CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

Guidance for Firm Operational Resilience

Version 2 | November 2023

TLP CLEAR

Contents

1 Introduction to the Guidance for Firm Operational Resilience 3

1.1 Purpose of the Guidance 3

1.2 Defining operational resilience 3

1.3 Definitions 4

2 Identifying Important Business Services 6

2.1 Phased approach for identification of IBS 6

2.2 Visualising the service relationship with processes and Resources 7

2.3 Defining business services 8

2.4 Defining Important Business Services 9

2.5 Governance, accountability & management of an IBS 11

2.6 Decision workflow for identifying IBSs 12

3 Impact Tolerances 15

3.1 Overview 15

3.2 Impact Tolerance examples 16

3.3 Testing Impact Tolerance Statement under Severe but Plausible scenarios 17

4 Mapping and assessments 18

4.1 IBS mapping 18

4.2 Special considerations for mapping Information/data 21

4.3 Resilience vulnerability assessments 24

5 Scenario testing 27

5.1 Scenario testing overview 27

5.1.1 Assessing scenario test results against Impact Tolerances 28

5.1.2 General guidance for developing a scenario testing plan 29

5.1.3 Fundamental principles for scenarios 30

5.2 Scenario testing approach 32

5.2.1 Define the scenario 32

5.2.2 Test ability to remain within Impact Tolerance 35

5.2.3 Assessing test outcomes 39

5.3 Scenario themes 40

6 Self-Assessment 54

6.1 Executive summary 54

6.2 Governance 55

6.3 Business services 55

6.4 Impact Tolerance 56

6.5 Service mapping 57

6.6 Scenario testing 57

6.7 Vulnerabilities, lessons learned and remediation 58

6.8 Embedding into the organisation 59

6.9 Appendices 60

Appendix A: Abbreviations 61

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, ORCG had commissioned the development of guidance for its members to assist with interpretation or implementation of these policies. ORCG then agreed at the end of 2022 to commission a refresh of the Guidance.

1.1 Purpose of the Guidance

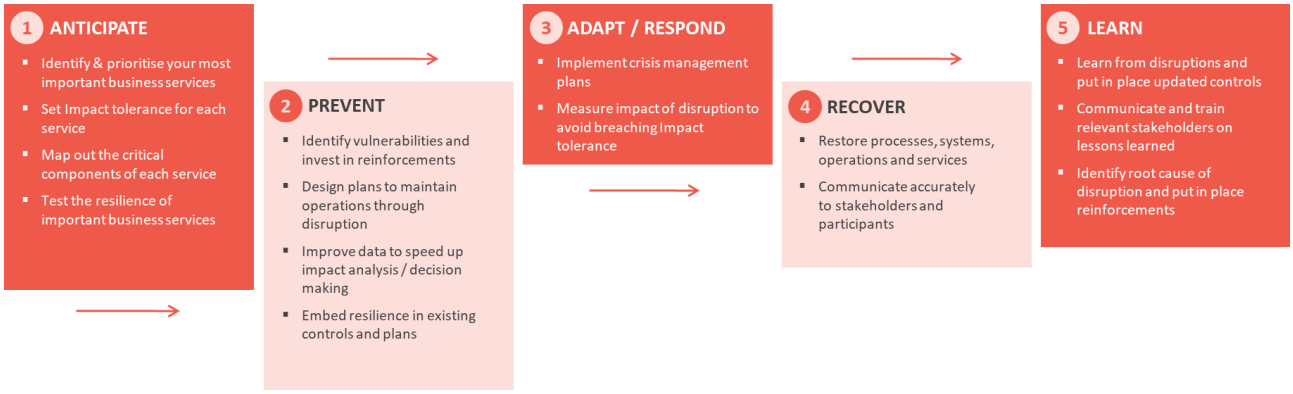
Following on to the development of the original guidance produced in 2021, this document provides an **update** to firms on the guidance to implementing operational resilience.

The guidance incorporates the key requirements set out by the UK regulators for implementing operational resilience into firms. The content should be considered as high-level principles that can be used proportionately by a firm accordingly to their size, scale and complexity. It is not intended to be prescriptive or mandatory, but rather to support completion of individual firm documentation that aligns to the organisation's 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 IBS to customers and clients, and minimise any impact on the wider financial system when, not if, disruption occurs'*.

Figure 1. Lifecycle of an incident



1.3 Definitions

Term	Definition
Business Continuity Management[1]	Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
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[2]	These are activities, services, or operations the discontinuance of which is likely in one or more Member States, to lead to the disruption of services that are essential to the real economy or to disrupt financial stability due to the size, market share, external and internal interconnectedness, complexity or cross-border activities of an institution or group, with particular regard to the substitutability of those activities, services, or operations.
Severe but Plausible (SBP) Scenarios	Scenarios that would result in a high impact and significant disruption, and while have a low likelihood occurring, remain plausible.
Important Business Services (IBS)[3]	A service provided by a firm, or by another person on behalf of the firm, to one or more clients of the firm which, if disrupted, could: 1) cause intolerable levels of harm to any one or more of the firm's clients; or 2) pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets
Impact Tolerance (ITOL)[4]	Means the maximum tolerable level of 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 holder or pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets
Intolerable harm[5]	Intolerable harm is something from which customers cannot easily recover, e.g., where a firm is unable to put a client back into a correct financial position, post-disruption, or where there have been serious non-financial impacts that cannot be effectively remedied.
Mapping	The process of identifying and documenting the processes that underpin IBSs, and the Resources that are critical to the delivery of these processes.

[1] BCI Glossary

[2] Critical Functions: SRB Approach

[3] important business service - FCA Handbook

[4] impact tolerance - FCA Handbook

[5] PS21/3: Building operational resilience: Feedback to CP19/32 and final rules (fca.org.uk)

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: A. the type of product, type of policyholder, and their current or future interests; B. the significance to the policyholder of the risk insured; C. the availability of substitute products that would offer a policyholder a similar level of protection; and D. 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 & Soundness[6]	Firms having resilience against failure, now and in the future, and avoiding harm resulting from disruption to the continuity of financial service.
Scenario testing[7]	Assess the ability to remain within the Impact Tolerance for each of its Important Business Services in the event of a Severe but Plausible disruption of its operations.
Vulnerability assessment	Identification of vulnerabilities and/or weaknesses in the delivery of an IBS within Impact Tolerance through assessment of how the failure of a Resource or process could impact the IBS.

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

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

2 Identifying Important Business Services

2.1 Phased approach for identification of IBS

The following is intended to assist firms in their approach to identifying business services and Important Business Services under PRA PS 6/21 and FCA PS 21/3.

Stage	Activities	Output
1. Information Gathering	• Obtain existing list of Critical Functions / Critical Economic Functions and Core Business Lines – if available/ applicable. • 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. • Discuss selections at industry level, if possible, to ensure consistency and appropriate levelling.	• Longlist of business services.
3. Determine Importance	• Define criteria for assessing importance of the service based on the intolerable harm to consumers, market integrity, financial stability, Safety & Soundness and, if applicable, Policy holder protection. • Leverage the industry principles; criteria used should be firm-specific. • Use assessment criteria to identify IBSs. • Define group IBSs where these exist[8]. • Obtain internal sign off from relevant stakeholders on the understanding that the selections made are subject to change.	• Shortlist of IBSs with demonstrable supporting evidence and rationale for the selections made.

[8] To establish the Group Important Business Services, the following conceptual steps are suggested:

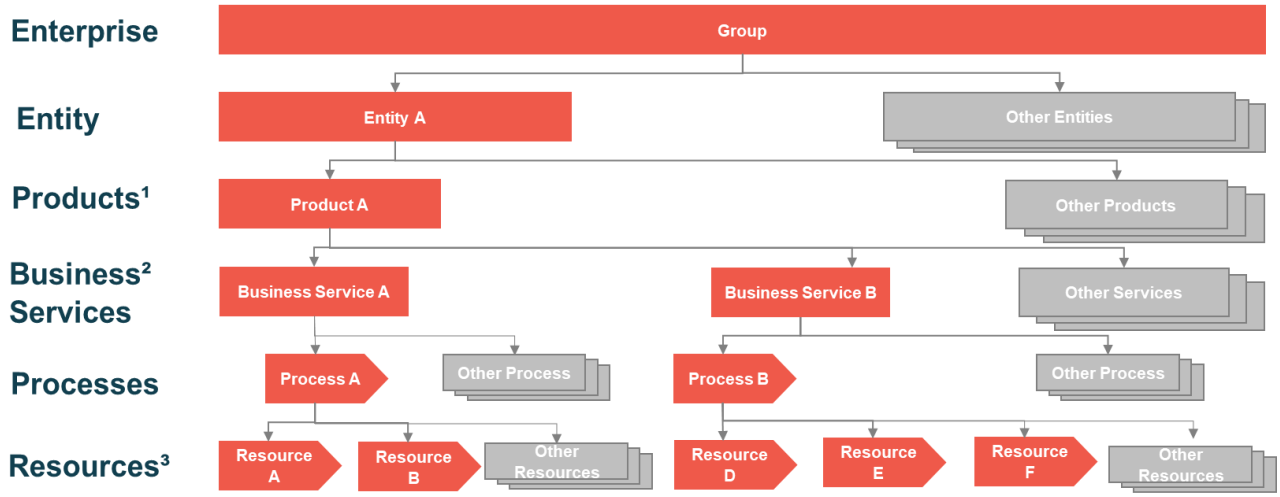
- For the institution's CRR entity/entities authorised by the PRA, establish the applicable UK Holding Company if such exists.
- If a UK Holding Company exists, all the Firms under that Holding Company must be established.
- For each of these Firms excluding the CRR(s), the external services offered 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 a Group Important Business Service

4. Map and Assign Ownership	• Map IBSs and capture dependencies/ Resources - people, technology, data (information), facilities and third parties - which support delivery. • For identified Resources, define which are critical to the delivery of the IBS and why. • Define important (and group important) business service ownership model / owners.	• Process maps. • Business service owners and ownership model / responsibilities matrix. • Resource inventories.
5. Govern and Iterate	• Ongoing governance and assessment of Operational Resilience including Board approval and related senior management oversight • 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, Important Business Services, Impact Tolerances and lessons learned documentation.

2.2 Visualising the service relationship with processes and Resources

Figure 2 illustrates the basic relationship between Products provided to external users and related services, processes and Resources. For simplicity, we have consolidated certain nodes within this schematic; these are shown in grey.

Figure 2. Service Relationship



1. 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 & soundness, policyholder protection, or financial stability.
2. It is possible and acceptable that a specific business service could support multiple Products. For example, "client balance enquiry" could support multiple product offerings.
3. A Resource can support multiple Processes.

2.3 Defining business services

To support the financial services industry in identifying their IBS, a list of principles has been identified to support organisations defining a business service, an IBS, the appropriate levelling, and granularity of an IBS, and for the governance, accountability, and management of IBS.

These principles aim to facilitate a consistency of approach thus enabling a systemic understanding of the financial market ecosystem and cross-industry operational resilience collaboration.

P.1 A business service must have a clearly defined external end user / set of users ("customers & consumers") which allows for the identification of both distinct services and "instances" of such services where needed.

- This is to ensure we can understand the specific intolerable harm caused to the business service's consumers (direct and indirect) if the business service was disrupted.

P.2 A business service must be provided to an entity external to the firm or group. Shared and internal services that are fundamental to the provision of the business service should also be captured, mapped, 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 consumers on a stand-alone basis. Additionally, if a service has no consumer value on its own, then it is part of another business service.

- If a service cannot be offered to a customer without having to consume another service at the same time, then the articulation is probably 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 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. Example: 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. 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, for example an insurance providers' 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.

2.4 Defining Important Business Services

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 time period for the disruption of the business service is one mechanism that firms can use to ensure focus on its most IBSs although there should be evidential justification for such an approach. It should be noted the resultant 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 apply an appropriate level of resilience given 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.

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

- **Consumers.** Where the outcome of disruption passes significant inconvenience and harm and reaches an intolerable threshold. 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.
  iii. Impact to vulnerable consumers.

- **Market Integrity.** Where the outcome of disruption detrimentally affects:
  i. Another organisation's ability to function normally or…
  ii. The consumers of other organisations.
  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. Financial institution to lose its financial institution licence.
  iv. Run on the financial institution.

v. Extreme regulatory censure.

vi. Firm reputational impacts.

vii. 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 would 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.

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

Substitutability of service should not be used in isolation to determine whether a business service is, or is not, an IBS.

- Substitutability needs to be considered in a wider context as defined by the FCA and PRA.

- Business services will qualify as 'important' when their failure could cause an intolerable level of harm to consumers or market participants, harm to market integrity, or threaten policyholder protection, the safety and soundness of individual firms, or financial stability.

- The factors that a firm should consider when identifying its IBS in relation to intolerable harm to consumer or market participants are set out in FCA SYSC 15A.2.4. 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:

  i. SYSC 15A.2.4 sets out the factors that a firm should consider when identifying its Important Business Services. An Important Business Service 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 weighting than another, therefore substitutability does not out weight other factors on its own when identifying an IBS.

  ii. A service should be considered an Important Business Service if disruption to it could cause intolerance levels of harm to its customers. Even if the service is substitutable.

  iii. Firms should consider a particular service as an Important Business Service if they cannot be easily substituted in the market.

- The factors that a firms should consider when identifying its IBS where a disruption of the service threaten policyholder protection, the safety and soundness of individual firms, or financial stability are set out in SS1/21, paragraph 2.5.
    i. 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 on in SS1/21 paragraph 2.5 (c).
    ii. 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 makes it clear that if a firm's 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.
        a. Firms should not assume that other providers will step in to provide an IBS when identifying IBS and setting ITOLs. The PRA expects firms to consider the impacts of disruption before they are mitigated.
        b. Identifying a lack of substitutability from other market providers will be an important consideration for those firms required to consider financial stability, when identifying IBS 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:
    i. Where substitution is available, these procedures should be evaluated as effective mitigation to remain within ITOL during severe but plausible scenario testing. If a firm can prove effectiveness of substitutability during testing, it will help to make them more resilient.
    ii. Firms should also consider developing and testing alternative mitigating actions where substitution may not be possible, such as disruptions to critical third parties or financial market infrastructure, or where other market participants are likely to be disrupted simultaneously.

2.5 Governance, accountability & management of an IBS

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 important group business services and respective ITOLs at the level of the group. Important Group Business Services are those 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.

- 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 businessperson, at a senior level, within the organisation.

- Because 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 IBSs can remain within their Impact Tolerance. 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.

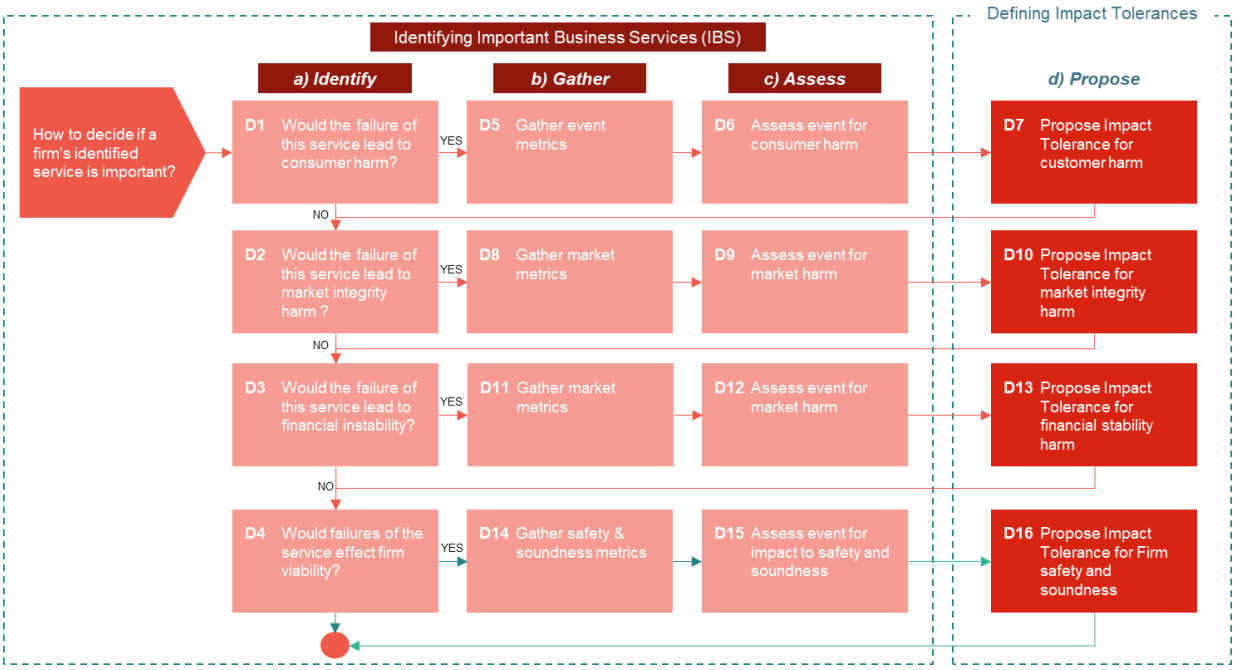
An organisation's IBSs should be reviewed on an annual basis, or as soon as practical, upon identification of a material change that has occurred, and approved by the organisation's Board or Governing Forum.

- 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.

2.6 Decision workflow for identifying IBSs

To support the Financial Services industry in identifying Important Business Services, a decision tree (as shown in **Figure 3**) has been constructed to support firms defining which services are IBSs.

Figure 3. Identifying an IBS



Decision 1

End-User Harm: Where the outcome of disruption passes significant inconvenience and is detrimental to one or more of the following:

- Physically or emotionally: disrupts access to basic needs e.g., food, utilities, transport, shelter.

- Financially: loss of income/earnings, charges incurred, loss of opportunity, settlement of debt, disruption of supply
- What's the impact to vulnerable consumers? How would the worsening of circumstances impact this?

Decision 2

Market Integrity: 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.

Decision 3

Financial Stability: 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, in particular the economic functions listed in SS19/13 Resolution planning.
- The potential to cause knock-on effects for counterparties, particularly those that provide financial market infrastructure or critical national infrastructure.

Decision 4

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

- Impact to capital.
- Financial institution to lose its financial institution licence or liquidity.
- Run on the financial institution.
- Extreme regulatory censure.
- Extreme firm reputational impacts.
- Loss of confidentiality, integrity, or availability of data.

Decision 5

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 from across a year to identify worst case scenario which considers known peak periods); how many of those are vulnerable (known).

- 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

Gather market integrity metrics.

- Are you a major provider in the market? (Using market share MI if available).
- 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

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

Gather safety & soundness metrics:

- Capital and liquidity information from recovery & 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

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

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

3 Impact Tolerances

3.1 Overview

Nature

- Defined at an IBS level; proportionate to an individual firm and its consumers / market share.
- Articulated in a clear, unambiguous, and easily consumable way; describes 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).
- The period of time is set to avoid intolerable harm manifesting to consumers, market integrity, safety & soundness/policyholder protection, and financial stability (collectively the "Regulatory Objectives".[9]).
- For each Regulatory Objective, the firm should identify all the different types of impacts that could arise if the IBS is disrupted. For example, value or number of transactions disrupted, lost revenue, & number of vulnerable customers affected.
- 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.
- 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.
- Assumptions used to define the Impact Tolerance statement should be transparent in the review/approval process.
- Impact Tolerances 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.

Context

- Relates to complete service disruption without the use of any mitigating action.
- The disruption analysis is cause-agnostic but should be set at the worst possible time/context in terms of impact.

Purpose

- Used to ensure, in events of disruption to IBSs, firm's ITOL thresholds are not exceeded. This is achieved by either complete recovery of the Service or utilisation of mitigating action (e.g., workarounds, service substitution).
- Used to drive investment in detective, preventative, response, and recovery strategies.

[9] Consumer protection and market integrity relate to the FCA; safety & soundness/policyholder protection, and financial stability relate to the PRA.

- Be measurable in a way that supports the ability of a firm to test its capability to remain within the Impact Tolerance thresholds in severe but plausible scenarios.

- A living and breathing statement, which should be 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 & qualitative metric*]

3.2 Impact Tolerance examples

Figure 4 is an illustrative example of setting ITOL by considering harm impact types and related metrics aligned to Regulatory Objectives.

Figure 4. Impact analysis of an Impact Tolerance

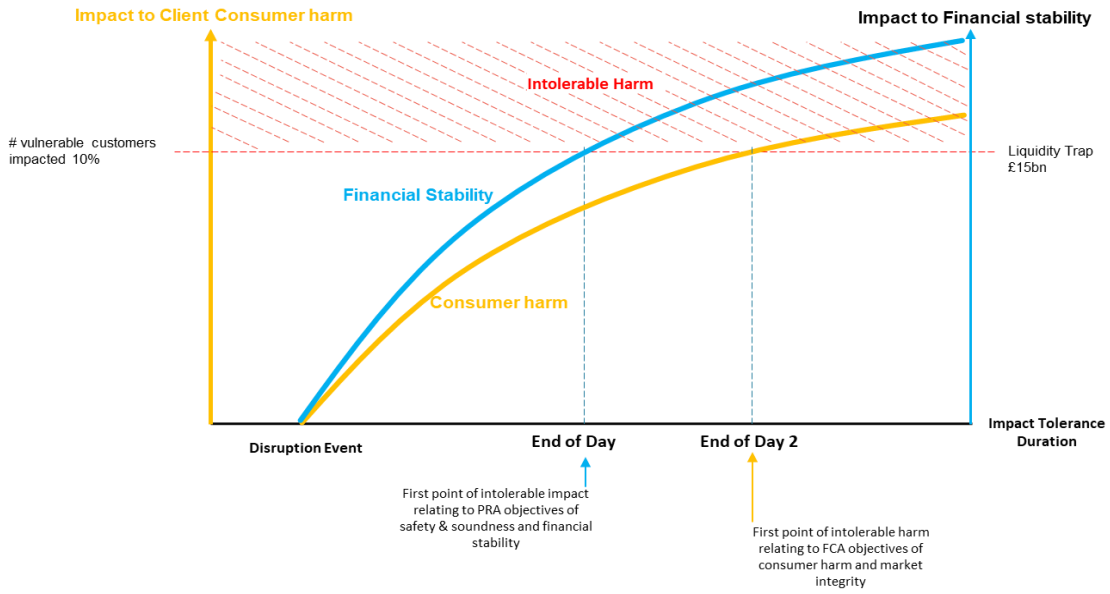
Impact Analysis – Prolonged Disruption of a Business Service				
Assessment Criteria	Examples - Factors firms consider assuming a firm's IBS delivery of high value payments through CHAPS is disrupted	Example – Metrics or Indicators	Intolerable Harm Threshold	Duration or time of day where the threshold may be breached
Harm to consumers	Vulnerable customers	# vulnerable customers affected	10%	End of day 2
	Customers in distress	# customers affected	10%	End of day 3
Market integrity	Clearing & settlement for Exchanges, CCPs	Value of payments to and from Exchanges / CCPs	£10m	End of day 3
Impact on Firm's Safety & Soundness	Failure to execute payments may impact profit & loss	Loss of business revenue	£200m	14 days
	Potential pay-out to customer claims & other liabilities	Value of filed transactions	£100m	c. 30 days
	Reputational damage	# clients affected and lost	20,000	c. 14 days
	Operational contagion	Knock on disruption to other firms, FMIs IBS	Any	End of day 3
Financial stability	Financial contagion	Liquidity stress (trapped)	£15b	End of day
		Financial loss incurred by other firms, FMIs	£100m	c. 5 days
	Loss of confidence	Significant price moves	c. 20%	Next day
		Withdrawal of deposits	c. 5%	Next day
Policy protection: policyholders affected by a disruption to the service	Agent bank for insurers	Value of payments to / from insurers	£100m	c. 30 days
				FCA Objectives / PRA Objectives

First point of intolerable harm relating to FCA objectives of consumer harm and market integrity

First point of intolerable impact relating to PRA objectives of safety & soundness and financial stability

Figure 5 shows, for the example above, how a disruption event unfolds over time for most time sensitive impact types relating to a) consumer harm and b) financial stability.

Figure 5. Identifying where intolerable harm unfolds



3.3 Testing Impact Tolerance Statement under Severe but Plausible scenarios

Scenarios testing is employed to establish whether a firm can achieve its Impact Tolerance Statement. Ultimately, SBP testing needs to demonstrate that the firm can meet its defined Impact Tolerances and therefore ensure material impacts are avoided.

- An ITOL Statement should be established according to quantifiable metrics that characterise intolerable harm across the themes of consumers, market integrity, safety & soundness/policyholder protection, and financial stability.

- The duration of an ITOL is set at the point where intolerable harm first occurs. Dual regulated firms should identify separate ITOL for their IBS where the delivery of that service is relevant to both PRA and FCA objectives.

- There are conceptually two ways to validate, against the firm's inventory of severe but plausible scenarios, that a firm can achieve its ITOL Statement.

- Firstly, the firm should demonstrate that it can recover the IBS within the duration of the ITOL Statement and in doing so ensures intolerable harm is avoided. However, recovery within the duration of the ITOL Statement may not be feasible or possible for a particular severe but plausible scenario.

- Secondly, if recovery of the IBS within the duration of the ITOL is not achievable for a particular severe but plausible scenario, the firm could then employ mitigation action to ensure intolerable harm is avoided. The firm needs to be able to invoke this mitigation within the duration of the ITOL Statement and in the context of the disruption caused by the scenario being tested.

- Should mitigation be employed, the firm needs to demonstrate that from the point of invocation to the point in time when the IBS can practically be recovered, the mitigation action avoids all forms of intolerable harm (assessed against all relevant quantifiable metrics/thresholds), and not simply that which manifest first.

4 Mapping and assessments

4.1 IBS mapping

Purpose

- To provide suggestions and principles to help firms mature their approach to the mapping of IBSs, Firms are encouraged to read the principles but develop their own mapping approach proportionate to their scale and complexity.
- To provide a high-level approach from scoping through to mapping, reviewing, and assessing for vulnerabilities, before presenting for governance.
- To define a set of principles which can be used to support these activities.
- To illustrate mapping using high-level diagrams and a fictional example.

Regulatory context

A firm must identify and document the people, technology, data (information), facilities and third parties necessary to deliver each of its IBSs. This must be sufficient to allow the firm to identify vulnerabilities and remedy these as appropriate (SYSC 15A.4.1 and PRA rulebook OR4.1).

Where a firm is reliant on a third-party for delivery of an IBS, it is expected that the firm will have sufficient knowledge of the processes and Resources that support the provision by the third party of the services the firm relies upon (SYSC 15A.4.2).

Firms were expected to have completed mapping by 31 March 2022, to a level of sophistication to identify IBS, defined ITOL and identify vulnerabilities, seeking further maturity beyond this date to maintain their Important Business Services within ITOL no later than 31 March 2025.

The regulators expect mapping to be updated annually or when material changes occur to the firm's business, an IBS or an ITOL. A material change (PRA 'significant change') is defined as 'a change that would negatively affect the firm's ability to use its mapping in order to meet these outcomes [identification of vulnerabilities and enablement of scenario testing]' (SYSC 15A.4.3).

Principles of mapping

P.1 **Firms must identify and document the Resources necessary to deliver its IBSs.**

P.2 **Mapping should be carried out with the aim of identifying vulnerabilities within end-to-end chains of activity and facilitating testing against ITOLs.**

P.3 **A Resource is to be included in the mapping if the risk of not including it is too high to be tolerated, i.e., if it could result in a breach of ITOL.**

P.4 **The approach to mapping should be proportionate to a firm's size, scale, and complexity.**

P.5 **Firms must have a consistent approach to mapping even though IBS are unique.**

P.6 Firms must create mapping documentation, e.g., templates and mapping diagrams, and include the rationale for inclusion of Resources, using 'golden sources' (master data sources) where possible.

P.7 Mapping documentation should be kept up to date and be subject to controls such as review and sign off by relevant stakeholders such as IBS owners (a RACI matrix may be useful).

Mapping process

Process flow for mapping Resources, assessing, and reporting vulnerabilities.

Stage	Activities	Output
1. Scoping	• Once IBS services have been identified and ITOLs set, use the IBS maps to identify the critical activities that underpin them. • 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. • The above Resources fall into the resilience pillars, but further granularity may be desirable depending on a firm's complexity. • Assess the criticality of each Resource at each step, e.g., could the unavailability of the Resource yield a breach of ITOL?	• For each IBS, list the Resources that support it, linked to the processes identified in stage 1.
3. IBS assessments	• For each resilience pillar, identify a set of resilience indicators that measure the resiliency of Resources in a consistent and repeatable manner. • Gather the necessary data to carry out vulnerability assessments at specified intervals. • Supplement the resulting MI with insights on the assessment results, accounting for changes in the resiliency position since the previous assessment	• Assessment outcomes including observed issues, vulnerabilities, and insights.
4. Scenario testing	• Select relevant SBP scenarios to assess the resilience, recovery, and restoration of IBS. • Continue to refine scenario testing in alignment with the mapping.	• Report outlining the results from testing and the proposals for remediation.

Mapping starts by identifying the end-to-end processes that are critical for the delivery of an IBS. To help identify these processes, firms may look at both their external and internal context. The external context includes emerging markets trends that might impact the IBS; by contrast, the internal context includes the firm's strategic direction as well as internal changes that might impact the IBS. Questions must also be asked around customer preferences and behaviours, such which products are considered primary, how customers prefer to interact with a firm e.g., digital, telephone, branch and which parts of a service are time critical.

As per Principle 6, 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 regulators. 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 SMEs and the relevant business areas.

A very simple, high-level map may be created roughly 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 protection and recovery Resources mapped to them. Firms may differ as to the inclusion of protection and recovery Resources as part of their mapping, given that the primary requirement for inclusion is the *delivery* of IBSs. However, one may argue that protection and recovery are also critical to the delivery of IBSs.

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

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.

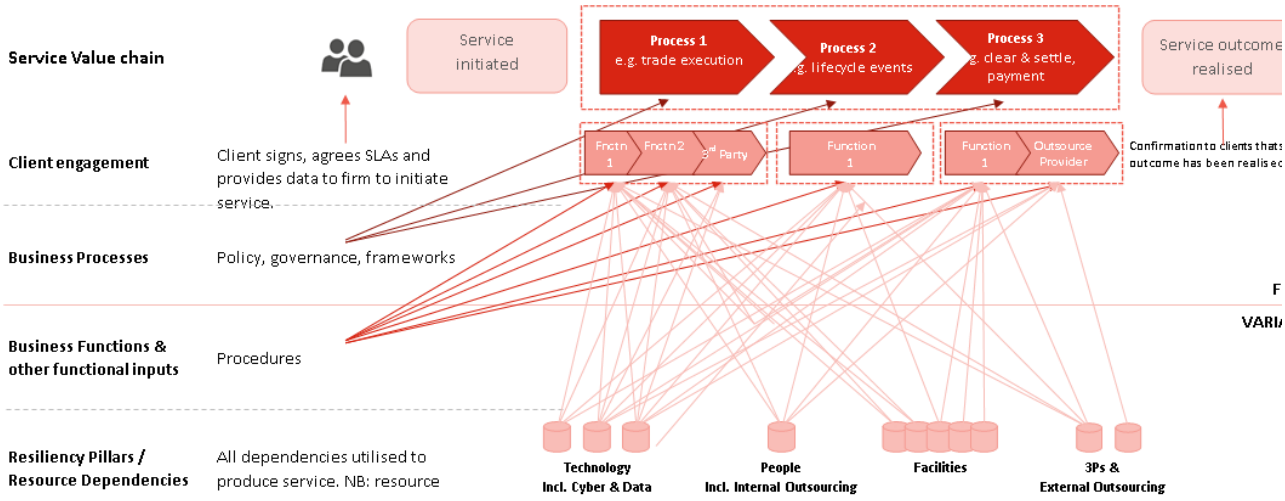
Mapping processes

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 of process



4.2 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 Important Business Service 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 Important Business Services.

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 FMEA, SPOF analysis may be considered) to ensure adequate confidentiality, integrity, and availability in relation to the defined ITOLs for the business service.**

Special considerations for critical information

The following considerations are relevant to assessing the resilience of information/data, where vulnerabilities may involve susceptibility to failure due to issues relating physical or logical design.

1. **Confidentiality, Integrity & Availability**
   To confirm that any existing information security standards have been appropriately applied, given the criticality of the IBS, particularly if changes in criticality have been identified through the mapping process. Additional vulnerability assessments may also be considered to confirm the robustness of existing processes.

2. **Recovery Objectives and capabilities**
   To confirm that the RTO and Recovery Point Objective (RPO) for data-related infrastructure failure scenarios would allow the IBS to remain within ITOL.

3. **Recovery plans and evidence of assurance activities**
   To confirm the reported capabilities have recently been exercised and that any post-test remedial activities have been completed.

4. **Known risks and issues and audit evidence**
   To confirm that pre-existing risks, such as outputs from risk and control assessments, have remediation plans in place that are owned, funded, and have the necessary governance in place.

5. **Information from previous related incidents**
   To confirm that problem records are in place, with a planned resolution for root causes of any major incidents.

6. **Design documentation**
   To confirm that appropriate levels of resilience to prevent service impacts have been built and tested, e.g., no single points of failure; load balancing; clustering; Failure Mode Effect Analysis, etc.

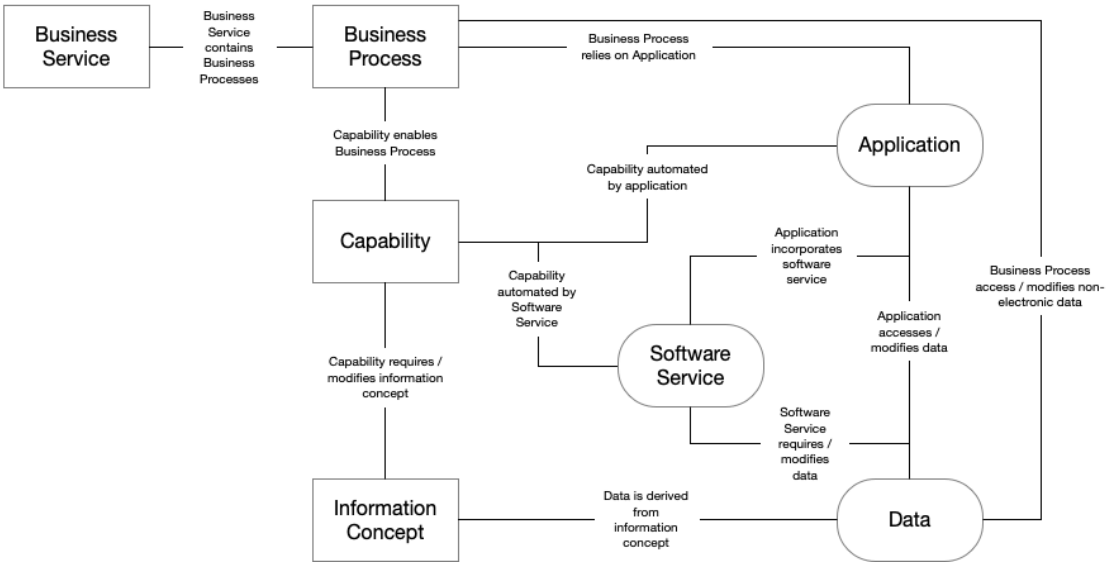
7. **Contractual dependencies which could impact the operation / maintenance or recovery of data**
   To ensure that there are no surprises when dealing with contracts, especially during an incident, where recovery times may be impacted.

8. **Immutable backups (copy of data that cannot be altered, deleted, or change in any way)**
   To confirm the availability and frequency of suitable immutable data backups, and how quickly they can be restored in a worst-case scenario.

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.

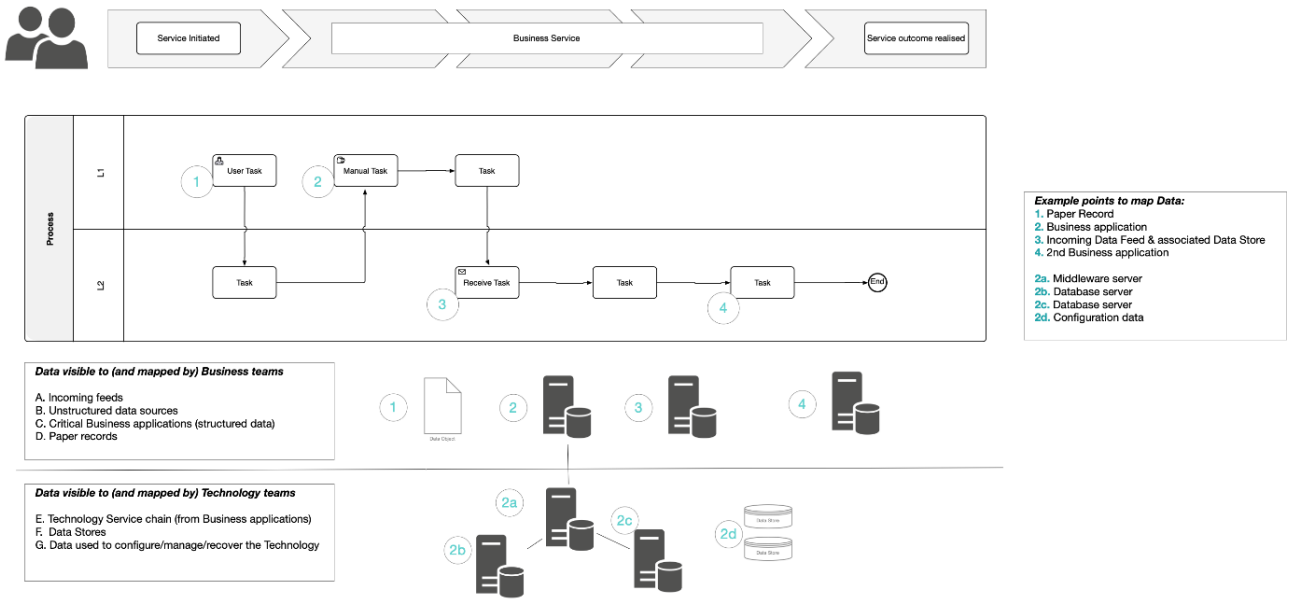
Figure 7. Business data model



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



4.3 Resilience vulnerability assessments

Critical Resources must be assessed to determine whether they are robust and fit for purpose, and for obvious vulnerabilities. When performing assessments, firms should use their own existing best practice guidance and methodologies, but as a starting point the following details could be captured and assessed.

Vulnerabilities may be seen as falling into two categories:

- Corporate or enterprise vulnerabilities that affect all IBSs. Risks to these will be reported and tracked by the managing area, e.g., technology or facilities.
- 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.

Principles

P.1 **Vulnerability assessments should set out to identify and assess vulnerabilities and areas for improvement. They should support the design of suitable test scenarios, should without mitigation have the potential to cause an ITOL breach, highlight the key areas for improvements and investment, and ultimately drive improvements in a firm's resiliency position.**

P.2 **The assessments should aim for consistency and repeatability. This may be achieved by assessing Resources in each resilience pillar against a set of common resilience indicators. Although resilience indicators are not mandated by the regulators, they help to provide oversight on a firm's resilience.**

P.3 **The aim of resilience indicators is to ask whether mapped Resources are fit for purpose. These indicators, jointly with high-level metrics and insights, inform current state and provide an input**

into resiliency 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 resilience lens, asking whether it provides any insight into the resilience of delivering the IBS.

P.5 As with scenario testing, vulnerability assessments should be designed to help determine the impact of disruption when Resources are not available. They should be designed to provide assurance as to whether IBS can remain within ITOL.

P.6 Assessments should be conducted on a regular basis (frequency defined by the firm) to track changes in a firm's resiliency position, and when significant changes take place such as mapping changes.

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 IBS and return to normal promptly following disruption. Vulnerability assessments are therefore best seen as a continuous cycle of assessment, learning and improved maturity.

Examples of 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 business. Hence, 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.

Resource pillar	Resource type	Performance indicators (lagging)	Conformance indicators (leading)
People	• Primary teams • Alternate teams	• Updated, known & accessible incident management & continuity/recovery procedures/documents. • Business Continuity plans for each area signed off and exercised. • Absence statistics for key roles • Suitably Qualified and Experienced Persons (SQEP) • Work area recovery • Availability of key people • Responsiveness of Op Res response system	• Staff turnover (FTE and contracted) • Performance management • Engagement and retention • Knowledge management • Succession plans • Insider threat • Cross-skilling • Availability of contingent staff/assets • Education & training of risks, mitigation & contingencies

Facilities	• Office sites • Contact centres • Data centres	• Key utility outages • Generator design, e.g., backup power source • Network provision • Air conditioning provision for data centres • Physical security • Fire safety	• Location risk/Natural disaster (flood, fires etc.) • Statutory compliance
Technology	• Systems / applications • Desktop builds • Supporting infrastructure	• Patching coverage rate • Frequency & severity of outages • Mean Time to Resolution (of service outages) • System availability • System downtime • Network spikes and utilisation bursts • Network performance • Service Level Agreement (SLA) conformance • Business services without a defined SLA • Service provider SLA conformance • Systems running without maintenance support • Volume of changes, e.g., unplanned changes • Backup and restore procedures • Incidents • Malware scanning & security conformance	• End of Service Life & support period • System capacity • Network availability • Network bandwidth • Monitoring • Errors where root cause unidentified • ITDR • Data recovery • Data privacy • Critical data not digitised • Technical debt (functional) • Penetration testing • Vulnerability scanning • Access management • Open security dispensations • Obsolescence
Processes	• Key stages • Actions	• Nonperforming processes (Audit) • KPIs & or KRIs as relevant to the service for trend analysis and to correlate IBS impact from incidents	
Third parties	• Important outsourced products / services	• Test of exit arrangements • Control testing • BC/DR Plans complete and accurate	• Switching impact • Concentration risk • Location risk • Financial health

5 Scenario testing

5.1 Scenario testing overview

Purpose

- To assist firms in testing their ability to remain within their Impact Tolerance(s).
- To provide suggestions and principles to help firms mature their approach to scenario testing.

It is not a best practice guide - each firm will need to develop their own testing approach proportionate to their scale and complexity.

Regulatory context

The UK regulators propose that *"firms should test their ability to remain within their ITOLs for each of their IBSs in the event of a severe but plausible disruption of its operations. This enables them to be assured of the resilience of their IBSs and identify where they might need to act to increase their operational resilience."*

In addition, regulators propose that *"firms should develop a testing plan that details how they will gain assurance that they can remain within Impact Tolerances."*

This approach is reinforced in the Basel Committee on Banking Supervision (BCBS) Principles for operational resilience (Mar 2021): *"In formulating the bank's tolerance for disruption, the board of directors should consider the bank's operational capabilities given a broad range of severe but plausible scenarios"; "The approach and level of granularity of mapping should be sufficient for banks to identify vulnerabilities and to support testing of their ability to deliver critical operations through disruption."*

Purpose of scenario testing

Scenario testing is used to understand and identify opportunities to improve the resilience of an IBS considering a range of severe but plausible scenarios. Scenario testing is about validating the effect detection, response, and recovery actions have on mitigating the harm factors that underpin the ITOL of 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 Impact Tolerances (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 Impact Tolerance or is investment required to develop a new capability?

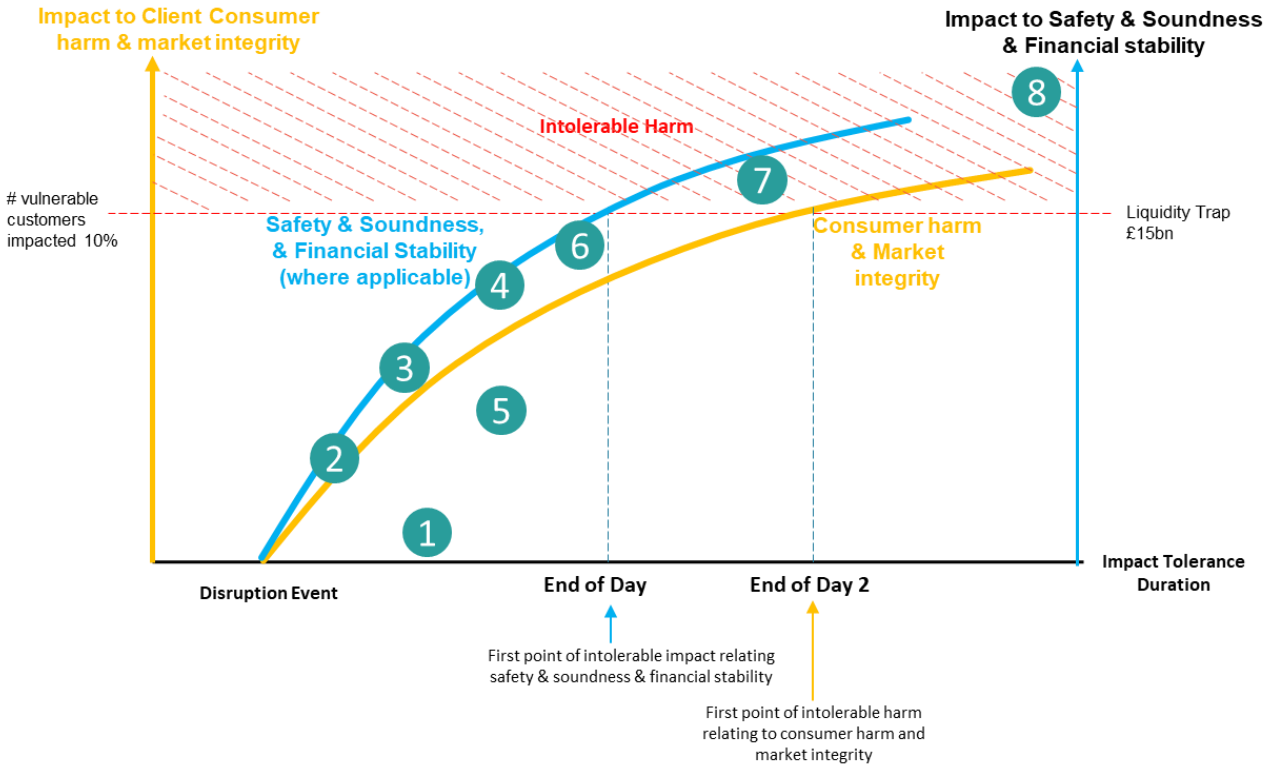
5.1.1 Assessing scenario test results against Impact Tolerances

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

For scenarios where firms are unable to meet Impact Tolerance 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 & market integrity and b) safety and soundness, and financial stability.

Figure 9. Examples of IBS scenarios



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 Impact Tolerance 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 Impact Tolerance 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.

5.1.2 General guidance for developing 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 Important Business Services. 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

- Although it is not mandated that testing is required yearly, it is good practice to ensure that a schedule for each Important Business Service per year is determined by individual firms and should be proportionate to the size and complexity of the firm. (FCA PS 21/3 ch5.16) vs 'regular' in PRA PS 6/21 ch7.16.
- There is an expectation that all Important Business Services will be evaluated against a range of scenarios, and gaps remediated, during the implementation window defined by the regulators. 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 Impact Tolerances 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 Important Business Services (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 an Impact Tolerance is more stringent than another, firm's must demonstrate they have considered both tolerances within their scenario design and execution. Just because you may meet the tolerance threshold of one criteria, 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 / 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 / ICAAP etc.

- Capabilities that are evaluated in anger (e.g., CV-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.

5.1.3 Fundamental principles for scenarios

Testing should play a key role in how firm's reach conclusions around remaining within tolerance. In some cases, solutions are still being developed or new vulnerabilities have been identified and at this point, further testing may have limited benefit until enhancements have been implemented. e.g., testing cyber recovery may have limited benefit while solutions are still nascent.

Principles

P.1 **The scenario library should be actively managed and updated, with a formal review on an at least annual basis or in the event of material change.**

P.2 **To ensure 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. Example sources to consider include internal disruptions, industry wide incidents and intelligence sources and global / national risk registers.**

P.3 **The scenario library and any new proposed scenarios should be agreed with a range of stakeholders to ensure adequate technical specialism, enhance credibility, and avoid "groupthink".**

P.4 **Scenarios should be scalable and challenging enough to test a firm's ITOLs. Where appropriate, testing should increase in complexity, breadth, and depth, as testing approaches mature.**

P.5 **Improvements and enhancements from prior testing should be considered for retesting as part of refreshed scenarios, ensuring they have fully remediated vulnerabilities / control weaknesses previously highlighted.**

P.6 As far as possible, existing testing and exercising methodologies should be utilised to prevent unnecessary duplication and a lack of coordination. Additional, bespoke scenario testing should be considered to supplement existing testing.

P.7 Once candidate impact scenarios have been chosen, the proposed list (*incl. type and approach*) should be reviewed, challenged, and endorsed by senior management committees (*firm specific resilience boards / committees*) on an at least annual basis.

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:

- National Risk Register (NRR)
- Global Risk Register (GRR)
- Business Continuity Institute (annual horizon scan)
- ORX Scenarios database
- ORIC International
- Insurance company models & 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)

5.2 Scenario testing approach

5.2.1 Define the scenario

Introduction

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 firms' 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 that 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 severe 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 IBS.
    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 severe but plausible 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 Subject Matter Experts that understand the key dependencies and vulnerabilities of the Important Business Service(s) should be involved in scenario development. For example, 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 Important Business Service 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

- An event 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:
    i. There are multiple different sources of corroboration.
    ii. The explanation of the concept or event is low complexity.
    iii. 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 severe 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.

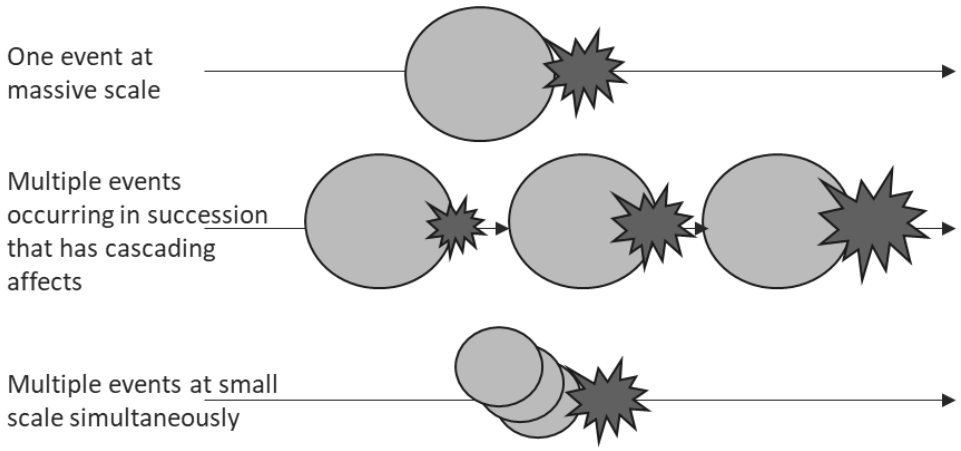
- The cause of disruption, and how that might reflect in the severity of the scenario, should be considered. For example, the capability of a threat actor is likely to affect the potential outcome of a cyber event because a nation state will have significant resources, and different motivations, when 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 IBS 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 has become implausible.
- 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



Tailored

- Use the results of end-to-end Resource / dependency mapping completed against Important Business Services 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.

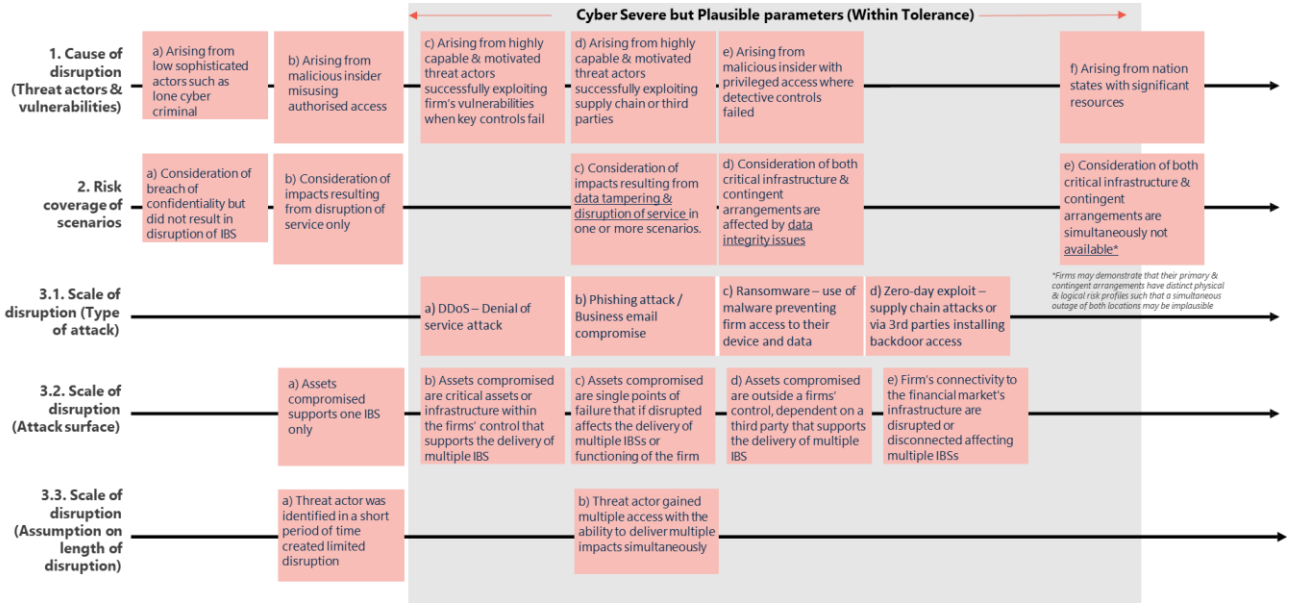
Assumptions

- It is key that scenario design assumptions are captured and understood.

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 IBS so the calibration of SBP will differ between firms. Please note the example below is calibrated in relation to systemically important firms.

Figure 11. Calibration of cyber scenarios



5.2.2 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. For example, 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 Impact Tolerance(s). 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.

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:
    - Impact Tolerance metrics used to define intolerable harm / risks to firm safety and soundness etc.

- Operational data at different periods including:
    - Demand & 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 Important Business Service.
- 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 appropriate response and recovery plans to confirm whether they are able to remain within Impact Tolerance. Actions to remain within Impact Tolerance 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 Important Business Service 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.
- The invocation of the Impact Tolerance(s) should be recorded from a time stamp perspective. This is to ensure that operational disruption being tested is tracked against the scenario and ultimately if the Impact Tolerances 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. For example, 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 Impact Tolerance 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 intolerable harm would be breached? Are there options for a partial resumption of service (manual payments for example), 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., consumer, market integrity, safety and soundness, and financial stability 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 the Resource profile might 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 the additional Impact Tolerance 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 Impact Tolerance statement (e.g., the point at which intolerable harm would occur), or could intolerable harm materialise more quickly or slowly than expected?

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 Impact Tolerance 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.

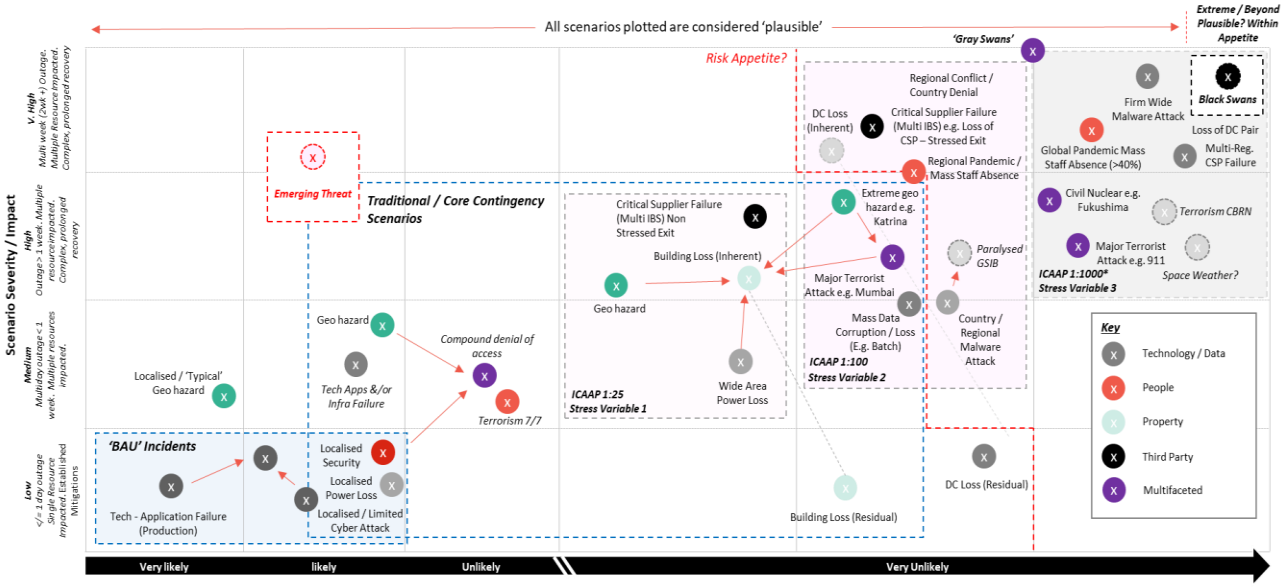
Test Type	Characteristics	Firm Level of Maturity in Operational Resilience	Planning Time & Effort	How does it support Testing to Remain within Impact Tolerance?
Drill	• Tests specific function or process • Usually requires physical action • Typically has a 'pass/fail' outcome	Low	Limited	Provides data 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 • Scenario based • 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	• Discussion based • No time constraints • Used as a tool to build competence • Elements of ambiguity to trigger creativity in participants	Low to medium	Medium	Provides an opportunity to walkthrough the steps and timeline for response and recovery. Elements of ambiguity should stimulate thinking on existing workarounds, contingencies, alternatives and substitutions.
Simulation / War Game	• Designed to depict an actual or assumed real-life situation • Competitive / contested environment • 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 • 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 impact tolerance is met or breached.

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

Severe but Plausible scenarios (Severity/Likelihood Matrix)

Figure 12 provides an indicative illustration of severe but plausible scenarios versus traditional contingency scenarios under existing capabilities such as business continuity.

Figure 12. Severe but Plausible scenario matrix



**This is purely illustrative. Under ICAAP banks holds capital against events of this scale / likelihood (e.g., 1:1000) but not necessarily the specific scenarios outlined.*

5.2.3 Assessing test outcomes

Assessing the outcome

SME judgement on the effectiveness of capabilities and recovery times is important, but tangible evidence will provide greater assurance. The conclusions on remaining within Impact Tolerances 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 Impact Tolerances.
- Evidence of firms' 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 Impact Tolerances:

- 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 Impact Tolerance 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?

5.3 Scenario themes

How to use scenario themes

The scenario themes serve two related purposes and should not be viewed as 'off the shelf' severe but plausible scenarios:

- They provide a baseline of potential impacts, or disruption events, that firms should consider planning for e.g., cybersecurity risks, impacts to third parties, failures of IT infrastructure, physical damage, and disruption due to unavailability or loss of people.
- They provide a broad set of themes that firms should incorporate into their coverage model for scenario testing e.g., covering disruption across the dependency pillars and impacts to data integrity as well as service unavailability. Whilst firms should focus on those scenarios that have most potential to cause

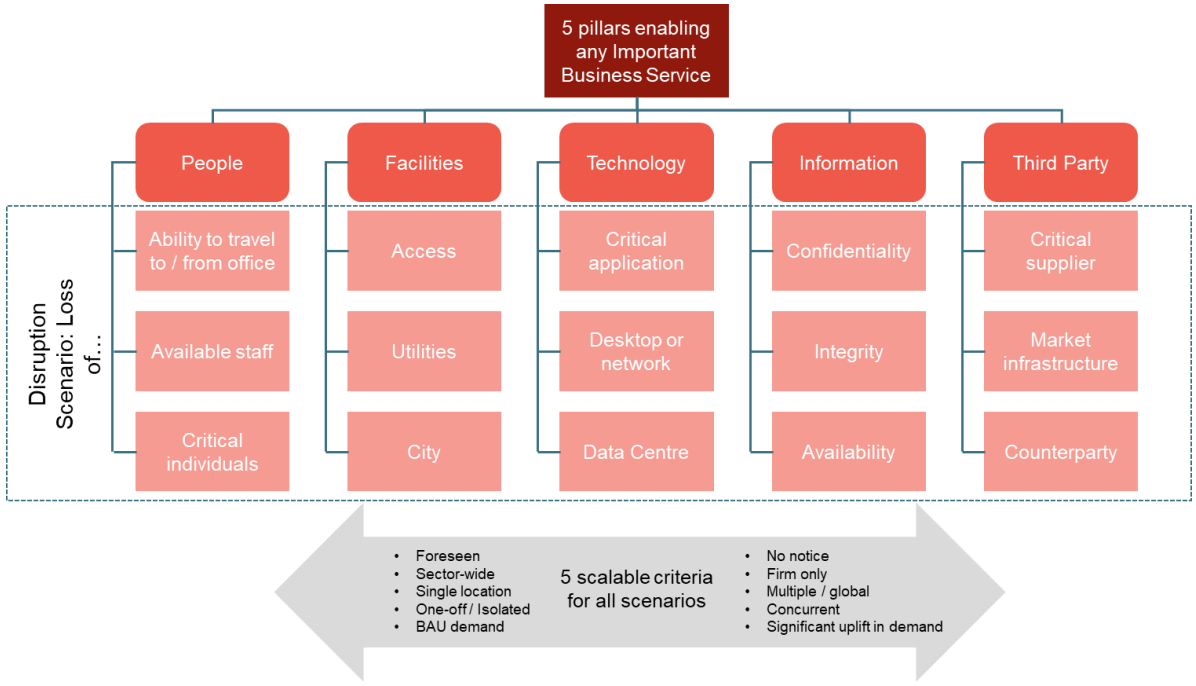
intolerable harm, they should consider testing response and recovery capabilities across all dependencies.

The scenario themes are intended to be:

- A limited set of discrete and distinct impacts that firms should consider planning for, and act as input when defining severe but plausible scenarios.
- Cause agnostic, wherever possible, because they are intended to guide response and recovery capabilities that are effective across a range of causes e.g., a data centre recovery must be effective regardless of a fire, electrical failure etc.
- Conversely a scenario used for a scenario test should have a specific cause that will provide insight into the effectiveness of a specific response and will also help engage participants in thinking creatively about the options available to mitigate harm.
- A specific cause will also help in defining mitigations / remedial actions. Defining a Resource as being unavailable, without a cause, in a scenario will limit the value of the test, as responses and remedial actions will be inherently generic.
- Focused on a single dependency type whereas scenarios for testing can combine multiple Scenario Themes e.g., a flood could impact people, premises, and third parties.
- Broadly static, whereas scenarios used for testing should be highly dynamic, considering the evolving threat landscape, including inputs from threat intelligence, and known vulnerabilities at a firm.
- A potential source of information for third party benchmarking e.g., a common way to review response and recovery capabilities with third parties.

Overview of the categories of scenarios and the criteria used to scale up scenario testing

Figure 13. Categories of scenarios for Resource pillars



Example scenarios

These examples have been added as a point of reference for firms to looking at the cause, risk coverage and scale of disruption of their own scenarios.

Cyber & Third-party Scenario 3. Highly capable threat actor in gaining remote access to an FMI's core payment systems	
Cause of disruption. Cyber attack (e.g., malware / ransomware)	• A threat actor exploits a firms' weakness in its logical access control by deploying malware on the firms' critical infrastructure and assets. The threat actor can obtain multiple access points to infect malware that encrypts files on the firms' systems and locks the firm out from access to systems and data. The scale of disruption affects multiple business lines as the malware was planted in multiple systems. Access at its recovery site is also affected as it relies on the same file that have been infected by the same malware. • No employee can access the firms' critical infrastructure, and customers are also unable to carry out transactions through its digital channel. This results in the disruption of multiple IBSs
Risk coverage of scenarios	Availability • Firms' IBSs are not available to customers for > 48 hours. The threat actor aims to deny access for legitimate customers to IBS by: o Wiping of data o Changing configuration data o Vulnerability exploit (application or infrastructure) Data Integrity • As the threat actor remains undetected, the actor continues to amplify the disruption by altering transaction records and business data resulting in loss of accuracy and completeness.
Scale of disruption	• Disruption impacts multiple business lines and multiple IBSs. IBS ITOL is 24 hours for financial stability, and there is a risk of contagion to the wider sector due to scale and length of disruption as the threat actor had multiple access points to the firm's systems. Customers such as large corporates, other financial institutions and FMIs are also impacted. There is likely to be significant knock-on contagion from large corporates and other financial institutions to the wider economy. • Given the nature of the scenario where the threat actor remained undetected and took further destructive action to corrupt transaction records, this reflects a prolonged disruption that is likely to exceed the ITOL set for the IBSs.

Cyber Scenario 2. Attack aided by malicious insider with privileged access that enabled modification of payment instructions to re-direct funds to threat actors' accounts	
Cause of disruption. Cyber attack (e.g., malware / ransomware)	• An organised criminal gang gains a foothold in the firm's network, facilitated by an employee, and is granted privileged access to payment and/or Banking systems. • This attack enables the modification of the databases or standing files that contain payment instructions which enables them to re-direct funds and payments to mule accounts inside and outside of the firms. The funds are then withdrawn (misappropriated) by the criminal gang. Significant reconciliation discrepancies were detected after the batch run and issues were escalated early the next day. As a result, the entire payments systems and the core banking platform was shut down.
Risk coverage of scenarios	Availability & Data integrity • Firms' payments related IBS are not available to end-users because of a threat actor modifying payment instructions.
Scale of disruption	• Extensive impact on retail banking business, affecting all IBSs. Many systems were disconnected. Customers would not be able to use channels to access their accounts, make transactions. However, backups are not corrupted. • The compromise also affected IT support staff who all have privilege access credentials, thereby delaying recovery efforts and prolonging the disruption of IBSs. However, impact to large corporates, other financial institutions and FMIs were contained as the firm were able to selectively process critical payments manually through alternative channels. • Period of disruption is up to 48 hours as the firm had to reconcile the accounts to ensure integrity of accounts, re-issue system authentication credentials to all users to ensure that all systems can be safely resumed.

Cyber & Third-party Scenario 3. Highly capable threat actor in gaining remote access to an FMI's core payment systems	
Cause of disruption. Cyber attack	• At 8pm the firm is told they have identified a staff member carrying out atypical activity on live payments data, which the firm is told to treat as malicious. • Just before midnight, the firm is told a large volume of payments have been modified, but they are not told precisely how. They are told that the malicious insider is contained. • Shortly after midnight, the firm discovers that the staff member facilitated an attack on another firm. This also involved modifying payment instructions.
Risk coverage of scenarios	Data integrity • Firms' payments data have been manipulated where the threat actor have modified payment instructions, thereby impacting some customers who may not be receiving any payments. • Payments data at the FMI, operator of the payment system have also modified, including payment instructions and master reference data.
Scale of disruption	• Given the scale of data corruption, payment services will not be available to all participants until integrity of the data can be assured, and similar assurances through reconciliation are undertaken at all direct participants of the payment service. • There is a systemic impact on the UK domestic payments given the extensive disruption arising from a corruption of data at the FMI. • The incident continued to unfold over a period of 4-5 hours, but the vulnerability has been exploited many months ago. The length of disruption is likely to be extensive given the scale of data corruption and the level of assurance required from the FMI and direct participants before the service can be resumed.

Third-Party Disruption Scenario 1. Threat actor gained access to the supplier's systems and planted a malware in their upcoming software update	
Cause of disruption. Disruption at third party (e.g., IT failure, software bug, cyber-attack)	• A threat actor can exploit the vulnerability of a supplier that is part of a supply chain providing services supporting a firm's IBS. The threat actor gained access to the supplier's systems and planted a malware in their upcoming software update that will be distributed to financial institutions. • When the software update is delivered to the firm, it managed to install a backdoor device that allows access. It was not detected by the supplier controls and testing before release, and firm installs a seemingly legitimate component in its production environment containing a hacker's fabricated backdoor. • Over time, the threat actor can gain knowledge of the firms' business and supporting infrastructure and took steps to compromise the integrity of firm's data by incorporating denial of service malware. While the attacker might only compromise a single instance of the software or firmware binary, it remained undetected and led to a spread by firm across to its full production environment during release. Fortunately, the attacker did not gain access to the firms' back up facility.
Risk coverage of scenarios	Availability & data integrity • When the denial-of-service exploit is activated, firms' IBS are not available to end-users. Al the time the threat actor remains undetected, the actor can gain access to data to overcome controls, exploit vulnerabilities to cause more damage to firms' operations and thus, affecting its IBS.
Scale of disruption	• The impact of the disruption is likely to affect multiple business lines, at different times and at different levels of severity. As the threat actor leans more about the firms' operations, the disruption will be more severe over time, and likely to impact the firms' customers, including other financial, institutions and FMIs. There is a risk contagion due to nature of interconnectedness with other financial institutions. • Impact of the disruption to other firms are limited as the firm were able to roll back the component that is in a good state.

Third-Party Disruption Scenario 2. Failure at a cloud service providers' availability zone across multiple regions	
Cause of disruption. Disruption at third party (e.g., IT failure, software bug, cyber-attack)	• A firm hosts its critical infrastructure supporting its core banking platform on the cloud, using multiple availability zones in a single region, and a backup arrangement in another region. The firm's workloads are supported across one single region (albeit across multiple AZs). • As a result of an unknown software bug, there is a failure at all the firms' availability zones across multiple regions and there is no estimate as to when services will be resumed, and status remained the same by the end of day. The firm is unable to carry out end of day processes and key deadlines on payments and reporting have been missed. • Recovery from a cold back-up arrangement to another region were not possible as the backup region was also affected. An alternative AZ in an operating region will need to be identified delaying the recovery process. This was identified towards the end of day and recovery commenced with the aim of completing all end of day processes and a full recovery by start of the next business day. However, the recovery was only partially successful as the firm is unable to fully reconcile the balances and it will require up to 1600hrs on Day 2 before all services can be recovered from the back-up region.
Risk coverage of scenarios	<u>Availability and data integrity</u> • The initial impact is the unavailability of all IBS supported by the core banking platform. However, upon completion of the restoration of data in an operating AZ to the back-up region, there were significant discrepancies in the reconciliation.
Scale of disruption	• All IBS relating on the core banking platform is unavailable, this includes all transactions, payment, and settlements. All digital channels are also disrupted, and IBS are not available to end-users. Disruption impacts multiple business lines firms or customer impacted include large corporates, other financial institutions and FMIs. There is a risk contagion due to nature of interconnectedness with other financial institutions. • Impact of the disruption to other firms are limited as the firm were able to manually process critical payments and the period of disruption extends to almost close of business day 2.

Internal IT Disruption Scenario 1. Disruption arising from a failure of firms' IT change	
Cause of disruption. Disruption at third party (e.g., IT failure, software bug, cyber-attack)	• Today is a full scale roll out of a new product on a firm's core banking platform. The implementation took place over the weekend. Shortly after the launch, customers begin registering concern on Twitter that they can either see information pertaining to other customers' account or cannot see any transaction information. Customers report the issue through other channels and the volume of calls rapidly overwhelm all customer channels, but the issue is still not escalated. Complaints are dealt and managed at an individual basis, and managers are unable to quantify the scale of the issue or identify a specific pattern or trend of customers affected. • The IT team begin work to identify the root cause and identified that customers' data (name and address) have been merged, and the trend shows that the affected customers all came from the new product. The new product IT team investigates the issue and confirmed that the source is indeed originating from the new product, but there is no way of identifying customers to "demerge" and cannot guarantee the completeness and integrity of customer details. • By mid-day, it was agreed that there is little confidence left in the integrity of the core banking platform the only remaining option is to shut down the system and **undertake a full-scale system recovery**.
Risk coverage of scenarios	<u>Availability</u> • The gradual disruption and eventual shutdown of the core banking platform will affect multiple IBSs reliant on the firm's core banking platform. <u>Data integrity</u> • The integrity of customer data means that a full restoration of customer data will be required.
Scale of disruption	• All IBSs supported by the firms' core banking platform will be affected. Any cash transfers or transactions reliant on the core banking platform will be affected. • Disruption impacts multiple business lines firms but mostly retail customers and small businesses. There is a risk to the liquidity of small businesses. Period of disruption extends to almost one week.

Scenarios by pillar

For each scenario category, there are a set of impact scenarios which provide details to inform the creation of detailed test scenarios.

Impact Scenarios	Impact Confidentiality, Integrity, or Availability	Examples of how impact might be realised	Additional information / Response considerations
INFORMATION			
• **Unavailability of critical data (single application)** • **Compromise of availability of data critical for accurate and effective functioning of payments, clearing, settlement or other processes through data deletion** • **Unavailability of data in both Production and DR (data is unreadable / locked or deleted)**	Availability	• Failed change • Malware \ Ransomware attack circumventing all prevention controls and deleting or encrypting the file making the application unusable. • Malicious inside • Human (or process) error	• Requires recovery of data from snap shots or back up mechanisms. Is not routinely assessed during DR testing, as disaster recovery is predicated on data being replicated and available in the alternate environment. • Data recovery from backup • Data recovery from Vault (probable future solution) **Example**: Travelex ransomware 2020 (Sodinokibi / REvil) **Ransomware examples**: Reveton, WannaCry, Petya, Bad Rabbit
• **Manipulation of critical data** • **Compromise of integrity of data critical for the accurate and effective functioning of payments, clearing, settlement or other processes through data manipulation**	Confidentiality Integrity	• Malware attack circumventing all prevention controls and modifying data. • Human error, malicious or unintentional	• **Detection**: Difficult to identify that an attack has occurred, particularly if data manipulation is executed without detection, bypassing reconciliation controls. Average detection time is commonly cited at 100+ days. • **Response**: Difficult to establish when and how the attack originated. • **Recovery**: Difficult to identify and revert to the 'last known good' state of data, given that analyzing and diagnosing data manipulation can be complicated and time consuming **Example**: **2010** – Hackers use the Stuxnet Worm to make minor changes in Iran's nuclear power program in an attempt to destroy it **Example**: **2016** – Both the World Anti-Doping Agency and Democratic National Committee are breached with hackers manipulating their data to embarrass the organisations.

Impact Scenarios	Impact Confidentiality, Integrity, or Availability	Examples of how impact might be realised	Additional information / Response considerations
• **Initiation of fraudulent transactions through unauthorised access of critical payment infrastructure**	Integrity	• Malware • Insider	• Predicated on systems remaining operational and activity going unnoticed. Standard containment activities would be employed. • Firms would need to look at infrastructure level for scheme issues as they may share underlying rails internally or in the scheme e.g., VocaLink infrastructure. • Critical payment infrastructure can be accessed through upstream services with varied authorisation controls (e.g., MQ using MTLS, APIs using OAUTH). Any flaws in authorisation controls can result in unauthorised access to critical payment infrastructure
• **Theft of critical non-public information** • **Compromised confidentiality of non-public information for use in insider trading, market manipulating action, intelligence gathering or other forms of unauthorised use**	Confidentiality	• Malware • Insider	• Could include Customer data (Personally identifiable information - PII) and corporate data (Intellectual Property - IP). **Examples**: In 2023 Clop stole personal details of more than 100,000 staff from BA, Boots and BBC. A compromise of SolarWinds Orion platform in 2020 penetrated thousands of organizations globally including multiple parts of the United States and UK governments, leading to a series of data breaches; Cope Marriott International (2014-2018) Impact: 500 million customers; Yahoo 2013-14, Impact: 3 billion user accounts; LinkedIn 2012 (and 2016), Impact: 165 million user accounts
TECHNOLOGY			
• **Wide scale unavailability of Network** • **Vulnerable network devices have been the attack-vector of choice and one of the most effective techniques for sophisticated hackers and advanced threat actors. This scenario goes beyond single link failures or site unavailability. The scale is all devices of a given type or manufacturer or unavailability of multiple critical locations.**	Confidentiality Integrity Availability	• DDoS attack • Seabed warfare / cable sabotage • Exploitation of vulnerabilities either manufacturer defects or weak configuration on network devices by cyber attack	• If the network infrastructure is compromised, malicious hackers or adversaries can gain full control of the network infrastructure enabling further compromise of other types of devices and data and allowing traffic to be redirected, changed, or denied. Possibilities of manipulation include denial-of-service, data theft, or unauthorized changes to data. This impact would need to be resolved ahead of any other impact assessments and service restoration activities and would require involvement of the network vendors of impacted devices. US CERT in 2016 has advised of the increasing threat to network devices, referring the discovery of a Cisco implant malware known as SYNful Knock, for the router's operating system. • Distributed Denial of Service (DDoS) attacks are included in this category. • Loss of VPN and/or ISP providers - i.e., not due to cyber-attack, but technical outages that mean the ability to service customers is impacted.

Impact Scenarios	Impact Confidentiality, Integrity, or Availability	Examples of how impact might be realised	Additional information / Response considerations
• **Loss of Public Cloud Service at the region level**	Availability	• Failed change • DNS failure • Cyber Event • Multiple causes are possible	• If we consider Amazon Web Services, the loss of a single Availability Zone (AZ) would be the equivalent to the loss of an internal data centre. Firms are responsible for provisioning across AZs and internal data centres and have various mechanisms for failover and / or load-balancing to limit or eliminate downtime. • However, as workloads may be provisioned within a single AWS Region (albeit across multiple AZs) a Region loss will cause an outage for all applications hosted solely in that Region. • Equivalent issues possible in GCP, Azure etc. An AWS service event occurred in Dec 2021 impacting workloads across the US-EAST-1 region as a result of an impact to DNS. • Options to reduce risk: multi-region, multi-cloud, or hybrid cloud hosting.
• **Disruption / loss of Core Infrastructure Services** • **Core underpinning name and directory services such as DNS or Active Directory are unavailable, or compromised (e.g., AD DS file potentially compromised, and a full domain password reset is required)**	Availability Confidentiality	• Golden ticket and other targeted Malware • Device or OS-related compromise (e.g., AD domain controllers impacted by Windows OS compromise) • Failed change	• Examples of Core Infrastructure include Active Directory where an entire domain is unavailable and needs to be recovered from a previous back up. Active Directory is vulnerable to Windows platform compromise as was seen with the NotPetya malware attack. Other Core Infrastructure services for consideration include Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), Build Servers, NTP, Backup Servers and Catalogues, HSMs, CyberArk (or other password management systems). • Core infrastructure impacts extend beyond unavailability of infrastructure to compromise of core directories 'on premise' as well as cloud hosted infrastructure including AWS (or other CSP) account and hardware security module (HSM) compromise. Review 'Service Account Attacks' such Windows domain compromise with Golden Tickets e.g., Mimikatz.
• **Devices rendered inoperable.** • **Devices, appliances, network components, hosts are inoperable e.g., master boot record or firmware overwritten. They may even have been rendered physically inoperable**	Availability	• Malware • Electromagnetic Shunt	• Rendering devices completely usable is rare. The need to rebuild hosts or devices, either on new or existing equipment, is more common on Windows devices following execution of malware which overwrites the Master Boot Record (MBR) with its code or corrupts the MBR, so the device does not reboot. Requirement to have secure backups of host gold images, software, configuration, and data.
• **Complete unavailability of a data centre or Cloud Availability Zone** • **All workloads within a DC / AZ are unavailable**	Availability	• Fire, Flood, Terrorism, Loss of network	• Recovery of Applications and Services to alternate Data Centres requires significant incident coordination and ideally utilises highly parallel, rapid, and tested approaches to recovery of critical applications. Rehearsed during Data Centre Recovery Tests.

Impact Scenarios	Impact Confidentiality, Integrity, or Availability	Examples of how impact might be realised	Additional information / Response considerations
• **Application failure in a single data centre** • **Failure of key infrastructure supporting a single application**	Availability	• Failed change • Infrastructure failure	• Complete or partial loss of infrastructure in a Data Centre supporting a single application that requires fail over to Disaster Recovery (DR) instance; evaluated via Production Crossover / flip flop, Data Centre Recovery Test or single application fail over events.
• **Data is inconsistent, inaccurate, or incomplete - Single Application**	Integrity	• Failover to DR instance • Recovery from backup or vault • Cyber-attack	• The overall accuracy, completeness, and consistency of data is compromised through deliberate (cyber event) or accidental action (failed changed). Impact is systemic. This event may cause complete unavailability of the business service. • Following recovery of a database there may still be outstanding tasks to manage the synchronisation of data within the application, and to reconcile data backlogs e.g., an intra-day incident where database failure was not clean, and transactions need to be re-applied / recreated.
• **Data is inconsistent, inaccurate, or incomplete across connected applications within one or more IT Service**	Availability Integrity	• Failover to DR instance • Recovery from backup or vault • Cyber-attack	• The overall accuracy, completeness, and consistency of data is compromised through deliberate (cyber event) or accidental action (e.g., failed changed). Multiple applications are impacted e.g., inaccurate data has cascaded to downstream systems which will need to be resolved. • Synchronisation of data across applications must be managed to reconcile data backlogs in the connected system. Transactions that were sent and processed but are no longer present post-recovery may need to be created prior to continuing operation. This event may cause complete unavailability of the business service.
• **Simultaneous unavailability of critical infrastructure, data, and applications** • **A high impact, low probability event that combines a number of impact scenarios where a platform (the Windows Operating System for example) is compromised causing the loss of core infrastructure services (e.g., Active Directory), databases, application servers, desktop estate and other services**	Availability	• Malware \ Ransomware attack deleting or encrypting system, application, or data files making the systems inoperable. • Unauthorised access to core systems management infrastructure / Service management capability (e.g., SCCM, Tanium, CHEF, etc.)	• This would not be a geographically isolated event but could require a significant global coordination effort impacting all business areas and locations. In the case of a systems management toolset compromise there could be disruption, destruction, or compromise of systems managed by that toolset including servers (Windows and/or Linux), Network (Firewalls / Switches / Router), and desktop estate. • Recovery is achieved by securing a defined set of critical infrastructure, data, and application components and a mechanism to support the restoration of services. • **Example**: NotPetya malware compromised the Windows platform at Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser.

Impact Scenarios	Impact Confidentiality, Integrity, or Availability	Examples of how impact might be realised	Additional information / Response considerations
THIRD PARTY			
• **Takeover of our external DNS records and domains**	Confidentiality Integrity Availability	• Exploitation of vulnerabilities either manufacturer defects or weak configuration on DNS systems	• Sophisticated threat actors have launched global campaigns targeting governments and commercial organisations worldwide. In Feb 2019, NCSC note they were not aware of any in the UK, but "the techniques could feasibly be deployed against UK targets". • If controls are bypassed this would allow for interception, or denial of all email, redirection of web traffic to attacker infrastructure, enabling man-in-the-middle attacks to eavesdrop on online channel user journeys, wide scale malware deployment to customers, or simply the denial of access.
• **Disruption of critical Supplier** • **Due to Cyber Event**	Confidentiality Integrity Availability	• All Cyber-related scenarios	• A coordinated response between a firm and the supplier to restore service. The Cyber-related scenarios detailed in this library could all be applied to Suppliers and the scenario would drive the support provided by the impacted firm to the supplier. For example, customer or client data compromise at a supplier would be managed differently to unavailability of a Supplier. • Could include disruption to utilities and infrastructure: power, transport, or telecommunications.
• **Unavailability of Critical Supplier (Non-cyber)**	Availability	• (All non-Cyber scenarios) incl.: o Fire, flood, terrorism, loss of network, failed changed, Infrastructure failure	• This Supplier impact is non-Cyber and therefore focuses on how a firm would manage unavailability of the Supplier and minimise impact on customer and clients as well as instigate workarounds and alternatives such as directing activities to other Suppliers or using different IT Systems to achieve the business outcome. • Could include disruption to utilities: power, transport, or telecommunications Also, liquidation / insolvency / short notice financial failure of suppliers.
• **Disruption of critical industry-wide services**	Availability	• Malware / Ransomware attack	• Disruption, or complete loss, of critical payments, clearing, settlement, or Central Counterparties for an extended period e.g., unavailability of critical FMIs such as VISA Europe or Faster Payments Scheme (FPS) • Alternates may be possible e.g., direct payments to BACS in place of FPS.
• **Disruption at another firm in sector**	Integrity Availability	• Various scenarios	**Examples** • Unavailability of a correspondent / agent Bank that you depend on. • Service disruption / unavailability at another firm that is a systemically important market participant, for a service where your firm is also systemically important. • Failure of a global systemically important bank (G-SIB) (this scenario may be more relevant to sector testing than per firm testing).

Impact Scenarios	Impact Confidentiality, Integrity, or Availability	Examples of how impact might be realised	Additional information / Response considerations
FACILITIES & PEOPLE			
• **Unavailability of a Mission Critical Building (Non-Data Centre)**	Availability	• Fire, flood, terrorism • Power outage • Earthquake	• The inability to access and/or occupy normal working environment at a single building, Campus, or location such as Canary Wharf.
• **Unavailability of colleagues supporting Important Business Services**	Availability	• Pandemic • Weather • Power cuts because of power shortages impacting colleagues working from home	• Unavailability of key staff supporting Important Business Services in any country, or in the case of a pandemic in multiple countries up to, and including, all locations (COVID-19). Considerations should include unavailability of key people with specific skills and / or responsibilities ('Material risk taker(s)' or 'Accountable Individuals') as well as the unavailability of a larger number of people that are required to safely operate a process

6 Self-Assessment

The regulations require firms to complete an Operational Resilience Self-Assessment which details how they are meeting the legislative requirements. This section is aimed to provide firms guidance on how to update and complete their Self-Assessment.

The main purpose of the self-assessment is to answer the question, **'Are our firm's IBSs operationally resilient?'** meaning the firm must ensure it can remain within its impact tolerance for each important business service in the event of a severe but plausible disruption to its operations acknowledging that achieving impact tolerance should not be counterproductive (FCA PS21_3: 15A.2.10) and that a firm might encounter circumstances which are beyond severe or implausible (PRA SS1_21: 6.10). Firms should use the specific requirements of the self-assessment rule to evidence to the Board the progress made towards achieving this outcome and provide the Board with sufficient detail to understand the status and challenge management, including specific vulnerabilities, remediation activities and investment required to remain within Impact Tolerances. Self-assessment must be produced at the Regulated legal Entity or Group level, and the self-assessment document must be signed off by the firm's Board annual at a minimum and may be shared with regulators (if requested).

The regulations have left firms to determine the best manner for the delivery of the Self-Assessment to the Board for sign-off, but firms should ensure that in whichever means of delivery (e.g., Word document, PowerPoint) the content is still sufficient that the Board have adequate assurance of the actions taken by the firm to allow for sign-off. Individual firms may choose to augment the core Operational Resilience Self-Assessment content with additional information, and that the level of detail provided in respect of the suggested content will vary by firm.

As firms mature their resilience programmes, the Self-Assessment will evolve to focus more on what has changed year on year, rather than on educating the Board. Firms may wish to alter their self-assessments as they mature to move the approach and methodologies to appendices and highlight in the main body of text any changes that have occurred. Firms should bear in mind that the self-assessment is a living document that needs to be regularly reviewed and updated when there is a significant change to the business. Regardless of the format a firm decides to take to produce their Self-Assessment, as set out in SYSC 15A.6.1, the Board are required to approve the complete Self-Assessment on an annual basis.

6.1 Executive summary

The executive summary should document and provide a high-level summary of what resilience activities the firm has undertaken in the last year. Firms who are undertaking their Self-Assessment for their second and subsequent years should emphasise in the executive summary the key changes findings from their previous year's attestation to this year's one.

The executive summary should set out what the firm's Board is being requested to approve, namely the self-assessment which should include identified vulnerabilities, the Self-Assessment and identified investment to improve resilience capabilities.

In addition, the executive summary should provide an overview of the entity including a summary of the operating model, the markets that products/services are delivered to, set out the context that has shaped the analysis and, finally, the approach taken by the entity around operational resilience. Changes to the operating model should then be reflected in the specific sections below.

Dual regulated firms have the option to produce a combined self-assessment that meets both the FCA and PRA requirements or produce separate self-assessment documents. This should be well sign-posted at the start of the self-assessment to ensure that all requirements are covered and to determine which self-assessment can be sent to which regulator.

6.2 Governance

Operational resilience systems and processes

- A high-level description framework that is in place to manage operational resilience and supporting methodologies used to carry out the activities which might be attached as an appendix.
- Framework activity to provide education and awareness within the business unit to develop competence and aid embedding of operational resilience.

Operational resilience governance

As part of the Self-Assessment, firms may want to document and address the governance structure, frequency of reviews (annually as a minimum) and requirements of the Board.

The regulators require that the firm's Board approve:

- the list of IBSs;
- the Impact Tolerance statements for each IBS;
- the following year test plan; and
- the Operational Resilience Self-Assessment at least annually.

Prior to the delivery of the first year's Self-Assessment, the Board should be asked to consider the frequency of which it would like to approve the firm's Self-Assessment (at least yearly), the format of how the Board would like to understand and track the outcomes of the Self-Assessment and the Board's expectation in overseeing material or significant changes to the Self-Assessment year-on-year.

Firms should ensure that the governance structure for resilience are documented and remain up to date, to allow the Board to have sufficient oversight on the governance of resilience across the legal entity. A firm should document the output of the review of each section of the Self-Assessment, including who was involved, when the discussions were held and evidence of the sign-off. Firms should also confirm oversight by the firm's second line of defence together with any interaction with the firm's internal audit function.

6.3 Business services

Approach to identifying IBSs

- List a firms IBS', split by legal entity or business function, including any changes year-on-year.
- Methodology used to identify and prioritise a firm IBS.

Firms may wish to include in their Self-Assessment (either in the main body or appendix) the business services that are provided to an external end user that could potentially be an IBS as well as a list of business services that were not deemed to be 'important', including the rationale behind this decision.

Annual review and changes

For the delivery of the Self-Assessment following on from the first Self-Assessment, greater focus should be placed on what has changed and the rationale for any changes compared to the methodology and approach for identification.

The main body of the Self-Assessment should:

- outline what new / IBSs have been identified and which have been removed, including sign-off and process taken; and
- articulate the process for the annual review of the IBSs, including which stakeholders were involved at each point and the governance route followed.

6.4 Impact Tolerance

Approach to setting Impact Tolerances

- List a firms ITOLs, including a statement of the ITOL, rationale of why it has been set at that level.
- Detailed methodology and approach used to define and set a firms ITOL for each IBS.
- Articulation of key types of impact caused by a disruption to an IBS.
- Identification of the harm that may be caused, including the requirements of both the Bank of England, PRA and the FCA for determining intolerable harm (for dual regulated firms).
- Metrics used to measure impact or intolerable harm across PRA and FCA ITOL consideration areas.
- Where additional metrics have been recorded against IBS (i.e., volume of customers, volume of transactions, etc.) in addition to time-based metrics, record the rationale as to why these metrics have been determined.

Annual review and changes

For the delivery of the Self-Assessment following on from the first Self-Assessment, greater focus should be placed on what has changed and the rationale for any changes compared to the methodology and approach for identification.

If Impact Tolerance have been changed since the last Self-Assessment approval, specify the IBS these tolerances are recorded against, what they have been changed to, the rationale for the change, who approved these changes, what governance steps were taken and when.

As a firm matures its BAU capabilities for resilience, greater focus should be placed in the Self-Assessment on factors that have or may alter the ITOL in the coming years including new metrics and incidents that have occurred which has either caused a review of ITOL or has reinforced the current view.

6.5 Service mapping

Approach to mapping

- Outline the methodology and approach taken by the firm to undertake the mapping of Resources including.
    - To what level the firm have mapped Resources at (e.g., application or down to underlying infrastructure), and the scope of what processes have been mapped (e.g., have internal shared services that are dependencies been mapped), including an explanation as to why elements may have been excluded from mapping.
    - Ensuring that the mapping has covered all Resource areas under operational resilience.
    - If the firm has opted to map additional Resources (i.e. Third Parties) why this decision has been taken and what benefits this adds to the understanding of the resilience of the IBS.
- Firms may want to set out high-level process steps for each of their IBS.
- How mapping has been recorded, who has been part of the process and how the mapping flows into management information (MI).
- Description of where and how mapping is being kept up to date.
- Description 'golden sources' used to support IBS mapping activities activity.
- How IBS dependencies (i.e., internal group agreements, managed services or third parties) have been considered into IBS mapping.

Gap analysis and maturity plans

Firms should provide a summary of the current gaps within IBS mapping including what hasn't been mapped and where mapping may be not fully accurate. This should highlight plans in place to mature the mapping process to allow sufficient overview of all Resources that an IBS is critically dependent on.

Leveraging mapping data

- Description of how mapping has enabled vulnerability identification and, where appropriate, has led to investment prioritisation.
- Description of how analysis has informed risk identification – i.e., third party risk, technology risk and business continuity activity.
- Description of how mapping and process impact assessment have focussed areas for scenario testing.

6.6 Scenario testing

Approach to testing, scope, and execution

A firm should incorporate the outcome of the scenario testing including, but not limited to:

- whether the scenario caused a breach of an Impact Tolerance and the time taken to recover. This should also include the time the service was restored, if there was no breach of tolerance to allow the Board to understand how close the service was to breaching.
- assumptions made on the recovery of services, where appropriate.
- summary of key observations and results from each test carried out in the previous year.

Other elements include:

- the plan, details for the type of testing completed throughout the year, and the rationale used to confirm the scenarios used including the selection of IBSs used within the test;
    - Firms may wish to include in the summary which Resource types were included, what type of scenario was developed (confidentiality, integrity, availability) as well as whether the scenario was deemed to be severe and plausible.
- an outline of any third parties or other entities within your Group were involved in the exercise.

Firms may also consider including material live events and the outcomes that have been gained from post incident analysis.

Outcomes of scenario testing

- Articulate the status of the firm's ability to remain within Impact Tolerances across key scenarios e.g., unavailability of locations, people, technology, third parties. This should include articulation of any identified scenarios where testing has demonstrated challenges with remaining within Impact Tolerances.
- Firms may wish to add detail on status of capability to prevent, respond to, mitigate, and recover from scenarios.

Testing plan maturity

- Document the approach a firm is taking to mature scenario testing.
- This may include outlining how the testing type will change in the coming years and how the scenarios being developed will increase in severity but remain plausible.
- Include the following years test plan (approach and schedule).

6.7 Vulnerabilities, lessons learned and remediation

A significant element of both the first years and subsequent years Self-Assessment should be on outlining the gaps, risks and vulnerabilities that have been identified through the work undertaken and the steps the organisation are taking or will be taking to remediate these to allow IBSs to remain within Impact Tolerance by the 31 March 2025 and beyond.

For situations where firms have identified challenges in respect of remaining within tolerances in the event of SBP scenarios, the Self-Assessment should include the relevant actions which the firm is taking to increase resilience.

Lessons learned

Detail the material lessons learned following:

- The completion of operational resilience activities such as Resource mapping and scenario exercises.
- Any live disruptions that were coordinated through the firm's incident / crisis management framework(s).
- Any near misses identified by the firm.

Identified gaps, risks, and vulnerabilities

- Include detail of those material gaps, risks or vulnerabilities that were identified as part of Resource mapping and scenario testing, which have already been remediated.
- State which IBS are affected by the material gaps, risks, or vulnerabilities due to either an Impact Tolerance statement being breached or is likely to be breached in the future.
- Include an assessment of size and materiality when Impact Tolerance statements have been breached.

Remediation plans and progressing

- Detail what actions will be or are being taken to remediate the findings.
- Document who has ownership of the remediation plans and the forecast for their closure.
- For any IBS that has breached Impact Tolerance in a SBP event, define how gaps, risks or vulnerabilities will be remediated and over what timescale up to and past the Operational Resilience transitional period (up to 31 March 2025). This should provide an indication of how long the IBS will be outside risk appetite.
- Remediation activities should be proportionate to the firm and be managed alongside a firm's risk appetite.
- Detail any investment requirements or further investigation for investment to maintain or strengthen the firm's Operational Resilience position.

Changes from previous year

- Highlight any changes to gaps, risks and vulnerabilities from the previous year including any updates on timelines, ownership or potential issues that have occurred since the last Self-Assessment

6.8 Embedding into the organisation

As part of the delivery of the Self-Assessment, a firm should look to incorporate each year an overview of how the firm is embedding the operational resilience requirements into the organisation.

Initially this may focus on frameworks, policies, standards, and the operating model (including roles and responsibilities).

As a firm's capabilities mature, entities may look to also include updates of how other areas of the business are embedding resilience into BAU such as through third-party reviews and technology design and the use of education and awareness activities to embed resilience into the culture of the firm.

6.9 Appendices

In addition to the information provided within each of the section of the Self-Assessment, it is important that the Board have available of all the materials that have been used to help support the information in the sections.

From Year 2 onwards, firms may wish to include previous years IBSs, vulnerabilities, scenario tests and ITOLs (if changed), previous years self-assessments and any management information that aides in defining the level of resilience of the IBSs.

The appendices can also be used to document committee papers, and evidence of the discussions had to validate each of the sections.

Firms should have available a large pool of evidence to assist with their self-assessment. Although not all this information may be provided to the Board within the main body of text, they should ensure they have a strong management audit trail to support the assumptions and conclusions made throughout.

Appendix A: Abbreviations

BAU	Business As Usual
CMORG	Cross Market Operational Resilience Group
CRR	Capital Requirements Regulation
DORA	Digital Operational Resilience Act
FCA	Financial Conduct Authority
FMEA	Failure Modes and Effects Analysis
FMI	Financial Market Infrastructure
IBS	Important Business Service
ICAAP	Internal Capital Adequacy Assessment Process
ITOL	Impact Tolerance
ORCG	Operational Resilience Collaboration Group
PRA	Prudential Regulatory Authority
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SBP	Severe But Plausible
SME	Subject Matter Expert
SLA	Service Level Agreement
SPOF	Single Point of Failure