and timely.
  - Use dashboards for real-time monitoring of resilience performance.
  - Regularly review and calibrate the metrics to ensure they remain relevant and effective; and
  - Automate the collection and analysis of metrics to improve efficiency and reduce manual effort.
- Internal reviews and audit reports should be presented to the committees that hold the relevant operational resilience accountabilities.

### Leveraging Non-Financial Risk (NFR) Management

Firms should identify which of their Non-Financial Risk (NFR) categories require operational resilience considerations and update relevant policies and procedures, ensuring that operational resilience outcomes and any specific requirements are clearly articulated. Given the interconnectivity, it is important that the articulation of any operational resilience requirements across different NFR documents are reviewed and considered holistically in order facilitate a comprehensive and coordinated approach.

While not intended to be an exhaustive list, it would be typical to see operational resilience requirements embedded in the following areas:

- **Change management and strategic planning** - operational resilience is a core consideration when assessing risks of transformation and change, in particular to support 'resilience by design' outcomes. This includes ensuring that changes are implemented in a way that minimises disruption and maximises the firm's ability to adapt and thrive in the face of uncertainty through building in redundancy, flexibility and diversity into change initiatives. Firms should consider how any change initiatives may result in new or altered IBSs, and reflect this in the resource mapping, and also consider the extent to which SBP scenario testing can be undertaken ahead of 'go-live'.
- **Non-Financial Risk (NFR) policies** – firms should consider how they can incorporate operational resilience outcomes in relevant NFR policies, especially where these are aligned to the operational resilience resources - people, processes, technology, facilities, and information. Particular focus should be given to:
  - **Outsourcing and Third-Party Management** – firms are required to understand how their outsourcing and third party dependencies support IBSs, and if these arrangements pose a threat to their operational resilience.
  - **IT Resilience / Disaster Recovery** – firms should consider the recovery arrangements in place for technology that underpins the delivery of IBS as part of their broader IT resilience strategies.
- **Business Continuity Management (BCM)** - effective BCM contributes to a firms' response and recovery capabilities. Consideration should be given to how the order of operational recovery prioritises IBS and

supports recovery strategies, how mapping of resources could be aligned, and how the scope of BCM testing may be able to support or complement SBP scenario testing.

- **Incident and Crisis Management** - effective incident response is critical to minimising the impacts of operational disruption and where an event disrupts a firm's ability to deliver IBSs within ITOLs, this is expected to meet test for regulatory notification.
- **Recovery and Resolution planning** – operational resilience needs to be maintained even in a resolution scenario, and so consideration should be given to any synergies with Operational Resilience in Resolution (OCiR) requirements, in particular how mapping of resources and assessments of criticality could be aligned, and how testing may be coordinated.

Operational resilience should be detailed within a firm's risk and control assessment (RCA), both for businesses areas managing the associated risks, and for any central team that coordinates operational resilience activities.

### Leveraging Enterprise-Wide Risk Management

Firms should review their existing Enterprise-Wide Risk Management (EWRM) toolset to leverage operational resilience insights, examples could include:

- **Risk Appetite** - ITOLs differ from risk appetite, in that ITOLs assume a particular risk has crystallised instead of focussing on the likelihood and impact of operational risks occurring, and so it is expected that risk appetite will be exceeded in SBP scenarios even if a firm has remained within ITOL. There is still benefit, however, from firms considering how they can use their risk appetite to support achieving operational resilience outcomes, as both risk appetite and ITOLs help to ensure a firm's operational resilience.
- **Horizon scanning and Material Risk Inventories** - it is important that firms have a means to monitor how their environment is changing and whether this will give rise to different vulnerabilities. Horizon scanning for disruptive risks and events should be considered through the lens of potential SBP scenarios in order to inform operational resilience testing plans, as well as to identify where lessons learned analysis may be beneficial to the firm. Consideration should also be given to the interconnectivity of emerging risks and events and the firm's material risk inventory to ensure that new or changing exposures are identified.
- **Regulatory Mapping** – firms should consider maintaining a means of tracing the specific operational resilience regulatory requirements to their own policies, procedures, processes and/or controls. Regulatory mapping can be used to identify compliance gaps, areas for maturity, impacts of change initiatives, and can also be used to support assurance or audit activity.

### Key Integration Principles:

- **Alignment, not Duplication**: Avoid creating separate operational resilience processes. Integrate requirements into existing frameworks, adapting them where necessary.
- **Proportionality**: Tailor the integration approach to the size, complexity, and systemic importance of the firm.
- **Focus on Impact:** Prioritise identifying and managing risks to IBS and their potential impact on consumers and market integrity.
- **Ownership and Accountability:** Clearly define roles and responsibilities for operational resilience across all relevant business areas.

- **Continuous Improvement:** Regularly review and update the integrated framework to reflect changes in the business, regulatory landscape, and threat environment.

## 7.3 Building a Culture of Operational Resilience

Operational resilience should be more than just a strategy within a firm; it should be part of the organisational DNA, where every employee understands their role in maintaining and enhancing the firm's ability to anticipate, prevent, adapt, respond to, recover, and learn from internal or external disruption.

Culture can be defined as shared attitudes, beliefs, values and norms that shape behaviours and outcomes within a firm.

Building a culture of resilience involves integrating operational resilience into the core values, practices, and mindset of the organisation. It should not be seen as a one-off task, but a continuous commitment that requires sponsorship from the top, integration into daily operations, and continuous adaptation to new risks and regulatory demands.

A number of practices are listed below that firms should consider embracing and embedding as they strive to build a culture of operational resilience.

### Senior Management and Board Commitment

Senior management and the Board must visibly champion operational resilience. This involves setting the tone from the top by setting and regularly reviewing the operational resilience strategy, integrating operational resilience into strategic goals, values and regularly communicating its importance throughout the firm.

Senior management and the Board must also ensure that sufficient budget and resources are allocated, not just for compliance, but for enhancing resilience capabilities within the firm (e.g., investing in technology solutions to support monitoring, analytics, and automation to enhance early warning systems for potential operational disruptions).

### Operational Resilience Education and Awareness

Regular and targeted firm-wide training and awareness programmes should focus on the importance of operational resilience, real-world examples, and the potential impacts of failure. This includes both theoretical learning and where possible, for those with specific operational resilience responsibilities practical learning and education exercises.

### Cultural Integration

Firms should consider aligning performance management measures with operational resilience goals to encourage positive behaviours that support embedding operational resilience within the organisation and its culture. This should be particularly relevant for any defined roles with key responsibilities or accountabilities for operational resilience within the firm.

Firms should also strive to encourage openness and foster a culture where staff feel comfortable reporting issues, risks or potential vulnerabilities without fear of reprisal.

### Industry and Regulatory Collaboration

Collaboration with industry peers and regulatory bodies is pivotal in embedding a culture of operational resilience within UK financial services firms. In line with regulatory expectations, firms should look to proactively engage with industry peers to discuss and share best practices, whilst being mindful of other conduct legislation such as competition law.

Engaging with industry and sector bodies like UK Finance and CMORG, or regulatory bodies such as the PRA and FCA helps to cultivate a shared understanding and approach to operational resilience. Collaborative engagement can also help enable firms to anticipate emerging risks, collectively elevate industry standards, and foster a more resilient and trustworthy financial ecosystem.

Through these interactions, firms gain access to collective knowledge, participate in joint resilience exercises, and contribute to shaping regulations that are both practical and effective. This not only ensures alignment with regulatory expectations but also promotes a culture where resilience is seen as a collective endeavour, fostering an environment where employees are regularly exposed to best practices, emerging threats, and innovative resilience strategies.

### Feedback, Measurement and Continuous Improvement

It is important that firms embrace continuous improvement, conduct thorough reviews to learn from incidents, and treat operational resilience as an evolving practice, not a one-time setup, adapting to new and emerging risks, threats and technologies.

Firms should strive to have mechanisms in place to assess the operational resilience culture within the organisation. By understanding the strengths and areas of improvement in their practices and behaviours, they can take targeted actions to build and maintain a robust culture of operational resilience.

# 8 Self-Assessment

## 8.1 Overview

### Section Objectives

- To assist firms in documenting a written self-assessment of their compliance with the operational resilience regulations (FCA PS21/3 and SS1/21).
- To provide firms with insight on the information to be documented in their self-assessment, enabling them to provide their Boards and senior management with assurance of their ability to deliver their IBSs within ITOL.

### Regulatory Context

The UK authorities require that firms document, and keep up to date, a written record (in the form of a self-assessment) of their compliance with the operational resilience regulations (FCA PS21/3 and PRA SS1/21) and the requirements set out. Firms' Boards are accountable for and required to approve the information provided in the self-assessment. In delivering this responsibility, firms' Boards must regularly review assessments of their IBSs, ITOLs, and the scenario analyses of their ability to remain within ITOL for these IBS.

The information documented within a firm's self-assessment should include, but not be limited to, the following:

- A list of **IBSs** identified by the firm, and justification for any inclusions / exclusions.
- The associated **ITOLs** and justification for the level at which they have been set.
- The firm's approach to **mapping**, and how that mapping has been used to identify vulnerabilities and to support testing activity.
- Details of the firm's strategy / plan for **scenario testing**, including description and rationale for the scenarios tested, the types of testing undertaken, and any scenarios identified under which the firm could not remain within their ITOLs.
- Any **lessons learned** when undertaking scenario testing or via practical experience (e.g., through incidents), and actions taken to address issues or risks.
- Details of any identified **vulnerabilities** that threaten the firm's ability to deliver its IBSs within ITOLs, including actions taken or planned, and justifications for the completion time.
- An explanation of the firm's **communication strategy**, and how it will enable the firm to reduce anticipated harm.
- For CRR consolidation entities (in the case of UK banking groups) or an insurer (in the case of UK insurance groups), to cover any identified risks to their ability to deliver IBSs within ITOLs arising from elsewhere in the group.

### Guiding Principles

P.1 **Whilst there is no set template, a firm's self-assessment should be written in a format which provides their Board and senior management with assurance of their firm's ability to deliver its IBSs within ITOLs. It should also clearly document any concern over the firm's ability to remain**

**within ITOL, and detailed information on the work needed to remediate any vulnerabilities and issues.**

P.2 **As a minimum, the self-assessment must include the information as set out in the operational resilience regulations, and should include justification and rationale for determinations, decisions and plans to ensure the firm's continued resilience.**

P.3 **Firms should also consider including any additional information needed to achieve P.1 above and to ensure appropriate and fully funded plans are developed to remedy identified vulnerabilities.**

P.4 **The self-assessment should be approved by the firm's Board at least annually. The firm's Board must also regularly review (e.g., quarterly) assessments of their firm's IBS, ITOLs, and the scenario analyses of its ability to remain within ITOL for these IBSs.**

P.5 **The self-assessment should be kept up to date, reflecting key framework and methodology enhancements, and any material changes to their firm's operational resilience position (including any changes to their IBSs, ITOLs and mapping) and roadmap to resilience. The self-assessment should also mature and develop over time as the firm develops their resilience, response, and recovery capabilities.**

## 8.2 Structuring the Self-assessment

Whilst the structure, content and level of detail provided in a firm's self-assessment should be specific to the firm and proportionate to the nature, scale and complexity of the firm's activities, the following information should be considered for inclusion (either in the main body of the self-assessment, or as supporting information):

### Executive Summary

- A clearly defined scope of what is / is not covered by the self-assessment (e.g., legal entities, business functions, etc.), and for dual regulated firms, whether it is intended to address FCA PS21/3 and PRA SS1/21 collectively or separately.
- A purpose statement for the self-assessment, including a clear articulation of any decisions expected of / made previously by the Board, including:
  - Approval of the firm's written self-assessment of its compliance with the operational resilience regulations (FCA PS21/3 and PRA SS1/21) and the requirements set out.
  - Approval of the IBSs identified for their firm and the ITOLs that have been set for each of these.
- A high-level overview of the information documented within the self-assessment, including key activities undertaken in the year and any key lessons learned / vulnerabilities identified / addressed.
- A high-level summary of the key changes / enhancements made to the firm's approach to operational resilience since the previous self-assessment.

### Governance

- An overview of the firm's operational resilience framework (or similar) and how this integrates with other frameworks across the organisation (e.g., third party risk framework, enterprise-wide risk management framework, etc.). Include reference to the documented methodologies used by the firm to undertake their operational resilience activities, and a high-level description of each. Detailed methodologies should form part of the supporting information.

- The firm's governance structure for operational resilience, providing a high-level overview of key committees and forums (including decision-making mandate, purpose, aims and objectives, etc.).

## Important Business Services

- An overview of the firm's approach to identifying their IBSs, highlighting any key changes / enhancements made to the approach since the previous self-assessment.
- An overview of the annual review process, including information on governance route followed and key stakeholders involved.
- A list of the firms IBSs, including rationale and justification for inclusion. Highlight any material changes made since the previous self-assessment.
- A list of other business services which have not been identified as important, including rational and justification for exclusion (especially when choosing to remove an IBS following the annual review process). Highlight any material changes made since the previous self-assessment.

## Impact Tolerances

- An overview of the firm's approach to setting their ITOLs, highlighting any key changes / enhancements made to the approach since the previous self-assessment.
- An overview of the annual review process, including information on governance route followed and key stakeholders involved.
- An ITOL statement for each of the firm's IBSs. Highlight any material changes made since the previous self-assessment.
- A list of the firm's ITOLs (a time-based metric and other metrics where appropriate (e.g., a volume and/or value metric)) for each of its IBSs, including rationale and justification for the level at which they have been set (i.e. clearly articulate the point at which intolerable harm is reached, and why). ITOLs should be provided against each regulatory objective applicable to the firm (i.e. consumer protection, market integrity, the firm's safety and soundness, financial stability, policyholder protection). Highlight any changes made since the previous self-assessment.
- A description of any trigger events / insights (e.g., incidents, current and emerging risk assessments, scenario testing outputs, customer and market research, mergers and acquisitions, etc.) which have justified or altered the level at which the firm's ITOLs have been set, including any rationale for this.

## Mapping

- An overview of the firm's approach to mapping, highlighting any key changes / enhancements made to the approach since the previous self-assessment.
- A description of each 'resource' type, and for each:
  - the level of mapping completed (e.g., for Technology, the application and underlying infrastructure);
  - the scope of mapping (e.g., internal shared services); and
  - any exclusions, including rationale and justification.

- A list of 'golden sources' (master data sources) and any limitations and gaps when using these in mapping.
- A view of the resources critical to delivering each IBS, and cross-reference to any identified vulnerabilities and lessons learned.

## Scenario Testing

- An overview of the firm's approach to identifying scenarios for testing, highlighting any key changes made to the approach since the previous self-assessment.
- An overview of the types of testing used within the firm's scenario test plan.
- An overview of the scenario identification / planning process, including information on governance route followed and key stakeholders involved.
- The firm's scenario testing strategy / plan, including:
    - a description of each scenario and any underlying assumptions,
    - rationale for the scenarios tested.
    - the type of scenario tested (e.g., by cause, risk category, threat type, etc.)
    - planned and actual test dates.
    - whether each test is a retest.
    - the type(s) of testing undertaken for each scenario.
    - the IBSs tested in each scenario.
    - the resource types / resources tested in each scenario.
    - whether any third parties / direct market participants were tested, and their level of involvement (if any).
- Scenario testing outcomes for each scenario, including:
    - whether the firm could / could not remain within ITOL for each of their IBSs, with clearly articulated justification and rationale, and evidence to support this.
    - an assessment of which ITOLs were / were not breached, and by what extent (e.g., duration, volume, value, etc).
    - service recovery timescales for each of the firm's IBSs, including specific times of disruption and recovery where appropriate.
    - response plans tested (including communication strategy and plans) and to what extent, if any, they were able to reduce / mitigate the level of harm (i.e. to consumers, market integrity, the firm's safety and soundness, financial stability, and policyholder protection),
    - a detailed breakdown of the firm's ability to detect, recover, respond to, mitigate, and recover.
    - the level of assurance over, and any assumptions relating to actions taken by third parties / direct market participants (where included in the scope of the test), along with any rationale.
    - cross-reference to any identified vulnerabilities and lessons learned.

### Vulnerabilities, Lessons Learned and Remediation

- An overview of progress made in addressing issues, risks or vulnerabilities documented within the previous self-assessment, including details of any remediation actions closed or in progress.
- A dashboard of any key resilience indicators which provide insights into potential vulnerabilities, aligned to resource type and/or IBS.
- Details of any identified vulnerabilities or lessons learned through mapping, scenario testing and via practical experience (e.g., through incidents) that threaten the firm's ability to deliver its IBSs within ITOLs.
- Remediation actions taken or planned to address any issues, risks or identified vulnerabilities, including:
    - a description of each action.
    - action owner.
    - actual or planned completion date.
    - action completion date, and justifications for completion time.
    - details of the level of investment or funding required / committed.

### Embedding operational resilience into the organisation

- Tangible examples of how the firm has embedded operational resilience into the culture of their organisation, including demonstrable evidence of senior management and Board commitment.
- Details of how the firm has embedded operational resilience into their firm, with consideration to the factors in Section 7 of this Guidance.

### Additional supporting information and appendices

- Detailed methodologies used by the firm to undertake their operational resilience activities.
- Dashboards which provide information and insights into the effectiveness of resilience across the firm, including key resilience indicators and other performance indicators.
- Any operational resilience maturity frameworks used within the firm, including a self-assessed position against these.
- Any additional information needed to support the firm's Board in approving the self-assessment.

# Appendix A: Abbreviations

| | |
|---|---|
| BAU | Business As Usual |
| BCM | Business Continuity Management |
| CMORG | Cross Market Operational Resilience Group |
| CNI | Critical National Infrastructure |
| CRR | Capital Requirements Regulation |
| CTP | Critical Third Party |
| D-SIB | Domestic Systemically Important Bank |
| DORA | Digital Operational Resilience Act |
| FCA | Financial Conduct Authority |
| FMEA | Failure Modes and Effects Analysis |
| FMI | Financial Market Infrastructure |
| FPC | Financial Policy Committee |
| IBS | Important Business Service |
| IGBS | Important Group Business Service |
| ICAAP | Internal Capital Adequacy Assessment Process |
| ITOL | Impact Tolerance |
| ORCG | Operational Resilience Collaboration Group |
| O-SII | Other Systemically Important Institution |
| PRA | Prudential Regulatory Authority |
| RRD | Recovery and Resolution Directive |
| RTO | Recovery Time Objective |
| RPO | Recovery Point Objective |
| SIFI | Systemically Important Financial Institution |
| SBP | Severe But Plausible (or Extreme but Plausible for FMIs) |
| SME | Subject Matter Expert |
| SLA | Service Level Agreement |
| SPOF | Single Point of Failure |

# Appendix B: Key Reference Material

## UK Authorities

- PRA’s Supervisory Statement SS1/21 ‘Operational resilience: Impact tolerances for important business services’
- PRA’s Supervisory Statement SS2/21 ‘Outsourcing and third party risk management’
- PRA’s Statement of Policy ‘Operational resilience’
- FCA’s Policy Statement PS21/3 ‘Building operational resilience: Feedback to CP19/32 and final rules’
- FCA’s ‘Operational resilience: insights and observations for firms’
- The FPC’s macroprudential approach to operational resilience

## Cross Market Operational Resilience Group

- CMORG Dynamic Scenario Library