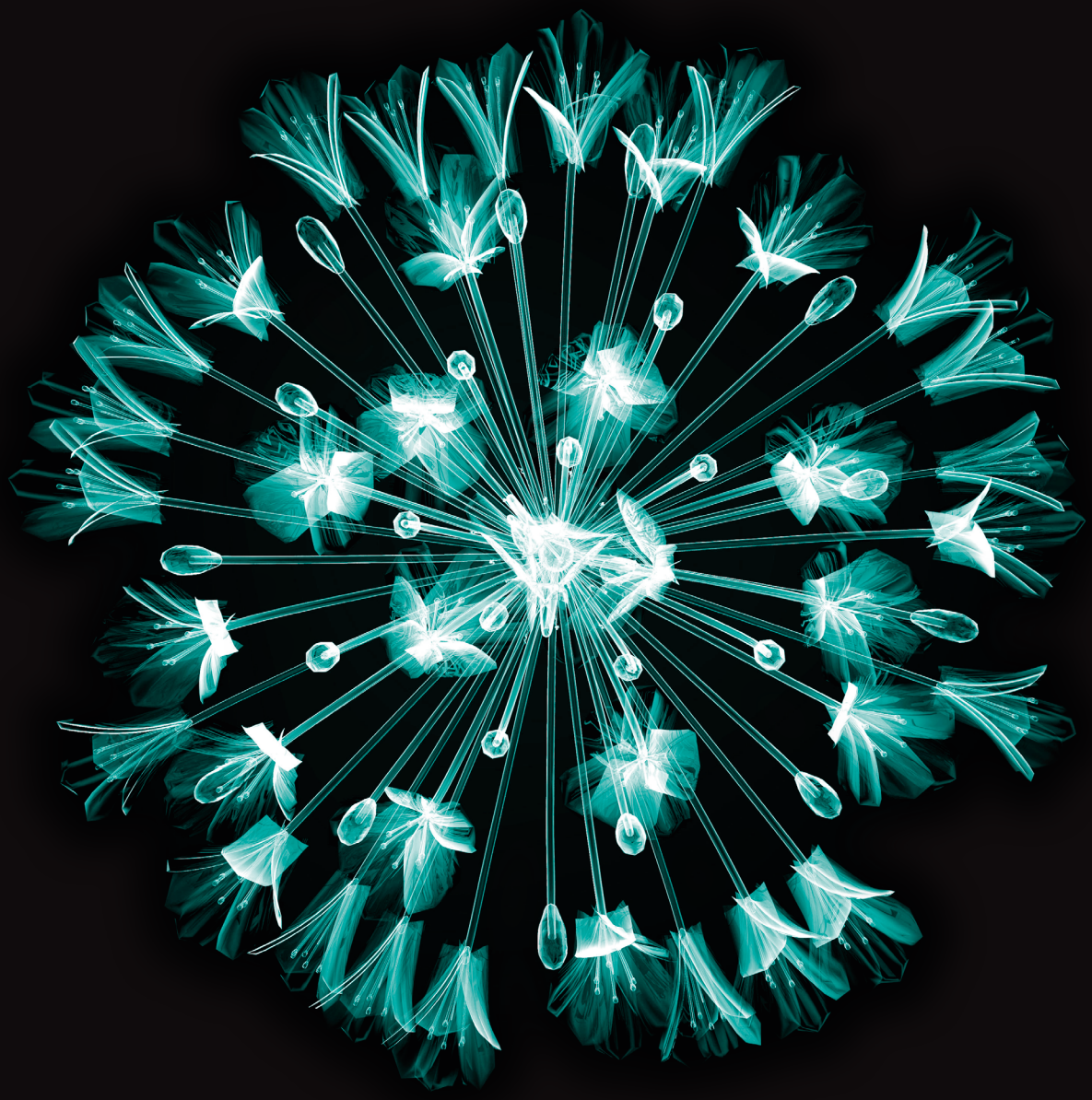
Deloitte.



Time to Thrive

A practical guide to implementing Operational Resilience in Financial Services

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Foreword

Within a few months of the publication of the joint PRA and FCA Consultation Papers on Operational Resilience at the end of 2019, financial services organisations faced some of the most challenging circumstances in recent memory. Although the specific events of the COVID-19 pandemic could not have been predicted, it was precisely scenarios of this magnitude and severity that the Consultation Papers were designed to address, underscoring the urgency for a regulatory framework to guide organisations in preparing for, and responding to, severe but plausible disruptions.

Whilst COVID-19 was extreme in its severity and reach, a pandemic had for some time been a highly plausible risk and one for which many organisations were at least to some extent prepared. How organisations now implement the Operational Resilience policy framework may naturally be influenced by the recent memory of the pandemic, and the resulting changes to the way we work going forward. However, the longevity and ultimate success of their implementation journey will be determined by their ability to anticipate and prepare for a broad range of potential threats.

With a new world order characterised by intense and increasing uncertainty and volatility, Financial Services (FS) organisations will need to continue to build adequate resilience arrangements to monitor, withstand, absorb, recover and emerge stronger from the many unknown challenges that lie ahead. Most organisations will be well underway with climate change scenario planning as part of Climate-related Financial Disclosures (CFDs) and will be looking ahead to the outcomes from the COP26 summit in November 2021 as they continue to analyse the impacts that environmental risks pose to the stability and future of their operations.

Any resilience framework will need to be dynamic. Organisations will also continue to be challenged by evolving cyber threats, supply chain disruptions, political instability, and the pace, scale and complexity of digital change. The ability to imagine their own future failure and consider a broad range of strategic, operational and regulatory risks will be a key driver of organisations' long-term resilience and success.

This backdrop of uncertainty has brought the importance of the newly published Operational Resilience policy framework into sharp relief. Indeed, of the organisations that we have worked with in the three years since the initial Discussion Paper was published, many have articulated a desire to adopt the policy set out by the supervisory authorities, not simply as a regulatory imperative, but as a matter of good commercial practice, a means of achieving better outcomes for their customers, and a means of securing a more resilient future for their own businesses and the sectors on which they depend.

As they enter the implementation phase of the regulatory framework, the critical importance of sector-wide collaboration and alignment will become increasingly apparent. It will be evident that the Operational Resilience strength of the UK Financial Sector as a whole is not just the sum of its parts but will be influenced by a wide range of non-FS organisations. FS firms will simply not be in a position to solve every resilience challenge on their own, and collective action will be required to solve the most pressing and significant challenges.

This will mean strengthening organisations' involvement in cross-sector resilience forums, such as the Cross-Market Operational Resilience Group (CMORG); proactively sharing information across organisational boundaries, and looking beyond financial services to the crucial part that other organisations, such as technology, telecommunications and other Critical National Infrastructure providers play in supporting the Financial Sector. As COVID-19 has effectively demonstrated, broadened perspectives and proactive collaboration are essential for organisations to not just survive, but thrive within the new risk landscape.

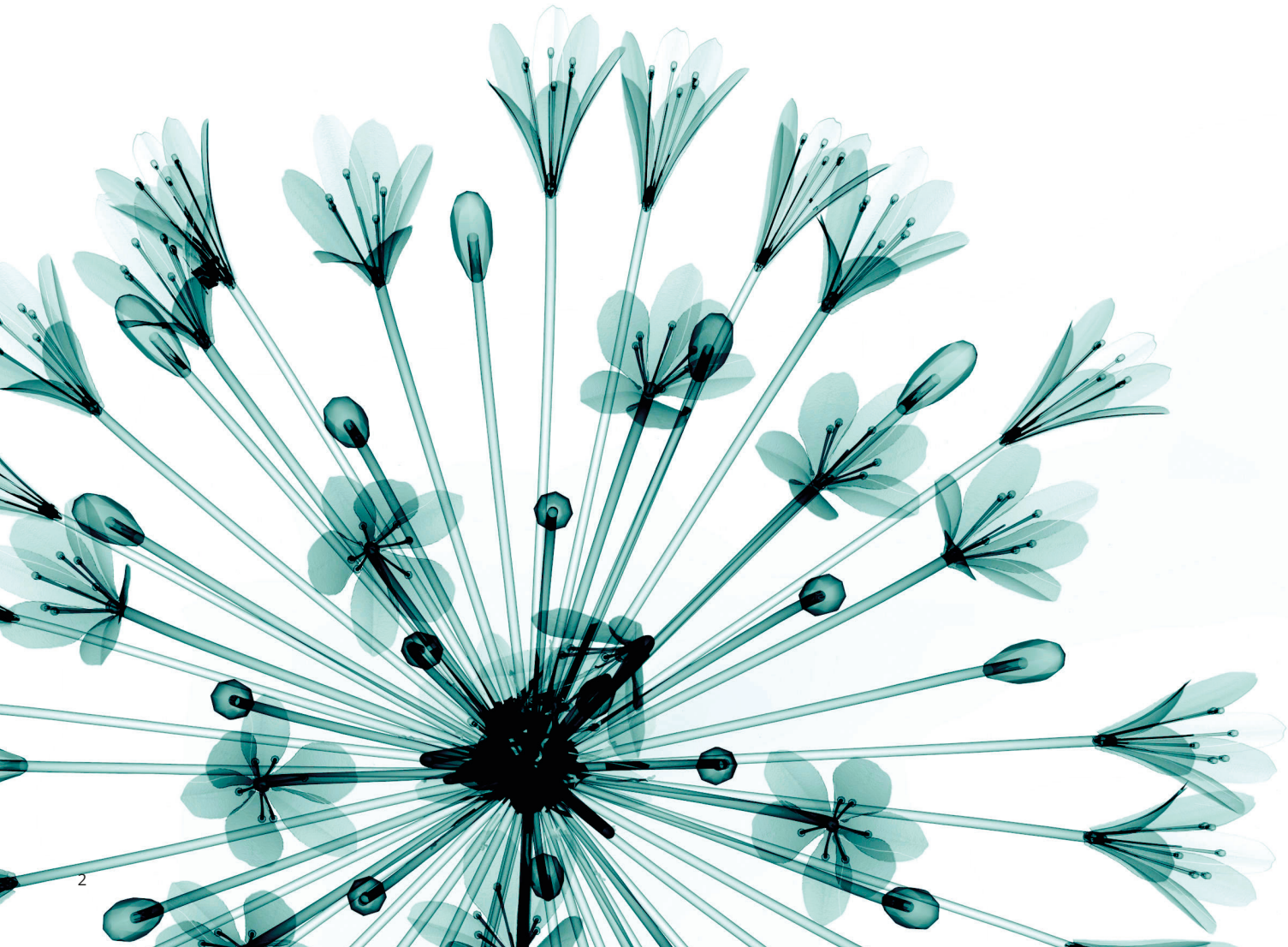
In this report, we build on our 2019 Time to Flourish paper, providing practical steps for organisations as they move beyond design into the implementation of the regulatory framework. We also share our observations on some of the common pitfalls that we have seen on the journey to date.

Introduction

The release of the final Supervisory Statements in March 2021 confirmed our view that the previous Consultation Papers (CPs) provided a sound basis for organisations to start work on the redesign of their Operational Resilience frameworks. The Supervisory Statements further provide important nuances and helpful explanatory guidance.

Organisations will by now recognise that the implementation timeframe for the policy is relatively short, with a 12 month period for the initial work followed by a three year transition period for organisations to develop and embed their capability to remain within the Impact Tolerance Limits that they have set for themselves.

The policy framework sets out five key steps for achieving an outcome of Operational Resilience, which we explain below and throughout the body of this report. In this section, we provide a high-level overview of each step that organisations are required to fulfil. More in depth discussion of the practical implementation considerations involved in each step is provided within the body of our paper.



1. IDENTIFY IMPORTANT BUSINESS SERVICES

The supervisory authorities have reinforced the principle that organisations should focus on achieving resilient outcomes for end users, the organisation, and the wider sector in which they operate. The supervisory statements introduce a number of helpful clarifications to better harmonise the definitions of Important Business Services (IBSs), including, for the PRA, further qualification that IBSs are "services provided by a firm, or by another person on behalf of the firm" to create more consistency with the similar wording used by the FCA. The regulators also note that IBSs are not internal services such as payroll, but rather services that deliver an outcome to customers, clients and external end-users.

This 'outside in' perspective, coupled with the concept of the IBS has prompted organisations to embrace a significant mindset shift with respect to Operational Resilience.

Whilst it is a logical change, for many organisations the adoption of a non-functional perspective on business operations is not a straightforward one, since it requires looking at business data in a new way; a new and more expansive operating model capable of harmonising numerous disciplines such as technology, third party risk management, and Business Continuity; and a strong governance approach with proactive inter-functional collaboration.

Despite the implementation challenges that these requirements may present, it is clear from the organisations that we have worked with that the emphasis on the 'outside in' lens of IBSs is welcome both as a commercial imperative and as a means of better understanding risk exposure against essential customer, client and end-user outcomes.

2. MAP IMPORTANT BUSINESS SERVICES

The policy statements require that organisations map the supporting resources (people, processes, technology, facilities, and information) that contribute to the delivery of the IBS.

Organisations should note that the resource mapping exercise applies irrespective of whether resources are delivered or provided by a third party. However, the statements emphasise that there is an expectation that organisations will understand the reliance placed on sub-outsourcers, focussing on whether the sub-outsourcing meets the criteria of 'materiality'[1], which includes the impact on the organisation's operational resilience and the provision of IBSs. Organisations are also expected to ensure that service providers have the ability, and capacity to appropriately oversee material sub-outsourcers on an ongoing basis in line with applicable policies.

Organisations will need to gain assurance from outsourcers regarding their ability to meet the requirements set out within their operational resilience policy, and the standards that they have set (albeit that this will be commensurate with the size and complexity of the outsourcing arrangement). The operational resilience regulatory requirements have to be considered alongside the third party and outsourcing risk requirements regulatory requirements. For some organisations, there is a reasonable expectation that outsourcers may need to perform mapping activities, whilst for others annual attestations of policy compliance may suffice.

Overall, mapping is expected to be proportionate to the size, scale and complexity of the organisation's operations, and conducted in a way that is commensurate with the business. The exercise is not intended to be exhaustive but to be performed to a level that identifies any vulnerabilities to the IBS and allows for meaningful testing to be undertaken (for instance placing stress on known single points of failure).

The policy statement establishes an annual frequency for the review and updating of mapping and a requirement for more frequent updates where there are material operational changes.

3. SET IMPACT TOLERANCES

The policy statements highlight the requirement that organisations set Impact Tolerances for their Important Business Services based on the principle that severe but plausible disruptions inevitably will happen. Consequently, organisations should be able to express how they will continue to deliver their services whilst remaining within the tolerances that they have set for themselves.

Organisations should set impact tolerance for their IBSs, constituting an expression of the limit of disruption to a service that a organisation is prepared to tolerate and should not be exceeded – an Impact Tolerance Limit (ITL). The policy statements confirm that dual regulated organisations need to set two impact tolerances for an IBS reflecting the statutory objectives of the PRA (market stability) and the FCA (good consumer outcomes).

The supervisory authorities have clarified that whilst organisations may understandably focus effort on remaining within the more stringent tolerance in a dual-regulated situation, they should consider that the ITLs and desired outcomes may materially differ due to the focus of either the PRA or FCA and so simply meeting the more stringent time-bound criterion will not be sufficient – organisations will need to give thought to the nature of the impact and the disruption caused. To this end, focussing on the more stringent tolerance will be acceptable if organisations can demonstrate that they have considered both the PRA's and FCA's objectives; how recovery and response arrangements are also appropriate for the longer tolerance; that scenario testing has been performed with both the longer and shorter tolerance in mind.

Disruptions to multiple IBSs may compound impacts and, as such, organisations should consider the failure of other, related IBSs when setting impact tolerances for single IBSs. This does not negate the need to set individual impact tolerances, but rather creates an expectation that the impacts of multiple IBS disruptions are considered.

The PRA's statement accepts that 'rapid technological change' may mean that organisations can suddenly no longer stay within their impact tolerance. However, in such scenarios it expects organisations to implement a remediation plan promptly to enhance their resilience in the face of that change.

Finally, all impact tolerances must include a time-based metric, albeit that this may be expressed in different ways. The 'duration' of a disruption is described as both a point by which harm needs to be reduced to a tolerable level, as well as elapsed time (which could compress or increase depending on when a disruption occurs). Other metrics are also likely to be used expressing the level or amount of tolerable disruption. These will differ from service-to-service.

4. SCENARIO STRESS-TESTING

Organisations are required to perform scenario testing to determine if they can continue to deliver IBSs within the Impact Tolerance Limits through a severe but plausible scenario. For FMIs, the term 'extreme but plausible' scenarios is used to deconflict with other supervisory areas.

Scenario testing is not envisaged as open-ended scenario rehearsals or exercising, but rather focussed testing on known vulnerabilities identified during the mapping, other risks on the organisation's risk register, and known events that have happened elsewhere within the industry and sector. It is designed to place stress on the ability to continue delivering the service, test assumptions about recoverability, and understand where resilience enhancements are required. To this end, the thinking that firms have done around Operational Continuity in Resolution, Business Continuity and Operational Risk are helpful inputs to developing a tailored operational resilience scenario.

Through scenario testing and their response to live events, organisations are expected to learn lessons, and identify and prioritise areas requiring greater resilience.

Organisations will be expected to test their IBSs frequently but not all will be tested annually, unless there is significant change indicating that testing is needed to confirm the organisation's ability to remain within its ITL.

Lessons learned, together with associated actions and remediations, are expected to be documented within the self-assessment.

5. SELF-ASSESSMENT

Organisations will need to prepare a written self-assessment confirming their compliance with the operational resilience requirements. As with other areas of the policy framework, the requirements do not prescribe the specific format that the self-assessments should take, but have included an overview of what should be included,[2] with the observation that the level of detail and exact content will again be commensurate with the size and complexity of the organisation's operations. The FCA policy statements clarify that organisations may expect to submit the self-assessment in multiple documents and with multiple file types.

The statements confirm that, whilst self-assessments do not need to be submitted on an annual cyclical basis, they should be available on request should the regulators require them. The earliest date that a request may be made to provide the self-assessment is 31st March 2022.

A review cycle for the self-assessment is not prescribed but frequent review is expected and proactive, out-of-cycle review is required where there are material changes to internal structures or processes impacting the IBS.

The supervisors' expectation is that the Board will play a leading role in the oversight of the self-assessment, providing ultimate approval for its content. This places the onus firmly on Boards to equip themselves with the requisite skills, knowledge and capability to discharge their responsibilities for oversight of Operational Resilience.

COMMUNICATIONS

Communications strategies are of integral importance to developing Operational Resilience, and organisations should develop communications strategies for both internal and external stakeholders as part of their planning for operational disruptions. Communications strategies should set out escalation paths for managing incidents, identify key decision-makers and determine how to contact key individuals, suppliers and the regulators.

The FCA statement notes that organisations may re-purpose existing communications strategies or plans provided that the originals are maintained in line with their primary purpose.

Consistent with their mandate, the FCA is primarily interested in how communications can be used to reduce the overall harm caused to customers, and especially vulnerable customers, during a disruption. Organisations should view their communications plans as integral to their mitigation strategies and not as ancillary to the broader Operational Resilience principles.

Communications strategies should set out escalation paths for managing incidents, identify key decision-makers and determine how to contact key individuals, suppliers and the regulators.

INTERNATIONAL REGULATORY COORDINATION

International regulatory compatibility and coordination will clearly be crucial for Financial Sector organisations as authorities around the world propose new Operational Resilience requirements. The UK regulators make clear that, while local requirements will not be perfectly aligned, they believe there is strong alignment in the core principles and mindset between emerging frameworks, and particularly between the UK framework and the Basel Committee on Banking Supervision's draft principles for Operational Resilience. As a result, they commit to working closely with their international regulatory counterparts and also state that they believe that international organisations will be able to 'work effectively across borders' in the area of Operational Resilience.

In December 2020 the PRA, as well as the European Central Bank and the US Federal Reserve released joint statements on their intention to cooperate in the supervision of the operational resilience of banks. In it they recognised the interconnected nature of cross-border banks and the shared interest between them as regulators in strengthening the operational resilience of the banking sector.

As we have written before, we believe that the level of regulatory convergence and supervisory coordination in operational resilience is an encouraging trend. To read more of our analysis on international regulatory alignment in Operational Resilience and what this means for organisations, please refer to: Resilience without borders: How financial services firms should approach the worldwide development of operational resilience regulation.

1. Identify Important Business Services

Organisations should identify the business services that they provide and determine their importance in relation to the adverse outcomes their disruption can cause to customers, clients and end-users; the viability of the organisation; and the stability of the broader sector.

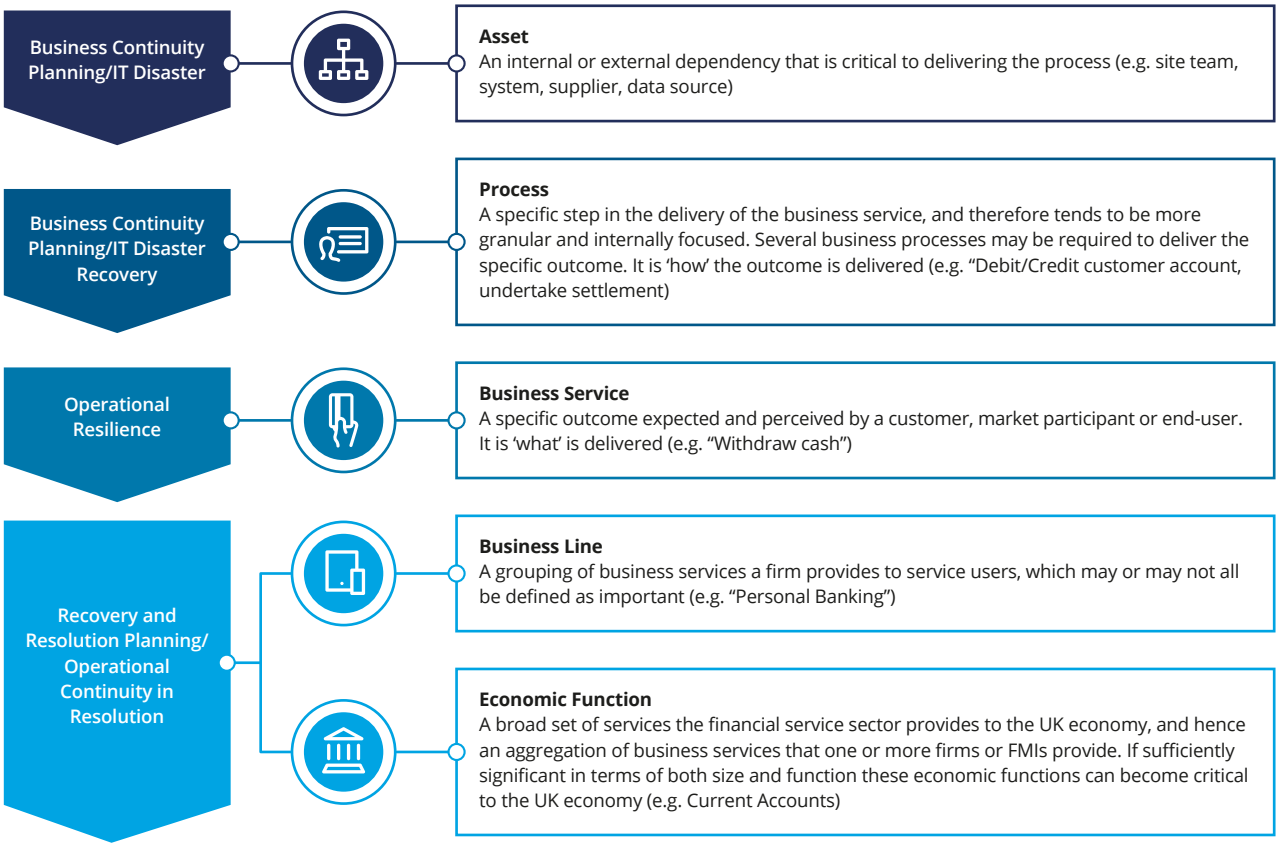
Characteristics of Business Services

In our 2019 publication 'Time to Flourish' we described a business service as the outcome expected and perceived by the end user – i.e. the 'what' is delivered.

This needs to be established before the 'how' it is delivered (which focuses more on granular, internal business processes). We also stated that the economic functions identified through Operational Continuity in Resolution (OCIR) and related initiatives, although not synonymous with business services, can help identify these. The diagram below provides a comparison of business services against other views used as the starting point for preparedness activities.

Many organisations have already undertaken work to understand the key interactions with, and key moments for, their clients and customers. Initiatives such as 'customer journey' mapping provide a useful outside-in perspective that can support the identification and articulation of business services. We believe that organisations should catalogue their business services, to both provide the basis for their prioritisation and transparency over which business services are not considered important.

Figure 1. Contextualising Important Business Services



To support the identification and cataloguing of business services we have found it useful to use the following criteria, all of which need to be met:

- **Is a distinct outcome** (the 'what' not the 'how' e.g. "making a claim")
- **Is provided to and recognised by an external end-user** (internal functions like IT or Payroll are not business services)
- **Is a separate service** (distinguished from business lines which are a collection of services e.g. "making a claim" and "receiving claims settlement" are separate services, whereas "Claims" is not)
- **Is not channel-specific** (multiple channels recognise alternate ways of delivering the service which is useful for resilience; however, "Making a claim online" would not be considered its own business service unless this was the only means by which to make a claim)
- **Can be described simply from an end-user perspective** (does not need technical language to describe)
- **Accountability is held by the Organisation** (even if it is delivered by a third party)

We believe that this activity is most effective when undertaken through workshops with appropriate subject matter experts who can help validate the catalogue and its supporting rationale. While we do not believe it is necessary for organisations to identify individual products as part of this, they should consider if certain products have distinct outcomes associated with them. For example, health insurance products have end-user outcomes not associated with more general property and casualty insurance products (e.g. receiving required care/treatment).

Characteristics of Important Business Services

Important Business Services are those business services whose disruption could cause intolerable levels of harm to one or more of the organisation clients, pose a risk to safety and soundness of the organisation, impact market stability of the sector. 'Intolerable harm' to customers and clients is a category that is new compared to conventional impact assessment approaches. The FCA describe intolerable harm as harm from which consumers cannot easily recover (e.g. an organisation 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). The Policy Statements also provide examples of these categories, including data points that organisations could use to assess against (e.g. percentage of market share, volume of customer base impacted, integrity and availability of data).

While organisations may repurpose existing impact and criticality criteria and matrices, we believe that the application of the impact categories to identify Important Business Services is primarily a qualitative, judgement-based decision, supported by a clear, simple rationale and appropriate data points. Through our work with organisations we have found it more efficient to select characteristics of importance first and then identify potential supporting data points (rather than collecting data points and then deriving characteristics).

Example characteristics against impact criteria are given below:

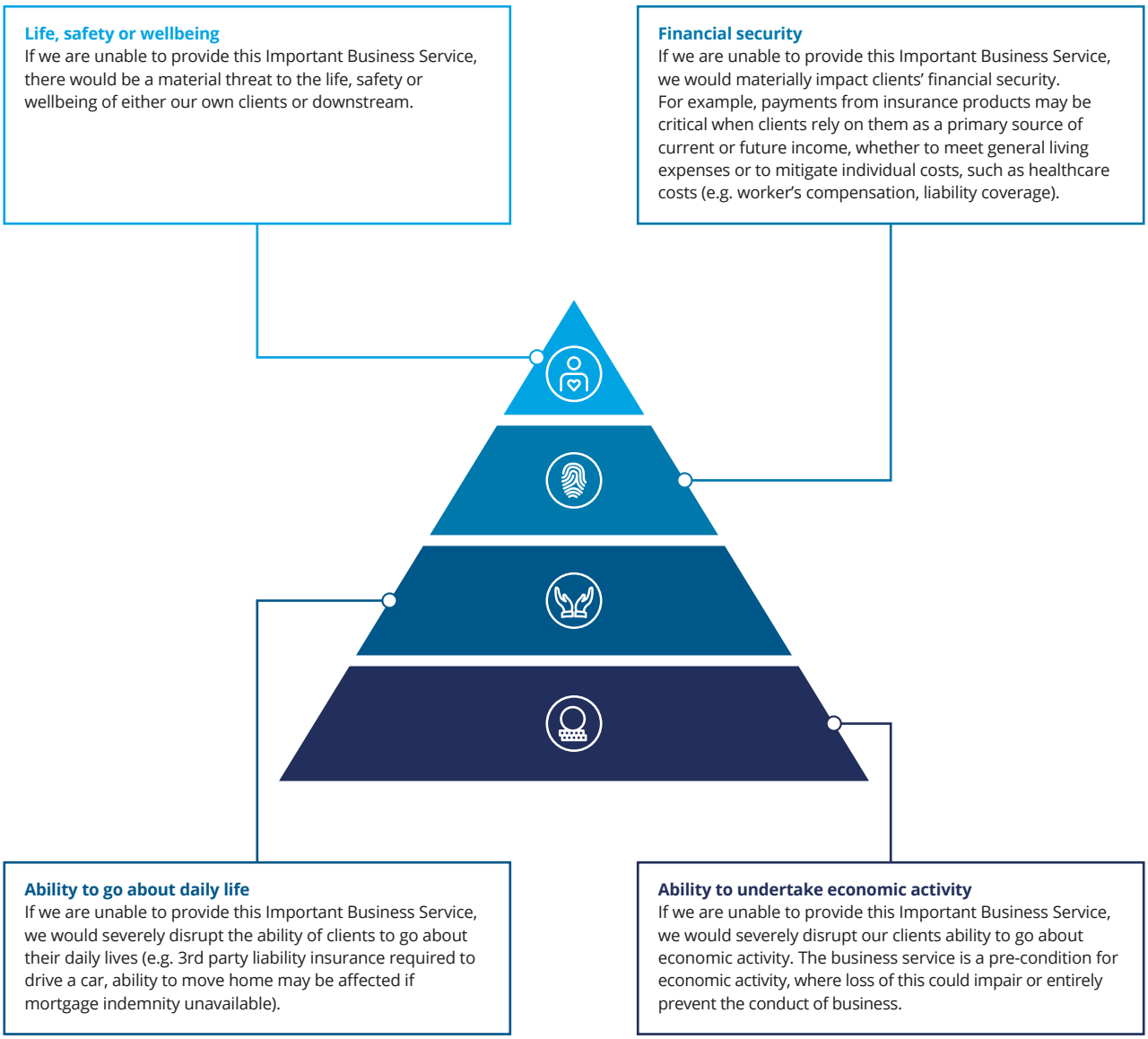
- **Intolerable harm to one or more of the organisation's clients:**
  - There are customers or clients who would be more susceptible to harm from a disruption or feel it more acutely because the service is:
    - » Vital to their health or financial security
    - » Vital to their ability to undertake economic activity
    - » Needed as a precondition to go about daily life
  - Linked to the above point, severe distress would be caused to clients and customers if the service cannot be provided when needed, and cannot be obtained easily from another provider
  - The disruption would result in severe financial detriment for clients/customer that cannot be easily corrected
  - A significant number of clients that use the service would be impacted (e.g. due to major market share of the service)
- **Financial stability:**
  - Disruption would be caused to broader markets
  - There would be damage to confidence in markets
  - Market prices would be negatively impacted
  - Disruption would be caused to counterparties
  - There could be disruption to financial system stability because of the organisation's role as a key market maker and dealer of a number of products
  - Risk of contagion to other financial services organisations who rely on the organisation's services to operate
  - The service is considered important to the UK financial system because:
    - » It supports a Critical Economic Function (CEF) identified by the regulators
    - » It includes concentrations of sensitive clients (e.g. governments, pension funds)
- **Organisational safety and soundness:**
  - There would be severe damage to the organisation's liquidity and financial position including: i) loss of profit, ii) costs to the organisation, iii) impact on share price, iv) withdrawals from funds, v) loss of future business, vi) policyholder protection, etc.
  - There would be severe impact to the organisation's regulatory and legal position including: i) regulatory fines and sanctions, ii) regulatory scrutiny, iii) governmental attentions
  - There would be severe damage to the organisation's reputation including: i) lost investments, ii) adverse analyst report, iii) adverse media commentary, iv) loss of confidence in management demonstrated by stakeholders and/or staff

Having a commonly understood set of characteristics from which to assess the importance of business services will support their validation with senior management and subject matter experts. This should be undertaken as part of internal cross-checking to understand if the business service or elements of it have been in scope of other related programmes (e.g. OCIR, BCP) and where this is not the case, if its identification as an Important Business Service is justified. Similarly where organisations undertake comparison with peer organisations, it is crucial to understand that there will be differences between peers, even if they are very similar – the importance is that the reason for the difference can be rationalised (e.g. by different market share, different services offered, different amounts of captive clients).

We believe that the assessment of the importance of a business service should be performed both at a local and global level – a service that is not important from a global perspective could be so from a local perspective.

The diagram below presents a 'hierarchy of harm' which can help to focus thinking when identifying IBSs.

Figure 2. The 'hierarchy of harm'



Business Service Ownership

The implementation of the regulatory framework will require organisations to establish clear ownership, accountability and responsibility for business services.

Operational Resilience teams should consider that whilst they may facilitate the process of identifying and rating business services, ultimate decision-making and long-term ownership sits within the business and with those who are closest to the delivery of service outcomes.

Identifying the correct individuals to make decisions and interventions relating to the resilience of business services can be a challenge: Business Service Owners should be sufficiently senior that they are involved in the organisation's strategic analysis and planning, but not completely removed from the practicalities of operational delivery.

In practice, Executive level owners may ultimately be accountable for business services but choose to delegate day-to-day responsibility to business service champions who are closest to operational delivery.

It is helpful for Operational Resilience teams to appoint relationship managers to support business service champions in understanding, for example, changing risk profiles relating to the service or whether service performance degradation is simply anomalous or could constitute a general trend towards an impact tolerance breach.

Board sign-off and approval

Boards should have ultimate accountability for IBSs and for their associated impact tolerance statements. Therefore, Operational Resilience teams will need to build confidence in the approaches that they are using and seek approval from the respective Board or Boards for the list of IBSs that they identify.

However, it will be incumbent upon Board members to ensure that they are collectively equipped with the requisite skills and knowledge to ask the right questions, to understand whether importance is robustly rationalised, to query omissions, and to understand the implications for the organisation's risk exposure where services are not considered to be within the scope of the programme. Building awareness, capability and confidence through robust and insightful MI and reporting can help here, as well as Board level participation in resilience testing and training activities.

2. Map Important Business Services

The policy framework requires organisations to understand the make-up of each IBS including the supporting resources – people, processes, technology, facilities and information – that are needed to deliver them, including where these are delivered by third parties.

IBS blueprinting and channel bias

Developing a blueprint of the Important Business Service is a useful output that can be shared with senior management to help facilitate understanding of key customer interactions and inherent vulnerabilities within the service.

Customer journey maps, where these exist, may prove useful as an accelerator in developing service blueprints, but these will often be done through a channel, rather than a service lens, and so will require some modification.

Operational Resilience teams should also in general avoid placing too much emphasis on channels (i.e. how the service is delivered) and focus instead on the outcome ('what is the outcome for the customer?'). This will minimise failures of imagination when it comes to building resilience (i.e. 'we deliver this outcome through this channel, it's the only way we can do it').

IBS blueprinting should be cognisant of channels, but focus on the key steps needed to deliver the service from end-to-end and from surface to core through customer-facing interaction points and central support functions to eventual outcomes.

Blueprints should include a high-level view of the resources (technology, teams or functions, facilities, information, processes) as well as reflecting any critical processing deadlines and peak periods in the delivery cycle.

The business architect's view

Those organisations that have enjoyed the most success at the mapping stage are those that have started with a high-level, business architectural view or blueprint of the IBS, rather than exhaustive bottom-up mapping.

The architectural view aims to illustrate the end-to-end delivery of the business service from the point of obligation (i.e. the point at which an organisation takes on a commitment to deliver an outcome for a customer, client or end-user) to the point at which that obligation is fulfilled.

In our experience, developing a picture of how the end-to-end service is delivered is best captured by Operational Resilience teams and validated in a workshop with cross-functional representatives who can identify customer touchpoints; central support functions (e.g. Payments Operations) who can articulate supporting processes and flows; and commercial and business relationship managers who can describe service operations and constraints, including those that are outsourced.

Architectural views may incorporate elements of customer journey mapping so organisations that have invested time and effort in developing front-to-back business process maps or customer journeys may be able to re-purpose elements of these to inform their IBS maps.

Identify internal and external resources

Organisations are required to identify all of the supporting internal and external resources (people, processes, technology, third parties, facilities and information) that make up the IBS.

Resources should be mapped to the end-to-end business service, helping to develop a picture not just of the assets and processes required to deliver the outcome, but also of the underlying vulnerabilities, single points of failure, and inherent resilience within those resources as well as any critical processing deadlines and peak periods of activity that they involve.

To map effectively, Operational Resilience teams will need to bring together SMEs from each of the resource areas and the business to understand how the service operates today and to bridge the gap between technical support teams and business users. For instance, business users may refer to applications in different ways from technology teams, or, depending on the maturity of the organisation's data management approach, may require clarification on data categorisation, processing and handling.

It is also helpful at this stage for organisations to consider any inherent or pre-existing resilience arrangements within the service and how viable or sustainable these strategies are. In addition to any recovery time and point objectives (RTOs and RPOs), it is helpful for organisations to capture:

- **Modularity** – where the service can be fulfilled by more than one resource (for example, workloads split between teams or suppliers; load balancing of cloud-native applications or network traffic)

- **Redundancy** – where there is excess capacity within the service (e.g. back-up systems; tertiary storage)

- **Substitutability** – where the primary delivery mode can be reasonably fulfilled by an acceptable alternate (e.g. alternate supplier)

Business process mapping

Since business services do not exist as an organisational structure or attribute in their own right (i.e. they are an outcome of a collection of processes and functions working together), they need to be mapped to business processes and supporting resources so that they can be brought to life, proactively monitored, measured and reported on.

This will mean understanding and defining the business process hierarchy and using business processes as the common denominator to map resources to the IBS.

Where limited prior business process mapping (BPM) activity exists, the mapping exercise may seem overwhelming and organisations should take steps at the outset to understand the level of granularity that is likely to prove insightful when it comes to determining risk exposure and building resilience.

Conventional business process hierarchies comprise four or five levels:

- Level 1: Operations
- Level 2: Mega-processes
- Level 3: Processes
- Level 4: Sub-processes/activities
- Level 5: Tasks

Organisations will typically find that levels 1 and 2 only provide a management function view and need to be broken down further so that critical resources and vulnerabilities of the end-to-end service can be identified. Levels 4 and 5 are likely to be too granular and mapping will become too exhaustive to be sustainable, and, there is likely to be limited differentiation in the use of resources so both the risks involved and the resilience solutions may look the same.

In practice, most organisations will find that Level 3 is optimal with selective mapping at Level 4 only where there is low confidence over risk exposure and mitigation (e.g. where the process has resulted in a high volume of Notifiable Events or Near Misses or persistent key control failures).

Select BPM tooling

Organisations will need to consider optimal tooling solutions for BPM early in the design and implementation journey since the data generated through the mapping exercise will quickly outgrow Microsoft Excel and Visio, though these tools may suffice at the initial blueprint or architectural level.

At this stage, it will also be important to think about the bigger picture for Operational Resilience working with enterprise architecture teams and the Chief Data Office to consider viable strategic solutions to data modelling, management and tooling.

For some organisations, the process of BPM and service mapping will require them to overcome a significant digital and data barrier and may involve conversations around re-architecting or re-purposing of data and housing an Operational Resilience data model within a data warehouse or lake (see section 6 below on next generation Operational Resilience).

Whatever decisions are taken, it will be prudent from an investment perspective that they are strategic ones, adopting the principle 'build once, use multiple times' and serving other needs within the business where possible and practical to avoid the accrual of unnecessary technical debt.

3. Set Impact Tolerances

Impact Tolerance describes the maximum acceptable level of disruption for each of the organisation's IBSs, assuming disruption to the supporting systems and processes. We have called this point an Impact Tolerance Limit (ITL).

ITLs determine the level of service to be achieved within a certain timeframe or by a point in the business cycle, after which the impact becomes intolerable. They provide the 'benchmark' for operational resilience for the IBS (i.e., the organisation will need to ensure the service can be maintained within the Impact Tolerance Limit under severe, or in the case of FMIs extreme, disruptions. This is non-negotiable from the Supervisory Statements perspective).

Impact tolerance statements will therefore help focus investment on resilience measures and should inform decision making during a disruption (e.g. support prioritisation of certain actions).

Following the publication of the policy framework, organisations now need to think carefully about how they construct their impact tolerance statements, given these will be used as success criteria for stress testing and will frame investment decisions around operational resilience. One of the main considerations organisations need to make is finding the balance between qualitative vs quantitative (judgement vs data) analysis to help determine intolerable harm and tolerance thresholds.

Developing impact tolerances runs the risk of getting lost in reams of data to try to find answers. We should remind ourselves throughout an Operational Resilience programme that the regulator's intentions are for a proportionate response. Determining where, and how deeply data analysis can support the setting of ITLs is important, and in our view striking the right balance between 'art (common-sense judgement based on a clear understanding of impacts) and science (data-driven analysis to support or validate the judgement)' is essential.

Disambiguating impact tolerance and risk appetite statements

Impact tolerance and risk appetite statements are related to one another but do have crucial distinctions. Simply put: a risk appetite statement describes the amount of risk that the organisation is prepared to tolerate – at this stage the risk has not been assumed to have materialised. By contrast, an impact tolerance statement refers to the amount of impact that is acceptable before irredeemable harm is caused to customers, markets, the organisation itself, or financial stability is threatened. Impact tolerance is indifferent to specific risks or likelihood since it assumes that the service cannot be provided (and therefore one or more risks have already materialised).

The supervisory authorities require that organisations set impact tolerance limits assuming that disruption will happen and, as such, impact tolerances statements do not imply a zero appetite or tolerance for disruption.[3]

ITLs determine the level of service to be achieved within a certain timeframe or by a point in the business cycle, after which the impact becomes intolerable.

Setting ITLs

Looking at this through a simple, but methodical approach has its benefits and we recommend breaking it down into four steps, with the aim of using judgement to better guide the data needed:

1. Tell the impact story

It is difficult to understand what impact is tolerable without firstly understanding what the impact could look like, and how it might change, as a disruption to an Important Business Service becomes more severe (e.g. it becomes prolonged and/or more widespread). Telling a simple 'impact story' can help identify where impact changes happen, consider the 'what if' should we breach desired recovery objectives and service level agreements; and helps to build consensus on what intolerable impact looks like. This could be done through a workshop, and should aim to describe the following stages of increasing severity:

a. The immediate impact at the point of disruption (i.e. when the IBS can longer be provided).

b. The impact at the point by which we would have ideally wanted to recover the service by (e.g. in line with SLAs or recovery time objectives), expecting that this would be inconvenience rather than long-term harm.

c. What the impact would be if we didn't meet our desired recovery objective or SLA, and how the impact would change (i.e. from inconvenience to harm, the nature of the harm and to who or what) as the disruption becomes more severe (e.g. goes on longer, becomes more widespread), affects specific activities (e.g. those needed by customers to go about daily life). Impact should be considered against clients or customers, markets, financial stability and the safety and soundness of the organisation.

d. What would characterise the point of intolerable impact, that is, the point at which the harm caused is so acute, long lasting or widespread, or threats to organisation viability and/or market or financial stability have crystallised (e.g. customers defaulting, wind-down plan thresholds breached).

Understanding how an increasingly severe disruption affects customers, the market/sector and the organisation themselves enables the identification of impacts that might have otherwise been missed. Key to this is engaging different perspectives in the conversation, including those from client services teams in addition to operations and technology teams. The rationale for why the business service was considered important in the first place will help here.

2. Identify and gather relevant information and data

Through developing the impact story, organisations will identify information or data needed to validate/change and ultimately complete the story. This will include baseline data to understand the business-as-usual functioning of the IBS and any periods of heightened demand or critical business processing deadlines. This information should be gathered over a reasonable timeframe taking historic data from a period, ideally, of more than 12 months so that cyclical patterns and exceptions can be identified.

Key sources of data will include performance indicators such as daily transactional volumes and values, timeframes, or customer types that help underpin the rationale for why the impact changes (e.g. inconvenience, to harm, to intolerable harm). These data points should be logged and followed up with appropriate subject matter experts before being incorporated back into the overall impact narrative developed in step 1. Some of these may have already been identified when the business service was identified as being important in the first place. The data points will help to form the basis for the tolerance threshold described in step 3 below. These data will help to build a picture of the overall health of the service and how it operates day-to-day.

3. Set the impact threshold

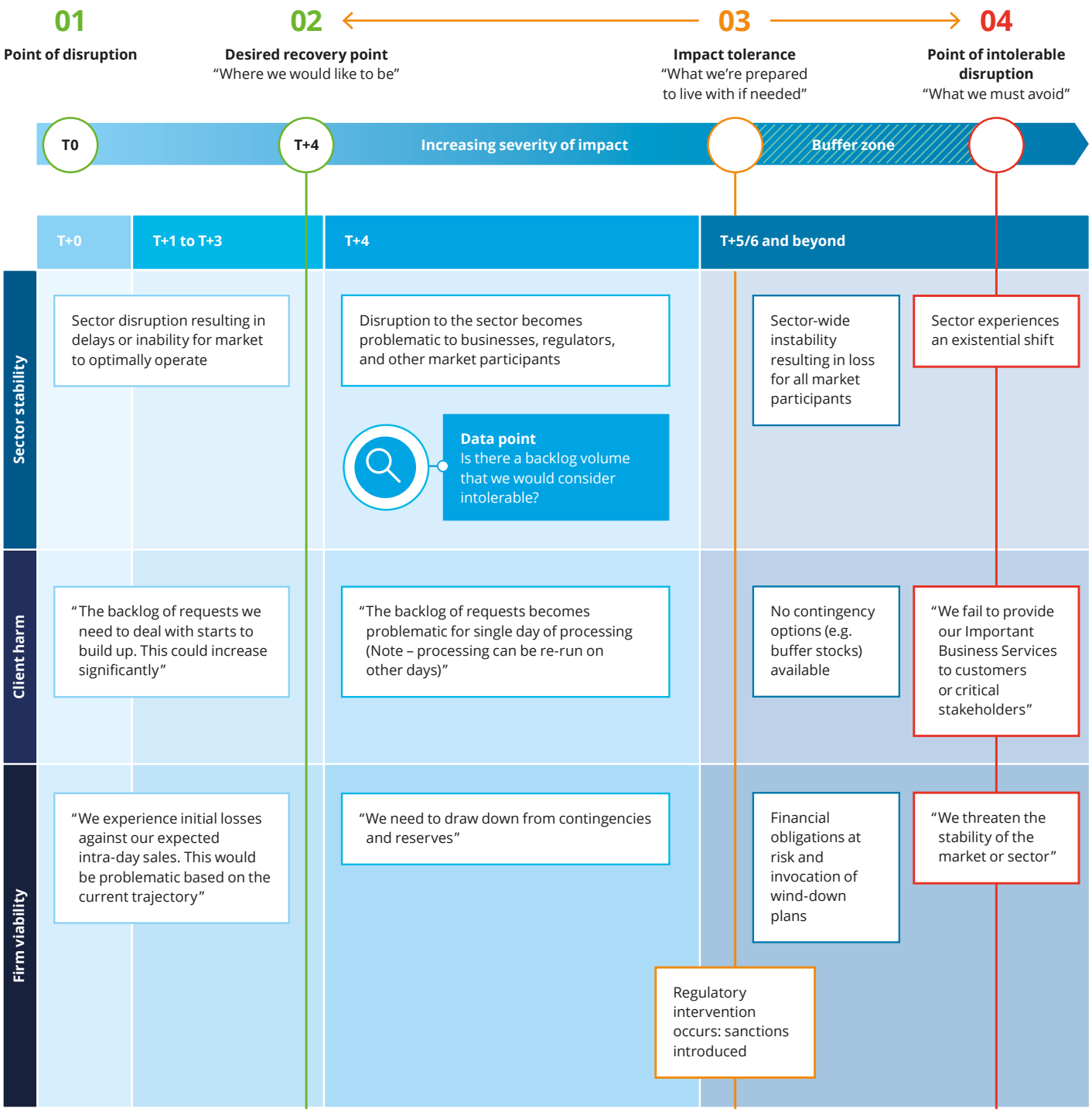
The completed impact story should be used to determine the Impact Tolerance Limit. Where this lies will be based on the impact descriptions, but setting the limit too close to the point of intolerable impact ('D') may indicate the organisation is willing to accept significant harm. Conversely setting the threshold too close to the desired recovery point ('B') could result in greater investment in resilience being required. Organisations should judge where between those two points the threshold should lie so that it balances the need to mitigate intolerable impact with an appropriate level of investment and effort.

To set a tolerance threshold, organisations should focus on two main metrics:

- A durational metric (this can be flexible, e.g. Maximum Tolerable Period of Disruption – MTPOD, or a specific point in the business cycle); and,

- Maximum Tolerable Level of Disruption (MTLOD)

Figure 3. The Severity Line



Metrics will be unique to each IBS. The MTPOD should take account of any key timings within the delivery cycle and assume that disruption happens at the worst possible point within that cycle. The MTLOD may be volume, value or relate to specific customer groups (e.g. vulnerable customers).

In setting ITLs, organisations should aim to validate the limits that they set by referring back to historical data that they have gathered which will help to corroborate tolerances by comparison to business-as-usual functioning and real world impacts that similar disruptions have caused. This will also aid understanding of what an 'intolerable' impact could like. As part of this, they may also consider substitutions and recovery arrangements, as well as contingencies and interventions that may bring down the impact.

The diagram above includes a 'severity line' which can be used to focus discussions in workshops to set impact tolerances. The severity line is used to help tell the story of how impact changes as a disruption becomes more severe and what drives this change (e.g. duration, scale, types of clients impacted).

This helps to determine a commonly agreed point of intolerable disruption, which can form the basis for defining the impact tolerance further.

Dual-regulated organisations will need to bear in mind that they may need to set two ITLs:

- For the PRA, ITLs will be informed by potential adverse impact to the organisation's safety and soundness or financial stability or, for insurers, the relevant degree of policyholder protection

- For the FCA, ITLs will be informed by potential adverse outcomes for consumers, the stability of the financial system, impacts on the orderly operation of the market, and loss or damage to the confidentiality, integrity or availability of data

In setting ITLs, organisations should capture a set of working assumptions to help contextualise their impact tolerance statement(s), avoid over complicating them and document their rationale for choosing the limit(s).

4. Develop outcome-based objectives
The final step should be the development of an impact tolerance statement. The statements should be simple and expressed as an objective to be achieved in a disruption, and must include time-based and other relevant metrics (e.g. complete a percentage of transactions with a specified timeframe or by a certain point in the day). Expressing an impact tolerance this way will help both as success criteria for scenario testing, as well guide response actions when a disruption occurs. ITLs should finally be explained to, understood and formally approved by the Business Service Owner and relevant Board(s).

The regulators have made clear that impact tolerance statements should show an appropriate level of resilience in the face of severe but plausible scenarios. It has also been made clear the onus is on the organisations, not the regulators, to set these impact tolerance statements, and these should be tailored by each individual organisation. That said, organisations should understand the full context of existing regulatory work as they undertake this analysis. The Financial Policy Committee's (FPC) 2019 'pilot' cyber risk stress-test set an important benchmark for how the most systemically important organisations should think about impact tolerances using the financial market stability lens, in terms of the scenario and stress levels used, but also the impact tolerance expected by the FPC. In 2022 the FPC will run a follow-up 'exploratory' cyber stress testing initiative with a more challenging scenario based on data integrity. These tests should be given careful consideration by organisations even if they are not involved in the pilot or exploratory exercises.

Organisations should consider the increased effect on intolerable harm if a single event causes multiple Important Business Services to be disrupted, or if multiple Important Business Services are disrupted through unrelated but simultaneous disruption. This might be from the failure of a shared resource or a widely impacting external event. However, there is no requirement to add a further impact tolerance statement per Important Business Service to cover off this additional thinking.

Those organisations unable to prove their ability to remain within their ITL will have a reasonable period[4] (up to a maximum of three years from 31st March 2022) to make the necessary investments and improvements in resilience to achieve this.

The PRA has also observed that, where rapid technology developments may mean that a organisation finds that its services are suddenly outside the ITL that they have set for themselves, they will be expected to put in place a rapid remediation plan to address this. This will require strong governance and proactive escalation from those responsible for resilience, escalating any issues that emerge outside IBS review cycles and establishing practical, proportionate and timely steps to remediate them.

Impact Tolerance Statements
Impact Tolerance Statements are an expression of the organisation's intent with respect to remaining within the impact tolerance limits that they have set for themselves. The key features of a good impact tolerance statement include:

- Derived from the upper limits (MTPOD and MTLOD) that the organisation identified and beyond which the disruption would be deemed intolerable
- Express a statement of intent for remaining within the ITL
- Describe the specific outcome that will be achieved

An example may be:

"In the event of disruption we must be able to execute 80% of average BAU trades within 48 hours and process 75% of client orders within 72 hours."

4. Scenario stress-testing

Scenario stress-testing should be used to determine whether an organisation can remain within impact tolerances under severe but plausible scenarios (or extreme scenarios in the case of FMIs).

The scenario test will highlight where vulnerabilities exist and guide investment choices to enhance resilience. To be effective, and to satisfy regulatory expectations, scenario testing must also include the dependencies that lie outside the organisation through material outsourced provision and sub-outsourcing arrangements.

The policy statements do not prescribe a particular method for scenario testing and instead encourage organisations to conduct testing that is proportionate to the impact potential disruption may cause. This means organisations need a flexible and agile approach to testing that can increase or decrease the severity and scale of testing.

The policy statements do, however, indicate the types of testing they might expect. These are not exhaustive and can be applied practically in a number of ways. They are also indicative of the level of maturity and sophistication in relation to testing; an organisation with a well-established resilience testing regime may be comfortable to undertake more complex scenario testing of important business services relatively quickly.

The regulators call out three types of test:

i. Paper-based assessments – a review of the documented technical and operational procedures required to recover business services;

ii. Simulations – involves putting into practise the response to a disruption, including detection, invocation, coordination, team work and information flows;

iii. Live-system tests – rehearsing the physical recovery of a particular asset in a coordinated and controlled manner (e.g. failover or full interruption testing).

Regulators are expecting an incremental and increasingly sophisticated approach to scenario testing. During the first 12 months of implementation organisations should be focused on proportionate activity that identifies vulnerabilities for remediation activity to be undertaken, should it be necessary. Testing maturity will increase over time as organisations adopt more sophisticated approaches, such as scenario modelling.

Simulations have been common practice for some time, but they focus on rehearsing organisation, coordination and information management processes, communications and decision making. The regulators require an integrated test plan, covering the various types of testing modes, which support each other.

Simulations should look more closely at the practicalities of putting the theory into practice and should be complimentary to scenario testing (paper-based) and live-tests. They test different aspects from those tested in scenario and live testing and should cover a wide range of scenarios looking across the entire chain of activities that support Important Business Services.

Simulations are based on a scenario and may impact one or more IBSs, and can also include the interaction each has on the other (common dependencies, common resources, reliant outputs from one important business service to another, etc.). They may be used to provide further evidence of the ability of the IBS(s) to remain within impact tolerance.

Live system testing may present the biggest challenge and should be approached with consideration to the impact that such testing may cause to live operations. Live tests aim to prove that an organisation can recover a specific asset or assets within an agreed time period. These are typically pass or fail tests (unlike a simulation test where there is more subjectivity in the outcome). Organisations should think about using techniques such as Digital Twins that help them to mature from paper-based to model-based scenario testing. Digital Twins enable organisations to run different 'what if' scenarios through the model to assess whether impacts remain within impact tolerance limits (see section 6).

Practicalities of scenario testing

1. Severe but plausible scenarios

In creating the context to test IBSs the regulator offers clear direction that the focus should be on severe but plausible scenarios. This means where the nature, scale or scope of the event goes beyond pre-considered measures and supporting assumptions. Organisations will have to think beyond conventional risk management and Business Continuity approaches when creating the right scenarios. It is worth noting that regulators do not require organisations to create scenarios that are existential – where the impact and plausibility is outside the scope of rational and reasonable planning assumptions – and instead to use a proportionate approach that will achieve the aim of scenario testing.

2. Selecting scenarios

When selecting scenarios organisations will find they have a range of sources to draw from, including historical data and near misses – both internally and from published cases outside the organisation. Internally, considering existing approaches to areas such as Recovery and Resolution Planning, ICAAP analysis, ICARA, customer journey mapping, operational resilience mapping, risk registers, etc., will help focus on the areas that can be leveraged. Externally, national risk registers, industry publications and insights, regulatory publications, cross sector events, and known events at other organisations can help stretch the thinking and plausibility of scenario design. It is worth remembering that the focus is not on the likelihood of an event occurring; operational resilience assumes the disruption has happened and a risk has crystallised; severity of impact and plausibility are the key considerations.

Scenarios should also be focussed on the absence or compromising of specific features of the IBS, not open-ended scenarios such as those used for Simulation tests. For comparable activities, organisations can consider the development of financial stress-testing and market-wide cyber stress-testing scenarios.

Scenarios should include one or a combination of the following (non-exhaustive) factors, affecting the delivery of IBS:

- Corruption, deletion or manipulation of critical data
- Unavailability of facilities or key people
- Unavailability of critical third-party services
- Disruption to other market participants
- Loss or reduced provision of technology
- External events, including cyber events

3. Structure and categorisation of scenarios

In order to allow an approach which can increase or decrease the severity and scale of the scenario three elements should be considered:

i. **Operational category** – There are five separate operational categories that a scenario should take account of: i) technology, ii) third parties, iii) people, iv) facilities, and v) information. These can be based on a real-world example, for instance a failed technology upgrade leading to a period of system unavailability or performance degradation.

ii. **Design variables** – Each of the operational categories can have design variables that change the way the base case scenario is derived. For example, the source of the issue (internal versus external), system impacts (confidentiality, integrity or availability), the nature of the failure (e.g. degradation, complete failure/loss of availability, loss of integrity).

iii. **Stress variables** – Stress variables can be used to alter the severity and complexity of the scenario. Typically, these would focus on duration, scope, volume, magnitude, and the removal of assumptions, particularly relating to recovery timescales or capability. By 'dialling' each up or down, scenarios can be adapted to present different challenges and variable stressors.

4. Scenario catalogue

Scenarios should be collated into a catalogue to capture the base (headline) scenarios, with a view then to creating multiple variants based on the design variables and apply increasing stress levels by using the stress variables. The catalogue can help to understand the breadth and coverage of testing across Important Business Services; some scenarios may impact multiple Important Business Services, others may focus on just one. It is within the scenario catalogue where the scenario headlines should also be captured; which IBS(s) the scenario impacts, (e.g. 'inability to trade due to fund liquidity issues'), as well as which design variables and stress levers could be applied.

Desirable outcomes

The objectives of scenario testing should be to confirm any known vulnerabilities or to identify any hidden ones, as well as to understand any gaps or weaknesses in contingency arrangements.

Simple scenarios may include testing the failure of critical components identified during the mapping stage and evaluating whether proven recovery arrangements and/or contingency measures are sufficient to keep within the ITL. More sophisticated scenarios will vary the inputs to the scenario, removing more than one critical component or adjust stress levers, for example, asking 'what if' the recovery took significantly longer or did not work.

The overriding aim of scenario testing is to confirm that the organisation can remain within the ITL that it has set for itself. Poor testing outcomes will require action to improve the resilience of the IBS(s) concerned. Ultimately, scenario testing may identify the need for further investments in resilience.

Common pitfalls of stress-testing

- Stress-testing needs to identify 'breaking points' in the organisation's ability to meet Impact Tolerance Levels (ITL), by dialling up the stress of the scenario and removing assumptions around successful continuity and recovery
- Stress-testing is not the same as Crisis Management exercising or Business Continuity Plan testing – it is based on focussed, not open-ended scenarios
- Organisations need to consider both external and internal events ('meteorites' vs. 'time bombs')

5. Self-assessment

The policy statement clarifies the expectations around the availability of self-assessments, noting that although they should be available when requested, organisations will not be required to submit these to the regulator on a defined schedule.

Self-assessments will, however, be submitted for Board approval once services have been defined and rated for their importance and stress-tested and should be re-submitted where there are any material changes and especially where it these changes result in the organisation being unable to remain within the ITLs that they have set.

Objectives of the self-assessment

The primary objective of the self-assessment is to provide a clear view on the Operational Resilience of the organisation's IBSs, and whether this is sufficient to remain within impact tolerances under a range of severe but plausible scenarios. Where Operational Resilience is insufficient the self-assessment should call out what actions are being taken to address this and by when.

Self-assessments should aim to describe:

- The organisation's **Important Business Services**, including the methodology that they have used to determine these
- The **Impact Tolerance Limits** set for these important business services
- The organisation's **approach to mapping**, including how the organisation has identified its resources, and how it has used mapping to identify vulnerabilities and support scenario testing
- The organisation's **strategy for testing** its ability to deliver IBS within ITL through **severe but plausible scenarios**, including a description of the scenarios used, the types of testing undertaken and the scenarios under which organisations could not remain within their ITL
- An **identification of the vulnerabilities** that threaten the organisation's ability to deliver its IBS within ITL, including the actions taken or planned, and justifications for their completion time
- The organisation's **lessons learned** exercise
- The **methodologies** used to undertake the above activities
- The organisation's **communications strategy** and how this will enable it to reduce the anticipated harm caused by operational disruptions
- Any actions planned to **improve their ability to remain within impact tolerances** and a justification for why the **timing of any planned actions are reasonable and in proportion** to the systemic importance of the IBS

Principles for good self-assessment templates

The supervisory authorities do not prescribe a template for completing self-assessments so organisations should consider the objectives outlined above and apply the following principles as they develop the content:

- **Evidence-based** – Content is based on sound evidence and not interpretive or aspirational
- **Transparent** – Self-assessments describe any working assumptions and limitations in the approach
- **Proportionate** – provides a level of detail commensurate with the size and complexity of the organisation's operations
- **Relevant** – provides essential but not exhaustive information and addresses the relationship between impact tolerances and the organisation's risk appetite
- **Timely** – Self-assessments should be updated regularly, and when material changes have occurred, to reflect the current state of operational resilience

Self-assessments should be signed off and approved by the relevant BSO, SMF24 and Board(s).

Governance, culture and operations

The effective implementation of the Operational Resilience framework will be determined by the strength of the governance and operating model that the organisation puts in place to support it.

Effective governance

Organisations implementing the regulatory policy should consider Basel Principle 1, using their existing governance structures for the oversight and management of Operational Resilience. However, organisations should be cognisant that existing governance structures may be built around management functions and do not always lend themselves to the lens of horizontal, end-to-end business services and the inter-functional collaboration that is essential to overseeing them.

For organisations subject to the PRA's SM&CR, regime, the management of Operational Continuity, Resilience and Strategy sits under the SMF 24, together with disciplines critical to the outcome of operational resilience, including:

- Business Continuity
- Cyber Security
- Information Technology
- Internal Operations
- Outsourcing, Procurement and Vendor Management
- Shared services[5]

The SMF24 is an exception to the general principle that SMFs can be shared but not split, since it can be shared or split between two or more distinct but equally senior individuals, e.g. COO and CITO. The PRA does not expect the SMF24 to be split between more than three individuals.

The essential principle when sharing or splitting the SMF24 is that individuals must not have a hierarchical relationship. Where this is the case, the more senior individual should be approved as SMF24. Where there is a split, the roles of each individual must be clearly disambiguated within their Statement of Responsibilities (SoR). In identifying accountability for the SMF24, organisations should also consider overlap with the FCA's Prescribed Responsibility in Allocation of Responsibilities.

For instance, it may be logical that the individual accountable for Recovery and Resolution Planning also has accountability for Operational Resilience and continuity under the SMF24, given the interrelationships between the subjects that they deal with.

Whoever assumes ultimate accountability for the SMF24 will need to champion Operational Resilience within the organisation, taking proactive responsibility for harmonising management functions from the top down. In practical terms, this will mean leading Operational Resilience Management Committee meetings and setting clear direction, understanding challenges and intervening where there are inhibitors to any necessary improvements to Operational Resilience.

This is a critical success factor since divisional mentalities will quickly impede implementation. Nonetheless, organisations will find that there are legitimate but challenging alignment questions to answer: *"if we identify a technology risk that undermines the resilience of our IBSs, who reports on it first: the Technology Risk or Operational Resilience team?"* Overcoming these sorts of challenges will require strong governance and consensus among supporting disciplines at the outset of implementation.

The principle that Operational Resilience should fall within existing governance structures should be extended to include risk management policies and procedures. This means that organisations will need to consider how to situate Operational Resilience within the Operational Risk taxonomy.

Disciplines such as Business Continuity sometimes appear as a risk categories within the Operational Risk taxonomy in their own right. However, organisations may adopt the view that since Operational Resilience is an outcome of effective Operational Risk Management, the risks that it covers are inherent within other areas of the taxonomy such as Third Party Risk Management, Operational Risk, Cyber Risk and Technology Risk. Notwithstanding, where the inherent view is adopted, organisations will need to give thought to the relationship between the Operational Resilience policy and the top risk(s) that it is intended to address. For this reason, Operational Resilience teams should regard their policy as an opportunity to set out a clear RACI for internal collaboration and management of Operational Resilience.

Organisations will need to consider how to align Operational Resilience with Operational Risk. Supervisors are clear that Operational Risk is adequately covered in multiple additional regulatory requirements. Operational Risk, while supporting the outcome of Operational Resilience, is not considered sufficient on its own, as it is managed in relation to an organisation's risk appetite, while Operational Resilience assumes these appetites have been exceeded and disruption will inevitably occur.

Operational Resilience challenges organisations to think about how to manage disruption in a holistic manner. In this regard, organisations should reflect how broader resilience areas, such as Business Continuity, Third Party Risk Management, Cyber Resilience, Technology Risk, etc., interact and how to apply a complementary and collaborative approach to manage disruption. The relationship between these areas, and Operational Risk, should be carefully considered and appropriate RACI frameworks and taxonomies should be used to clearly articulate relationships and management activities.

Organisations should clearly articulate within policies how the responsibilities across the resilience areas delineate and how they collectively contribute to the outcome of operational resilience. In addition, thought should be given to how Operational Resilience incident reporting is governed across these areas and whether they constitute a Notifiable Event. Further guidance in this area is expected from the regulators in Q4 2021.

An additional but significant factor to consider is the relationship between Operational Resilience and existing policies. Organisations will have an opportunity to consider overlapping policies and duplication of effort and rationalise and simplify these once the Operational Resilience approach is established. For this reason, second and third line teams should have a good understanding of the practical implications of the Operational Regulatory policy, a sound appreciation of the methodologies used and regular involvement in the trajectory of the programme.

Risk culture and a mindset shift

Risk culture is a critical success factor in the implementation of the policy framework and ultimately the improvement in Operational Resilience. The regulators place great emphasis on the tone from the top, with Boards and senior management playing a key role in moving away from a protective and process driven approach to one in which outcomes are considered in a holistic cross-cutting service view and disruption is considered as inevitable.

Second line teams should aim to strengthen Operational Resilience through supportive practices and healthy challenge that goes beyond simply assessing controls and monitoring KRIs, and looks deeper at cultural aspects. This will mean actively participating in Operational Resilience committees and working groups; understanding barriers to implementation and cultural change; and working alongside first line teams to inculcate an operational resilience mindset.

Better outcomes will come from early and proactive identification of vulnerabilities to Operational Resilience so second line teams should regard their role as instrumental in terms of instituting the right culture and behaviours with respect to risk monitoring, escalation and reporting. At the same time, Operational Resilience teams should regard it as their role to communicate effectively and broadly about the benefits of Operational Resilience to increase adoption of policy requirements and guidance.

Second line teams should aim to strengthen Operational Resilience through supportive practices and healthy challenge that goes beyond simply assessing controls and monitoring KRIs. This will mean actively participating in Operational Resilience committees and working groups; understanding barriers to implementation and working alongside first line teams both to set realistic timeframes for remediation activities against identified risks and, in some cases, actively helping to meet them.

Better outcomes will come from early and proactive identification of risks to Operational Resilience so second line teams should regard their role as instrumental in terms of instituting the right culture and behaviours with respect to risk monitoring, escalation and reporting. At the same time, Operational Resilience teams should regard it as their role to communicate effectively and broadly about the benefits of Operational Resilience to increase adoption of policy requirements and guidance. Organisations will also need to give consideration to the design and assurance of controls for the Operational Resilience 'management system' (the policy framework) for Operational Resilience. There should be a number of controls to ensure that the policy framework remains in effective operation through the years ahead.

Securing buy-in

Operational Resilience teams should be cross-functional comprising SMEs from across each of the resource areas as well as relevant areas such as Business Continuity, Cyber Security, Incident and Crisis Management, Business Change and Operational Risk.

Breaking out of resilience silos in pursuit of a common goal may be challenging, and can be best achieved through a strong top-down commitment to the Operational Resilience agenda. However, Operational Resilience teams will also need to consider how they communicate the benefits of the programme to stakeholders within the business, i.e. those who are ultimately responsible for decision-making about Important Business Services. Treating Operational Resilience as a regulatory compliance exercise will not generate the enthusiasm and commitment needed to effect the change in mentality and approach that Operational Resilience requires. Considering and articulating the commercial benefits of faster, more reliable, less risk-prone services for customers will likely be a more compelling argument for investments of time, effort and resources in Operational Resilience.

Service ownership

It is important for Operational Resilience teams to view their role as Operational Resilience champions. They do not own Important Business Services, the risks associated with them or decisions about investments in their resilience, which sit with the business and SMF24. As such, it may be useful to establish Business Service Owners who are responsible for the service – its performance and its resilience.

Reporting and Management Information (MI)

Monitoring and reporting on Important Business Services may present some challenge, depending on how systems are architected and the maturity of data collection. Operational Resilience teams need to develop the capability within their monitoring model to look around corners and anticipate what may happen, understanding where there may be trends towards impact tolerance breaches. This will mean monitoring a broad spectrum of existing data sets but looking at these through the business service lens.

From a data analytics perspective, proactive monitoring of IBSs may require organisations to establish the service as a data element by 'anchoring' it in, or tagging it to, existing business processes. This will require an integrated data model that can bring together the different domains that contribute to Operational Resilience. As we have discussed above, processes will act as the common denominator for capturing data elements relevant to the business service.

For most organisations, some level of data re-purposing or re-architecting will be required to service the needs of Operational Resilience since data are likely to be configured for vertical or functional management purposes and will not include a service lens. One key step that organisations can take is to bring a horizontal service view into the Risk & Control Self-Assessment process (RCSA) to view Notifiable Event, Near Miss, risk and control data against the service.

Organisations will also need to consider how they can align operational metrics and KPIs to the service. For instance, most organisations will be able to view P1 incidents by business application, but will not be able to view the volume of P1 incidents across an end-to-end business service. Similarly, they may be able to view attrition rates by business function, but not across a service. To do this, data may need to be re-purposed, analysed against business processes and then rolled up to the service.

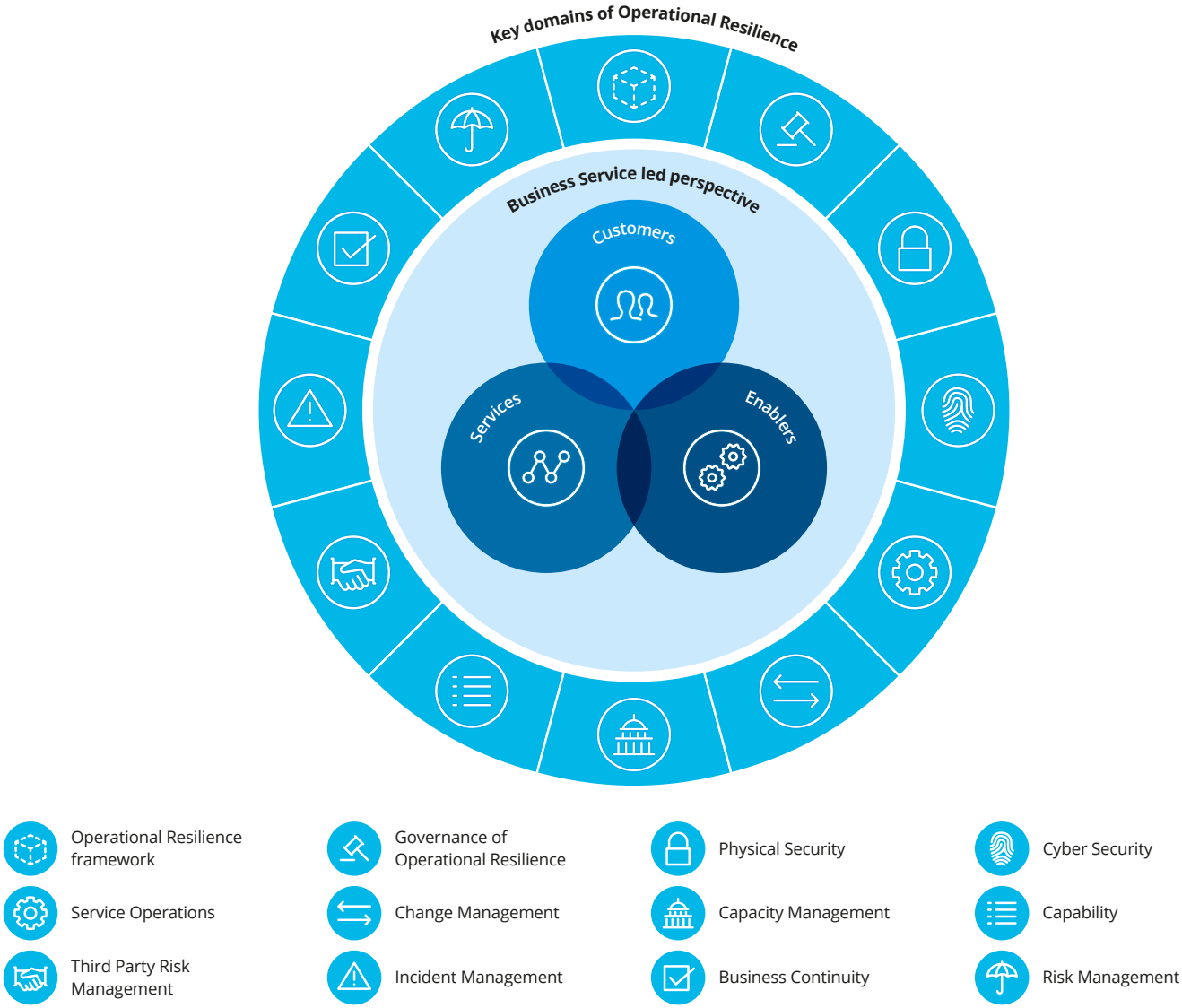
Teams can choose to invest in data analyst capabilities to process this data in accordance with reporting schedules but it may be worth identifying more strategic automation solutions to overcome this challenge and to move the organisation towards automated self-service dashboards with live data on the performance and risks associated with IBSs that Business Service Owners and interested stakeholders can access as required.

Operational Resilience teams should aim towards reports that enhance senior management decision-making about Operational Resilience. This will likely require monitoring on four levels:

- The status of programme activities and implementation (e.g. percentage of IBSs that have been mapped and stress-tested)
- The status of capabilities required to support Operational Resilience, focussed largely on Key Control indicators (e.g. proportion of IBSs with approved and tested Business Continuity Plans; proportion that have been subjected to stress-testing)
- Key performance and risk indicators for each of the resource areas that support Operational Resilience (e.g. volume of P1 Technology incidents across the IBS in the prior reporting period)
- Key performance and risk indicators for the end-to-end business service (e.g. Impact Tolerance breaches, Near Misses, or new external and sectoral risks)

Operational Resilience teams should aim to balance the metrics that they select to generate both prior period reporting and forward-looking indicators of potential trends towards impact tolerance breaches. They will need to work closely with resource teams and with Operational Risk to set appropriate triggers and limits for the metrics that they set. They will also need to define use cases for reporting – for instance, in addition to the self-assessment, reporting for Business Service Owners with selected KRIs and KPIs may be useful.

Figure 4. Key domains of Operational Resilience



Next generation Operational Resilience – tools and techniques

All key components of an Operational Resilience framework will benefit from digitalisation and cutting-edge management techniques. In the following section, we will illustrate this by providing five examples of how tools and techniques can support the effective implementation and embedding of Operational Resilience.

Operational Resilience Management System (ORMS)

An Operational Resilience Management System can support the integration of existing systems and data sources used as part of related frameworks – such as Business Continuity Planning (BCP) tools, Governance, Risk & Compliance (GRC) platforms, or incident management systems:

- An ORMS consumes information from existing systems and data sources utilising APIs
- It provides users with tool support to collect and track information from SMEs and can be connected to digital modelling solutions
- The dashboards and reports that ORMSs provide facilitate the key Operational Resilience tasks and can be used to address regulatory requirements

Digital twins

As organisations mature in their Operational Resilience journey, they can start to consider modelling with testing sophistication moving from paper to model-based. To do this, organisations may wish to apply techniques for modelling from Digital Twins, starting with low-fidelity models. Over time, the organisation may want to build higher-fidelity models, such as those typically used in engineering.

A 'digital twin' is a virtual replica of a process, service or asset that can be used together with live or simulated data to examine the efficiency of a process. Digital twins can support scenario stress-testing by allowing for the end-to-end testing of a service outside the live production environment, in other words reducing the risk posed by full interruption testing and allowing for the full service to be tested in a way that it is unlikely to be in production.

- While not yet very common in the Financial Services industry, digital twin technology is already applied successfully in other fields, such as for aircraft engine maintenance and to optimise Formula 1 race cars. As the technology is maturing, it will soon be more broadly available to organisations outside these domains
- 'Digital twins' have many use cases in Financial Services, and in particular for operational resilience testing
- Digital twins can be used to show what will happen (i.e. the impact) if a resource fails or degrades; what will happen if a recovery or contingency solution is applied; and allow organisations to vary the effectiveness of the recovery/ contingency
- They also enable the identification and modelling of emergent attributes such as virtuous and vicious cycles, tipping points, single points of failure, and resource/flow bottlenecks

Automated run books

The key steps in operational resilience testing, and in recovery and response from real incidents can be accelerated and automated by the use of dedicated tools consolidating functionality in one location, thereby providing 'automated runbooks'. Automated runbooks have three main components as explained below:

- Recovery process digitalisation
  - Hosting of recovery plans to ensure that plans are ready to be executed when needed (as a test or as a response)
  - Reference data sourced from multiple systems
  - Fast creation of new plans with flexible templates
  - Continuous improvement through the sourcing of previous event data to drive continuous improvement
- Orchestration of live system tests & recovery
  - Support for dynamic and interactive live system tests and recovery, including intra-team communication and event logging
  - Orchestrates and executes the steps for recovery or fail-over of systems
  - Provides real-time view of completion of the recovery process for future analysis
- Visualisation and reporting tools
  - Visibility into real-time and upcoming events and drill-down views into the details
  - Aggregates data from disparate sources
  - Provides a comprehensive source of records for regulatory reporting, compliance and analytics

Dynamic reporting dashboards

Dynamic dashboards can be generated using business intelligence software such as Power BI or Tableau and enable BSOs, Operational Resilience teams, and other interested stakeholders to proactively monitor the status of IBSs outside reporting cycles and committees. Reliant upon automated data feeds, dynamic dashboards perform a similar function to IT Ops dashboards with live data illustrating the status of risks and performance and providing early warning indicators of perfect storm scenarios or trends towards impact tolerance breaches.

The key steps in operational resilience testing as well as in recovery and response from real incidents can be accelerated and automated by the use of dedicated tools consolidating functionality in one location, thereby providing 'automated runbooks'.

Dashboards can offer layered reporting using aggregate data sets designed to help inform decision-making around resilience. MI and reporting should give confidence in how ready the organisation is to respond to disruption and where future investment in resilience is needed. It should provide information rather than mere data. Grouping metrics into categories can help to support senior management and the Board in these decisions:

Performance reports – Are our IBSs working as expected? These are likely to be real time indicators, e.g. are payment volumes and customer behaviour following expected patterns?

Vulnerability reports – What specific weaknesses do we have in the way we deliver our IBSs? Based on past performance, these metrics could include actions taken based on outcomes from stress-testing exercises, timeliness of responding to incidents and recurring issues such as number of cyber-attacks over a set period.

Disruption reports – Do we understand our key 'resources' and can we see where these may become impaired? These are aimed at predicting short – to medium-term pinch-points based upon recent performance, such as percentage of staff attrition, areas of rolled back changes and critical supplier performance.

Readiness reports – How prepared are we for a major disruption? These indicators should help us to gauge how well we could cope and what strategies are in place to protect our business. Example metrics could include the number of Business Continuity Plans tested during the last year, the percentage of stressed exit plans in place for critical suppliers, and confirmation that the penetration testing schedule is up to date.

All metrics will require triggers and limits (with RAG rating or similar) and MI to explain their significance, which will need to be developed in conjunction with Operational Risk and the resource and capability leads. Much of this data may be collected at a process, functional or team level but will need to be manipulated to aggregate it against the business service. As discussed elsewhere in this paper, this will most likely be achieved by using business processes as a common denominator and rolling up the data to the business service.

Agile

Embedding agile methodologies not just in IT change but across other areas of the organisation can deliver significant benefits for Operational Resilience. In software development, agile was originally designed to bring together cross-functional teams and their customers/end users to discover requirements and find solutions through collaboration. For this reason, it is particularly well-suited to the 'outside in' perspective that Operational Resilience targets since it focusses primarily on outcomes, not inputs to delivery.

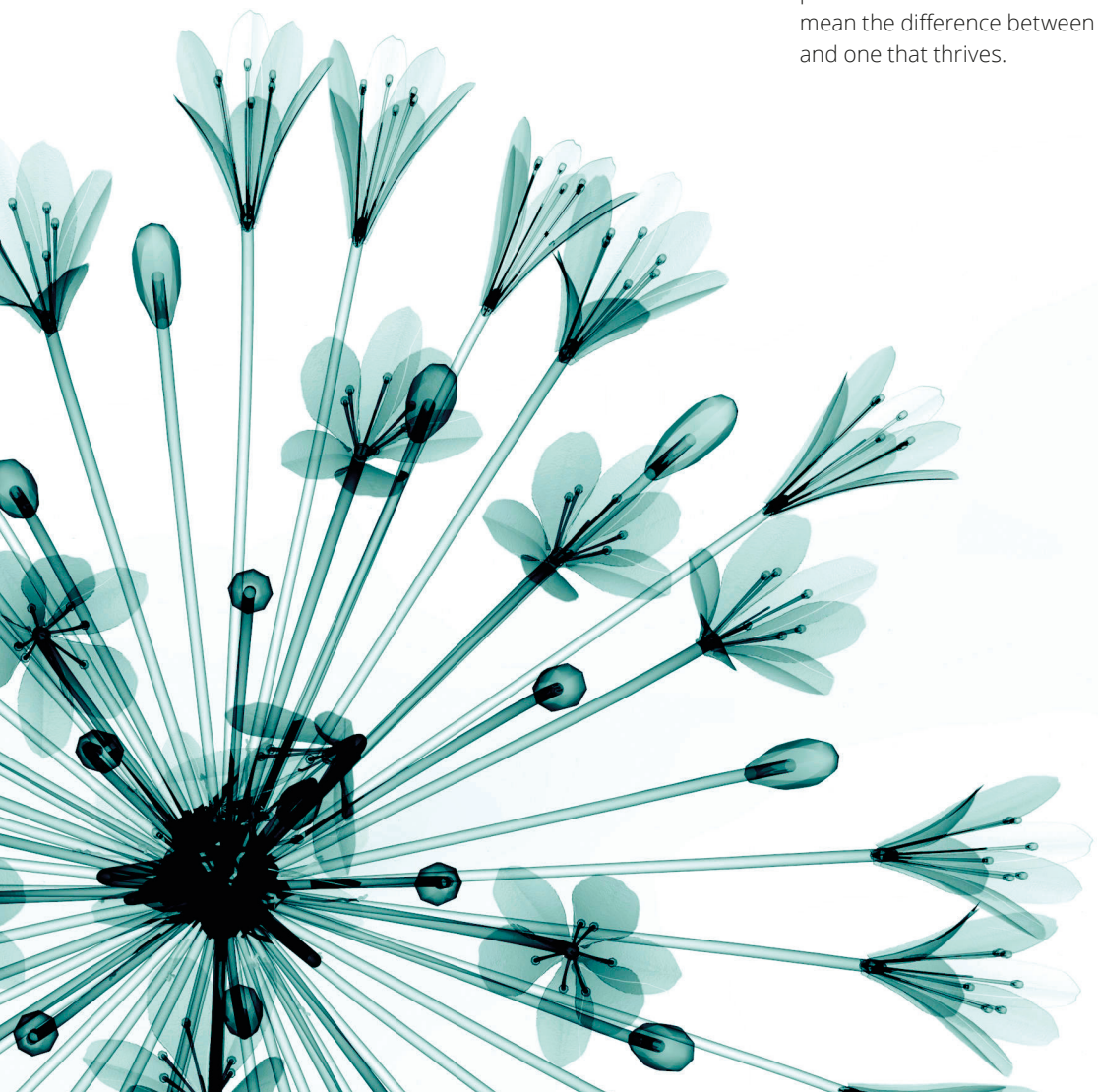
Agile advocates adaptive planning and delivery in smaller increments with continuous improvements rather than cliff-edge releases. It can be used as a methodology for better understanding the outcomes that the IBS is trying to achieve: bringing together multi-functional teams and resource areas and for iteratively improving IBS performance.

Conclusion

Organisations have to comply with mandatory regulatory requirements around Operational Resilience to ensure that they are resilient at firm level. However, in a highly interconnected Financial Services ecosystem, a more holistic approach to resilience is important and requires collective action.

For this reason, organisations should commit to, and prioritise involvement in, cross-industry forums such as the Cross-Market Operational Resilience Group (CMORG), Cyber Collaboration Centre (FSCCC), Financial Services Information Sharing and Analysis Center (FS-ISAC) proactively participating in the development of industry standards, and solutions that can help to mitigate organisation-specific as well as sectoral risks to Operational Resilience. Organisations may also benefit from participation in the various bodies and associations that represent the sector, for instance, the Financial Sector ISORG, the LMA, the Building Society Association etc.

Although organisations will need to become resilient in their own right and to the best of their ability, it is worth investing in collective action[6] and strategies, such as pooled audit and assurance activities, peer-to-peer intelligence and information exchange, and proactive identification of sectoral concentration risks. This could mean the difference between a Financial Sector that just survives and one that thrives.



Appendix 1

Operational Resilience regulation across international jurisdictions

Application of operational resilience, outsourcing and third-party risk management initiatives to branches and subsidiaries

	Banks		Insurers		Investment Firms		Financial Market Infrastructure (FMI)		Payment/E-money institutions	
	UK branches of third-country firms	UK Subsidiaries of third-country firms	UK branches of third-country firms	UK Subsidiaries of third-country firms	UK branches of third-country firms	UK Subsidiaries of third-country firms	UK subsidiaries of third-country FMIs	Third-country FMIs servicing UK market	UK branches of third-country firms	UK Subsidiaries of third-country firms
PRA Supervisory Statement on Operational Resilience	No	Yes	No	Yes	No	Yes (If a dual-regulated investment firm)	No	No	No	
BoE Supervisory Statements on FMI Operational Resilience	No						Yes	No	No	
FCA Supervisory Statement on Operational Resilience	No	Yes	No	Yes	No	Yes	Yes	No	No	Yes
PRA outsourcing and third-party risk management policy	Yes, but expectations are applied proportionately	Yes	Yes, but expectations are applied proportionately	Yes	Yes, but expectations are applied proportionately	Yes	No			
FCA Guidance for firms outsourcing to the Cloud and other third-party ICT services	Unclear. FCA guidance doesn't mention UK branches of third-country firms. But, the guidance doesn't apply to credit institutions subject to the EU Capital Requirement Regulations (EU 575/2013)	Yes. But, the guidance doesn't apply to credit institutions subject to the EU Capital Requirement Regulations (EU 575/2013)	Unclear. FCA guidance doesn't mention UK branches of third-country firms	Yes	Unclear. FCA guidance doesn't mention UK branches of third-country firms. But, the guidance doesn't apply to investment firms subject to the EU Capital Requirement Regulations (EU 575/2013)	Yes. But, the guidance doesn't apply to investment firms subject to the EU Capital Requirement Regulations (EU 575/2013)	It applies to central counterparties, central securities depositories and Regulated Markets	No	Unclear. FCA guidance doesn't mention UK branches of third-country firms. But, the guidance doesn't apply to payments and e-money institutions are subject to the EBA's outsourcing Guidelines*	Yes. But, the guidance doesn't apply to payments and e-money institutions are subject to the EBA's outsourcing Guidelines*

* In light of Brexit, the FCA expects firms to continue to apply the EBA Guidelines to the extent that they remain relevant as they did before the end of the transition period

Contacts

If you have any questions about the issues covered in this report, please contact with one of the team.

Rick Cudworth
Partner
Reputation, Crisis & Resilience
+44 20 7303 4760
rcudworth@deloitte.co.uk

Sarah Black
Partner
Risk Advisory
+44 20 7007 9543
sarahblack@deloitte.co.uk

Suchitra Nair
Partner
European Centre for Regulatory Strategy
+44 20 7303 7963
snair@deloitte.co.uk

Neil Bourke
Director
Reputation, Crisis & Resilience
+44 20 7303 4682
nebourke@deloitte.co.uk

Gavin Simmonite
Associate Director
Reputation, Crisis & Resilience
+44 20 7007 3102
gasimmonite@deloitte.co.uk

Lucy Gemmill
Senior Manager
Reputation, Crisis & Resilience
+44 20 7303 4656
lgemmill@deloitte.co.uk

Scott Martin
Senior Manager
European Centre for Regulatory Strategy
+44 20 7303 8132
scomartin@deloitte.co.uk

Endnotes

1. PRA SS2/21.
2. Cf. SYSC 15A.6 Self-assessment and lessons learned exercise documentation
3. Prudential Regulation Authority Consultation Paper CP29/19, Operational Resilience: Impact Tolerances for Important Business Services, December 2019, section 3.11.
4. The PRA has been clear that the three year period is an upper limit and not a target. For systemically important firms, the expectation will be to address vulnerabilities more quickly – complexity of operations will not be a reasonable justification for delay.
5. Prudential Regulation Authority Supervisory Statement SS28/15, Strengthening individual accountability in banking, December 2020.
6. https://www.bankofengland.co.uk/speech/2021/may/lyndon-nelson-uk-finance-webinar-building-operational-resilience

Deloitte.

Designed and produced by 368 at Deloitte. J21524