

Deloitte.



Time to flourish

A practical guide to enhancing operational resilience in the UK financial services sector

Contents

Executive summary	01
A new mindset	02
Five opportunities to enhance operational resilience	06
1. Business services	08
2. Impact categories	10
3. Impact tolerances	12
4. Communications	17
5. Scenario testing	18
Summary	20
Next steps	21
Contacts	22
Notes	24

Executive summary

The UK financial services sector has experienced market shocks as diverse as the global financial crisis, geopolitical events, technology failures and a hostile cyber environment. In response, regulatory attention is focusing on how firms and financial market infrastructures (FMI) improve their operational resilience to high-impact events.

In July 2018, the Bank of England (BoE) and Financial Conduct Authority (FCA) published a discussion paper (DP) recognising the complexity of the financial services sector. It proposes how firms and FMI can improve operational resilience to severe but plausible events.

In the past, the regulatory authorities set up a range of initiatives including Recovery and Resolution Planning (RRP), Operational Continuity in Resolution (OCIR), the Dear Chairman Exercises (DCE) focusing on firms' technology resilience (DCE I and DCE II), and more recently, the Financial Policy Committee's (FPC) cyber stress testing pilot initiative. Each of these demonstrated the authorities' interest in building a financial services sector that can absorb the impacts of unexpected events without further contributing to them.

With the release of the DP ('DP 1/18') the BoE and FCA extended the thinking to go beyond specific measures for specific events, to more broadly how firms and FMI plan for and respond to high-impact events which could adversely affect customers, their own viability and the sector's stability.

This marks the beginning of a clear direction of intent for operational resilience by the regulatory authorities, and uses principles and approaches from industry standards and existing regulatory initiatives. It also reconsiders risk management systems designed to mitigate disruption to customer service, such as business continuity and IT disaster recovery, in light of recent disruptions and a heightened risk landscape.

We believe it provides an opportunity for firms and FMI to enhance their operational resilience by:

- making senior leadership accountable and creating a mindset that considers more severe disruptions as inevitable
- aligning operational resilience with the operational risk framework. These are two sides of the same coin; risks need to be managed effectively, but if they materialise they must be mitigated
- using severe but plausible scenarios, alongside impact tolerance statements, to assess and test resilience measures, identify gaps and invest appropriately.

In this paper, we give our views on the changes the DP presents and five implementation opportunities that could improve the sector's operational resilience. Where practical and appropriate, we have used worked examples to illustrate these points. These are based on our experience of supporting a broad range of financial institutions that are working to address these areas.

"I would like our firms to be on a WAR footing: withstand, absorb, recover."

Lyndon Nelson
Deputy CEO & Executive Director
Bank of England

A new mindset

The DP makes important observations about the overall operating landscape, governance and mindset changes required when building operational resilience. These are summarised below.



Assume disruptions will happen and they could be severe

Recent high-profile disruptions across a broad range of industries have shown that preventative measures, while important, cannot guarantee against disruption.

The DP emphasises that disruptions are inevitable and that organisations must be able to reduce their impact. It also sets out that disruptions could be severe, going beyond what is typically considered in standard business continuity approaches.

This is helpful to emphasise that preparation for an operational disruption is as important as attempting to prevent one. Firms and FMI need to adopt a twin-track approach to planning activities that considers severe but plausible events in addition to routine disruptions where the nature and required response are well known and pre-determined.



Operational resilience requires a broader perspective of risk

The DP recognises the increased complexity of the environment in which financial institutions operate and the associated challenges of protecting customers and other market participants. These challenges include: technical innovation, changing consumer behaviours and expectations, keeping pace, challenging environment and system complexity. This helps widen the discussion of what operational resilience covers and the breadth of functional involvement required to understand and meet these.

Operational resilience needs to consider a broader range of strategic, regulatory and operational risks. Firms and FMI will require a joined-up approach to do this, as well as a deeper understanding of human behaviours.

Internal alignment

Firms and FMI need to align, what are often separate risk, management systems, such as business continuity, cyber and information security, operational risk and vendor risk. By doing this they will better understand how they directly and collectively contribute to the overall resilience of business services.

This will require effective governance and leadership to break down existing siloes and move operational resilience into the overall operational risk management approach. Improved alignment of risk management systems promotes better sharing of good practices and helps establish common understanding of what is important to the firm or FMI, the impacts of a disruption and the priorities during response and recovery.

“Operational resilience needs to consider a broader range of strategic, regulatory and operational risks as well as a deeper understanding of human behaviours.”

Firms and FMI need to consider if there is parity in their treatment of strategically important risks. For example, the DP recognises cyber as a key risk that threatens operational resilience, but also acknowledges that other types of risk can cause significant consumer detriment and present a serious threat to the viability of firms and stability of the sector as a whole. So while resilience to cyber events is vitally important and merits specific attention, a similar step-change is needed across operational resilience as a whole.

Sector alignment

Building operational resilience cannot be achieved overnight or by one firm alone.

The UK finance sector has high levels of systemic risk caused or exacerbated by having several critical activities concentrated among a few key suppliers such as: custodian banks; clearing houses; cloud service providers; payment systems; and business process outsourcing suppliers.

Any individual firm or FMI cannot address this as it is market phenomena. A cross-market approach to resilience that exposes vulnerabilities presented by shared dependencies is therefore very important.

Cross-industry fora are helpful here. The Cross Market Operational Resilience Group (CMORG) provides opportunities to unify the industry on operational resilience matters, promote information sharing as events unfold, disseminate learnings after they are resolved, and sponsor a sector-wide exercising programme.

Sector-wide exercises are important to bring the industry together, improve familiarity with communication channels, coordinate planning and decision-making processes, and identify vulnerabilities from dependencies on shared suppliers or critical market infrastructure.



The Board must play a leading role

Boards have the explicit remit to ensure the effective governance of an organisation, including full oversight on matters affecting reputation and viability. Key to helping Boards fulfil their duties is a sound approach to operational resilience, backed up by proven outcomes and capabilities.

Recent events have raised whether Boards are adequately equipped to assess operational resilience. This may be due to poor quality reporting to Boards in this area, compounded by an inability to ask the right questions. Organisational culture is another factor – particularly where there is a perception that senior leaders and Boards do not want to hear bad news.

Firms and FMI need Boards that ask the right questions to ensure operational resilience has the appropriate priority. Boards do not need to be experts in operational resilience but should be able to challenge their executives so they are confident the right operating model and culture is in place to support resilience. For some firms and FMI, this will require greater focus on improved reporting and assurance mechanisms. For most, it will require Boards to be more involved in understanding and approving impact tolerance statements, reviewing the outcomes of scenario-based testing and approving high-impact changes.

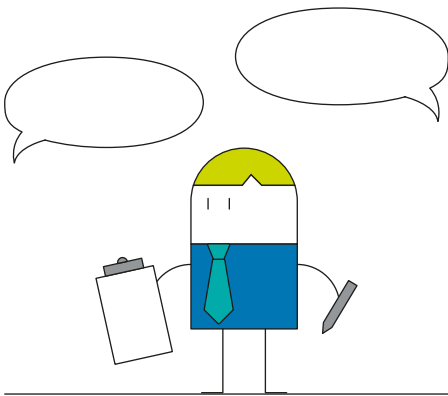
“This will require effective governance and leadership to break down existing siloes and move operational resilience into the overall operational risk management approach.”





Five opportunities to enhance operational resilience

The DP introduces key concepts that could improve the operational resilience of firms and FMI, and the sector more broadly, if adopted. These are summarised below and explained in more detail throughout the paper, with worked examples where relevant.

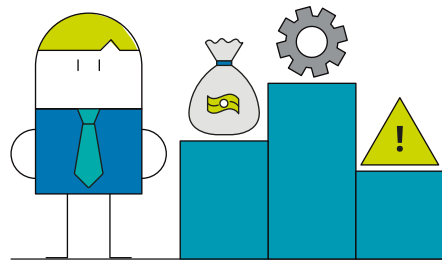


1. Business services

Firms and FMI should adopt a business services view. This will focus time, effort and resources on what is important to the customer, consumers more generally and the sector as a whole.

They should consider how the business services they deliver are perceived by those who receive them and develop a deeper understanding of what they think, are likely to feel and do if the service is disrupted. This will identify vulnerable customers, the potential to cause harm and inform the best course of action in a crisis.

Firms and FMI also need to understand key interactions and identify operational dependencies, such as systems, staff, data, suppliers and locations, which directly support the customer experience and where disruption could have the greatest impact.

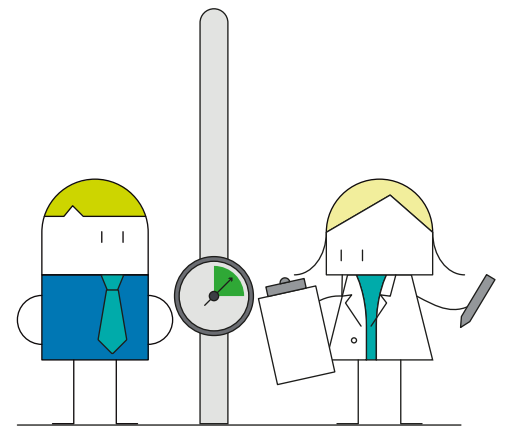


2. Impact categories

Business services should be prioritised by their relative importance against three main categories:

- Financial stability
- Organisational viability to the firm or FMI
- Customers and other market participants.

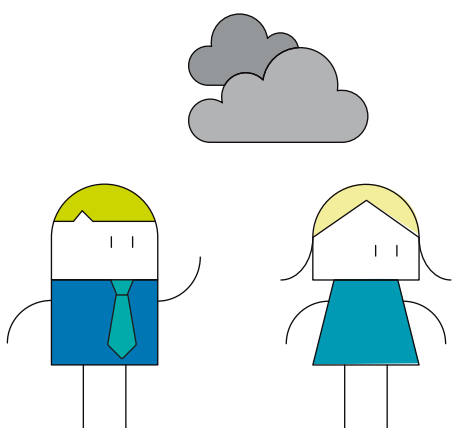
Firms and FMI need to consider the adverse outcomes or harm that the loss of a service may cause. Importantly, two of the three categories highlighted would require firms and FMI to take an outside-in perspective of impact.



3. Impact tolerances

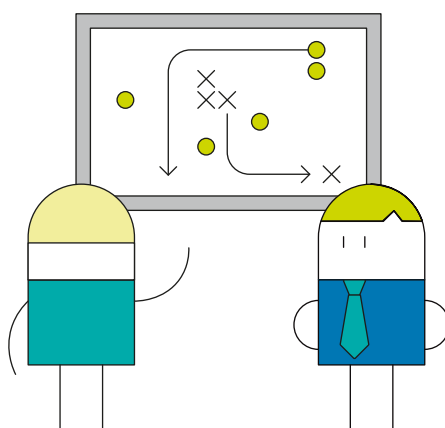
Firms and FMI should express their tolerated threshold for severe but plausible disruptions to important business services and set an objective to ensure that threshold is not breached. These are not just time-based but clear business statements of outcome-based objectives.

The regulatory authorities will likely specify impact tolerance expectations for certain systemic business services, such as payments. This has already been seen in the FPC's approach to the 2019 pilot cyber resilience stress tests, where an impact tolerance was set by the FPC for the recovery of payment services for the UK's most important financial institutions.



4. Communications

Firms and FMI should thoroughly think about how to manage prompt and meaningful communications during a disruption, including ensuring the necessary capacity to do so, to maintain confidence in the organisation and reduce harm caused.



5. Scenario testing

Once tolerances for disruption are established, they should be tested against dynamic scenarios to prove they can be met.

The scenarios should be severe but plausible. They should push the organisation to the brink of its tolerance threshold and not assume a straightforward recovery. It is possible that the UK regulatory authorities will specify certain scenario conditions against which they expect larger firms and FMI to test.

“Firms and FMI need to consider the adverse outcomes or harm that the loss of a service may cause.”

1. Business services

The DP advocates that firms and FMI focus their operational resilience approach on important business services and economic functions, including what is needed to deliver them. Time, effort and resources should be channelled into protecting what is important to the outside world, not just themselves.

A business services approach to resilience requires organisations to consider:

What is a business service?

The meaning of a 'business service' will vary by firm or FMI, but it should be considered as a product or service provided to, and recognised by, customers or market participants.

A business service is the outcome expected by a customer, market participant or end user. It is 'what' is delivered.

This is different to a business process which is how the outcome is delivered, and therefore tends to be more granular and internally focused. Several business processes may be required to deliver the overall outcome.

An outcome-focussed perspective allows firms and FMI to identify alternate means of delivering that end user expectation when supporting processes and assets fail.

The economic functions identified through RRP related initiatives over the past decade, although not synonymous with business services, can help identify these.

Who is accountable for the business service?

Firms and FMI should consider how to assign accountability for a business service that may cross several business units, departments and functions. This may require specific accountabilities that focus on the coordination and alignment of operational resilience activities across geographies, functions and potentially business lines.

Which business services are most important?

Not all business services and economic functions are equal in importance. Some may be more integral to 'real economy' activity, and others enable inter-firm business and underpin market stability.

Investment and management attention should focus on those services where disruption could significantly harm customers or end users, threaten the firm's viability or broader sector stability. The section on impact categories explores this further.

How are these business services delivered?

It is important for firms and FMIs to understand how a business service is delivered and how those who receive it may behave if it is disrupted.

Firms and FMI can identify risks relevant to the service by mapping important business services to their operational dependencies. For example: locations, systems, suppliers and people; and business cycles such as critical deadlines. This can enhance the development of contingency or business continuity plans and inform scenario testing. Firms and FMI should focus on achieving a level of detail that identifies sources of risk, rather than exhaustively mapping the entire service.

Questions to answer



Definition

What is a business service?



Accountability

Who is accountable for the business service?



Importance

How important is the business service, based on an impact assessment against harm done, organisational viability and financial stability?



Dependencies

What is needed to deliver the business service?



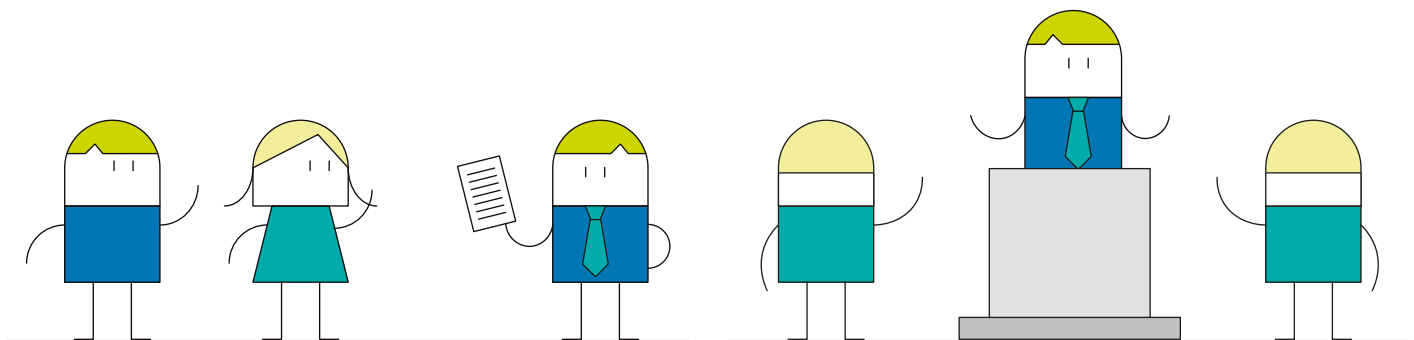
Behaviours

What will the user of the service think, feel and do if it is disrupted?

Definition: Economic function

Economic functions are a broad set of services the financial services sector provides to the UK economy, and hence an aggregation of business services that one or more firms or FMIs provide. If sufficiently significant in terms of both size and function, these economic functions can become critical to the UK economy.

Defining business services: some key considerations

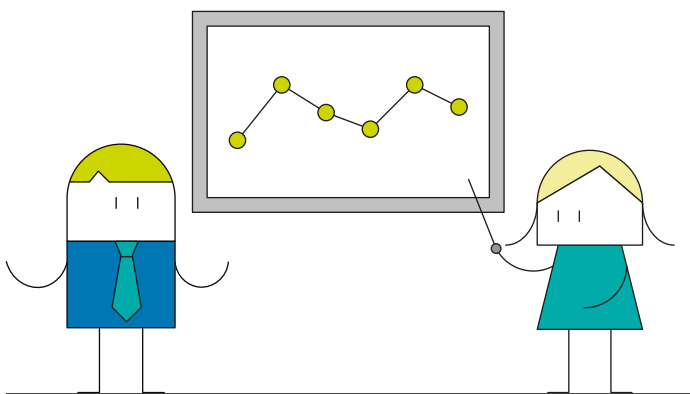


Service ownership

- Is ownership and accountability for the service well defined? How does this fit into the firm or FMI’s governance process? Does this include accountability for the resilience of the business service?
- Are services integrated across borders and do other jurisdictions have different regulatory requirements for operational resilience?
- Do complex legal entity structures mean that service governance could be duplicated or unaligned?

Determine importance

- Can the work done on economic functions for operational continuity in resolution help inform how important business services are defined?
- Are the impact categories aligned to those suggested by the regulatory authorities? See impact categories section.
- Do we have a sufficiently developed view on harm done and to who?
- Is the importance of the business service determined using an equitable framework to ensure consistency?



Map dependencies

- Which aspects of the value chain are most critical to the delivery of the business service?
- Are there any essential service components or crucial deadlines that alter how the service is prioritised?

“Adopting a business services approach helps to inform investment decision-making around operational resilience.”

2. Impact categories

Firms and FMI must consider the adverse outcomes or harm that the loss of the business service may cause to understand how important it is.

The DP sets out three impact categories to evaluate the disruption of a business service:

- **Financial stability:** The stability of the market and broader economy would be threatened
- **Organisational viability:** The very existence of the organisation could be at risk
- **Customer and other market participants harm:** There would be considerable detriment to end users of the service.

These categories provide a common means to assess the relative importance of a business service and enable a scalable assessment depending on the size and complexity of the organisation. Smaller institutions are likely to focus on customer harm and organisational viability, while larger and more systemic ones will also consider financial stability.

An outside-in perspective

Two of the three impact categories – financial stability and customer harm – will require firms and FMI to focus on external impacts. This represents an important mindset change and highlights increased regulatory interest in the harm that any one institution may cause to the real economy and financial services sector as a whole.

Considering impacts to the outside world will encourage firms and FMI to put the entire range of relevant stakeholders' interests first and should ultimately lead to better response capabilities.

Understand customer harm

Approaches traditionally used by some organisations to consider the external impact of a disruption are likely to have focused on the number of customers affected rather than the detriment experienced. The DP suggests the need to go further and evaluate the actual impact of disruption on the real economy.

To understand all dimensions of harm caused, firms and FMI must develop a more nuanced set of indicators, metrics and impact criteria beyond the scale of the disruption. This may include the ability to identify and prioritise vulnerable customers, or to understand how the disruption could affect consumers' ability to go about their daily lives.

For example, if additional support or the restoration of basic banking and payment services to vulnerable customers should be prioritised, how are such customers identified and how might this acceptably alter the relative prioritisation of other critical services? Greater understanding of perceptions of the service and likely behaviours in a disruption are important to ensure a more rigorous approach to mitigating customer harm.

Tailor the response




In a disruption firms and FMI can better prioritise by considering different stakeholders and perspectives. This includes looking beyond corporate clients and trading partners to the customers beneath. For instance, a firm that trades on behalf of a credit union should consider the downstream impacts of a disruption on vulnerable customers.

For events with clear systemic impacts, this could mean averting threats to financial stability before addressing consumer concerns.

For events where the primary impact is on the real economy, affected consumers might need to be prioritised ahead of market participants. Figure 1 shows what this prioritisation could look like in a payments disruption scenario.

Figure 1. Indicative impact categories and considerations for payments services

Prioritising payments by type according to harm caused

 Payment type	 Example	 Considerations
Harm to financial stability	<ul style="list-style-type: none"> • Bank-to-bank • Scheme 	<ul style="list-style-type: none"> • Could bank-to-bank or scheme reconciliations and settlements be delayed until after customer transactions have completed?
Legal certainty or urgent payments	<ul style="list-style-type: none"> • M&A • House purchase • Mortgage clearance • CHAPS 	<ul style="list-style-type: none"> • What is the volume of payments impacted? • Can stand-in or manual processes be used to execute payments in the short-term?
Vulnerable customers (retail or commercial)	<ul style="list-style-type: none"> • Vulnerable customers • Customers in distress 	<ul style="list-style-type: none"> • Of all payments not settled, how many are clearly identifiable as relating to vulnerable customers? • Where might this information come from? • How would a need to complete payments for vulnerable customers alter the relative prioritisation of payments?

3. Impact tolerances

Senior leaders and the Board will be responsible for approving impact tolerance statements indicating the firm or FMI's impact tolerance level during the loss of a business service in a severe but plausible scenario.

Limitations of conventional approaches

A severe but plausible scenario is one where the nature, scale or scope of the event goes beyond pre-considered recovery measures and supporting assumptions. While outputs from conventional risk management and business continuity approaches are often used to inform recovery plans such as risk appetite statements and recovery time objectives, recent severe disruptions show that these can be easily breached.

Firms and FMI must identify an objective or goal (the impact tolerance) that will focus investment in resilience measures and their actual response during a disruption. This should ultimately minimise harm when the Plan A recovery has not worked or become redundant. It will help prompt organisations to reassess the validity of their plan A and develop a plan B in the form of workarounds or alternative contingency arrangements. This should be part of the overall operational resilience toolkit.

Impact tolerances can also be used to understand how best to target investment so that resilience capabilities enable the impact tolerance to be met.

Express an outcome-based objective

Firms and FMI should express impact tolerance statements briefly and simply as a desired outcome or objective, linked to the service provided. Accompanying metrics should be used where practical and appropriate.

This may include a level of service to be achieved within a certain timeframe or by a point in the business cycle after which the impact becomes intolerable. In this context, an impact tolerance statement as currently envisaged in the DP is different to the maximum tolerable period of disruption used in business continuity planning, as it should consider variables other than just incident duration. For example, levels of service to be achieved and customer outcomes needed to reduce harm.

We believe this approach is sensible, defining not just for how long, but how much for how long.

Firms and FMI should establish a set of working assumptions to contextualise and avoid over complicating the statement itself. For example, it could be assumed that the disruption occurred at the worst possible time in the business cycle. Additionally, there would need to be an indication of how long any workarounds or alternative arrangements can be sustained before they are unworkable.

Impact tolerance statements cover severe but plausible scenarios, whereas risk appetite statements and recovery time objectives typically cover low tolerances for disruption and an assumed ability to resolve the situation quickly through pre-planned measures. In severe disruptions, this assumption is being challenged and alternative and interim options should be considered too.

Each important business service should have one or more impact tolerance statement. The statement should typically be scenario-agnostic and provide a valid reference to test resilience capabilities and frame investment decisions. Impact tolerances should be tested against a range of severe scenarios to confirm they can still be met, and to identify scenarios where they cannot be. See scenario testing section.

Example impact tolerance statements

"We aim to settle 85 per cent of payments intraday"

"In the event of a disruption to customer payments (outbound) we aim to achieve 30 per cent completion rate within four hours"

"We aim to achieve a minimum approval rate of 90 per cent for face-to-face transactions within one hour of a disruptive event, and maintain this for a minimum of 24 hours if needed."

Figures 2, 3 and 4 are illustrative and worked examples to show how an impact tolerance could be derived and used to guide a response to a severe but plausible scenario where additional contingency measures are required.

Figure 2. Setting an impact tolerance

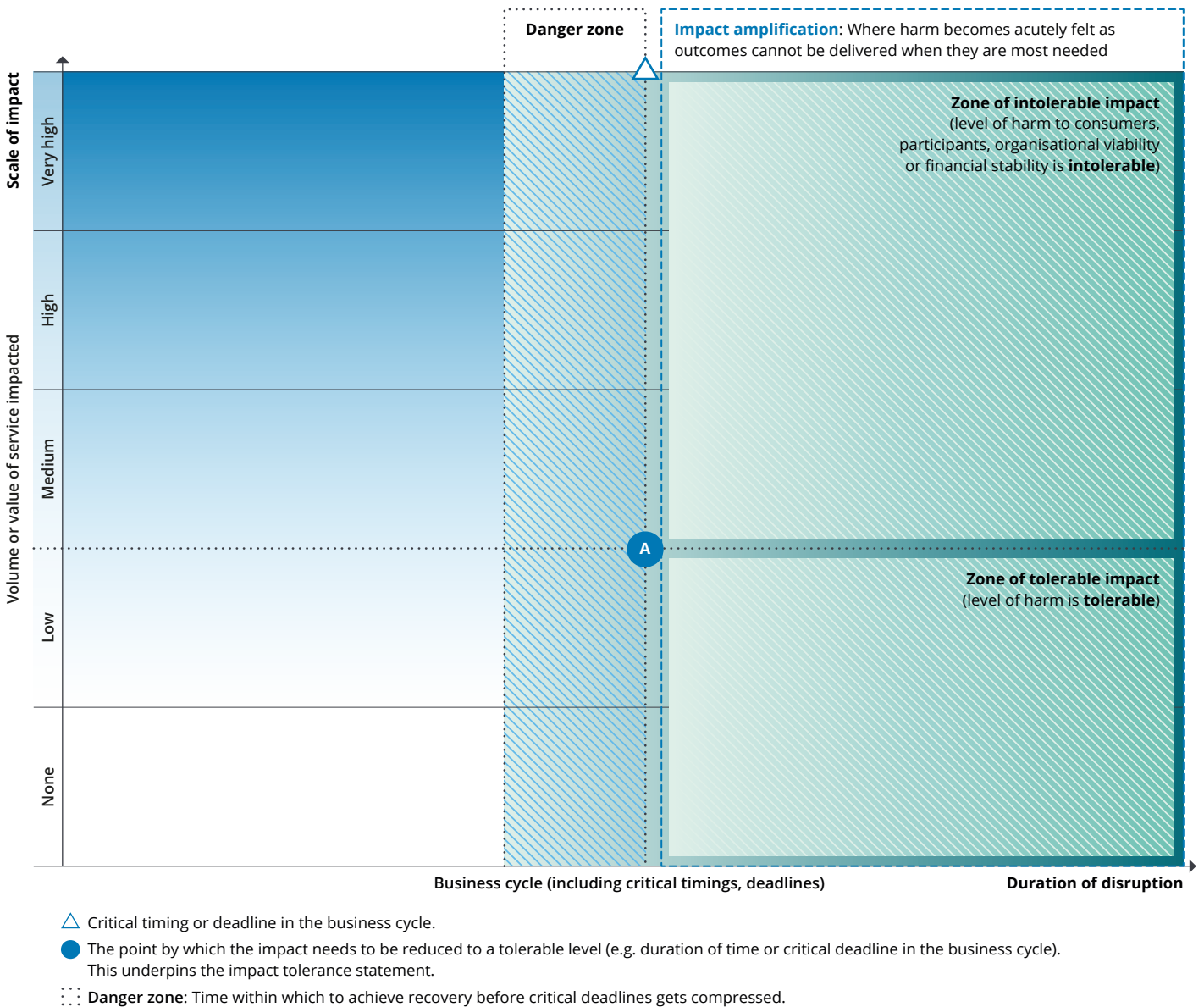


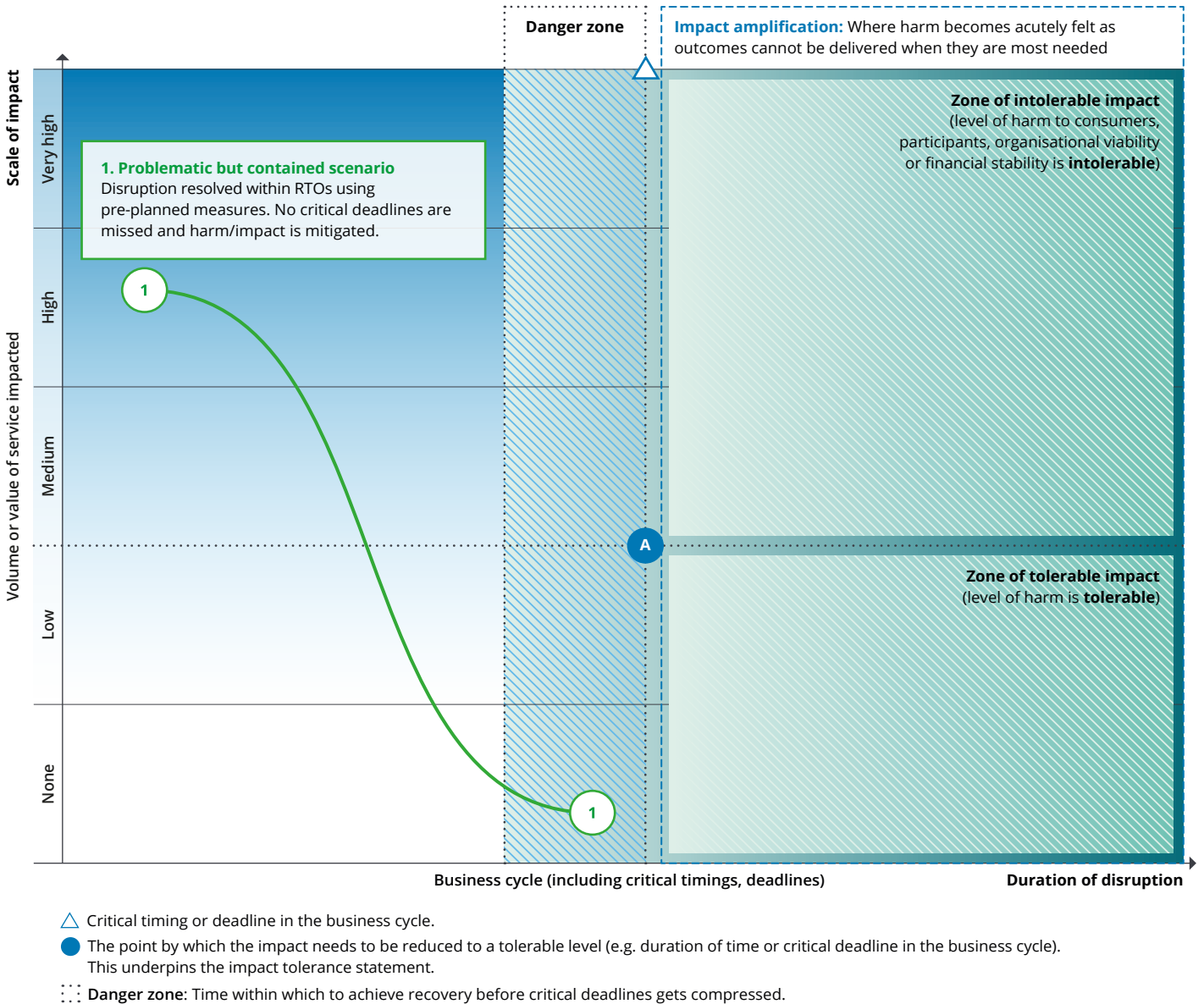
Figure 2 shows how an impact tolerance may be set. It considers the degree of business service recovery needed and by when, to avoid intolerable harm to consumers, participants, organisational viability and financial stability ('A').

The recovery needed could be reducing the scale of the disruption to a tolerable level, for example 85 per cent of payments settled. The when could be expressed as a timeframe, such as within four hours, or a deadline such as intraday.

Definition: Impact tolerances

Describe firms and FMI's tolerance for disruption. It references specific outcomes and metrics such as the maximum volume of disruption, criticality of ensuring data integrity or number of customers affected.

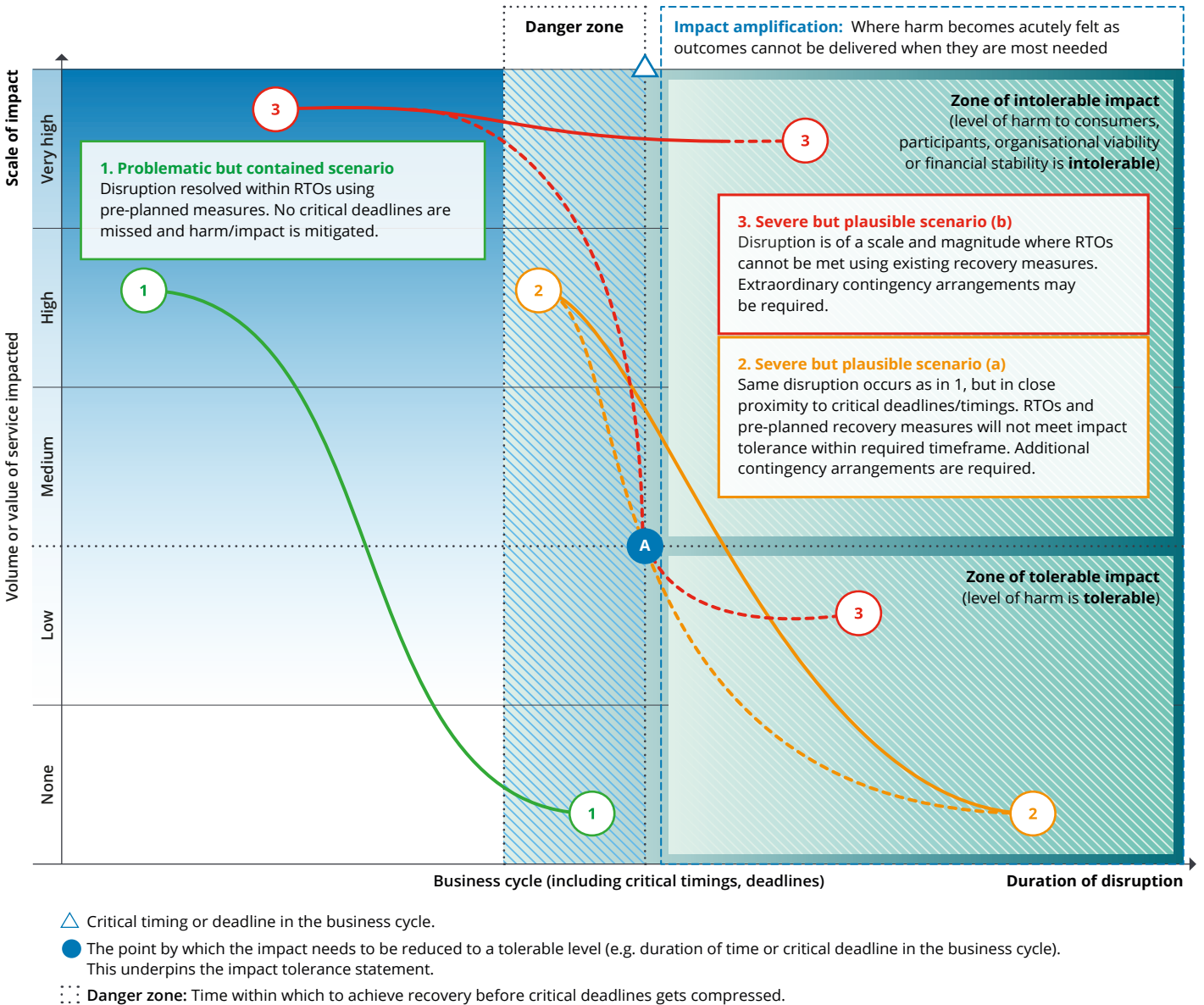
Figure 3. Problematic but contained scenario



The solid green line (1) in figure 3 indicates a ‘problematic but contained’ scenario that typifies a desired recovery. The disruption may be limited in scale or considered resolvable within risk appetite and recovery time objectives using pre-planned measures. Critical deadlines or timings are unlikely to be breached, limiting the harm to consumers, participants, organisational viability or financial stability.

An example may be a limited failure of one or more IT services requiring them to be failed over to an alternate data centre in accordance with documented and practised IT disaster recovery plans.

Figure 4. The severe but plausible scenario



The solid amber and red lines (2 and 3) in Figure 4 indicate severe but plausible scenarios where the disruption is of a significant scale or is unlikely to be fully resolved within desirable timescales or before critical deadlines.

Unless a level of recovery is achieved before a certain point, there will be intolerable harm to consumers, participants, organisational viability or financial stability. To stay within the impact tolerance may require additional or extraordinary arrangements, such as alternate processing, to be deployed alongside conventional recovery measures. This is indicated by the dotted amber and red lines.

Figure 5. Disruption to payments transactions: Worked example

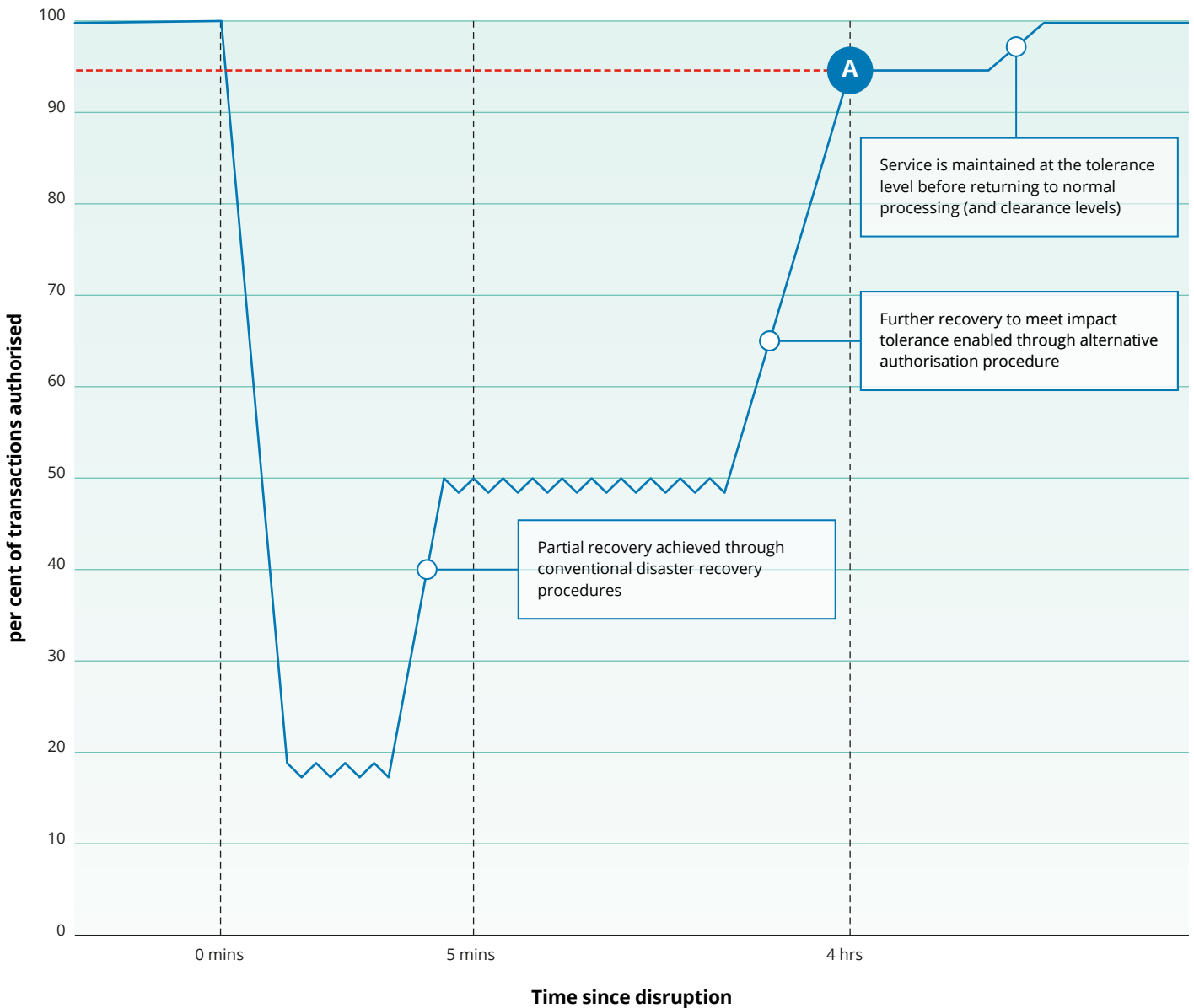


Figure 5 is a severe but plausible disruption that has resulted in the unavailability of transaction authorisation beyond desired recovery time objectives.

The impact tolerance in this example is to achieve 95 per cent of transaction authorisation within four hours of a disruption (A). Extraordinary measures such as alternate processing are required to achieve this operating level.

4. Communications

It is essential to consider human behaviour in any response and recovery scenario.

Good communications seek to inform, maintain trust and confidence, and provide clear actions. They should avoid human behaviours making a difficult situation worse and help people make appropriate decisions or choices to reduce potential harm.

The DP suggests communications need to be an integral part of the operational resilience capability.

Prompt and meaningful

The DP indicates that communications during a disruption should be prompt and meaningful. This can be difficult since the two can be discordant. Communicate early and you can mislead if information shared proves incorrect. Communicate late or infrequently and you can amplify the impact of the disruption.

Firms and FMI need to communicate early to avoid creating a vacuum. Customers expect immediate communication, and if they don't hear from the firm or FMI themselves, they will look elsewhere.

An early statement is unlikely to be meaningful. Simply remove acknowledging a problem and that it is your problem, not someone else's, however, is helpful.

It is important to avoid optimism-bias, keep to what is known, what you are doing and what can be done to mitigate the circumstances.

Some level of communication, even if it is not fully committed, can achieve the objective of reducing harm.

Guiding principles

Firms and FMI should consider what communications are ultimately trying to achieve, setting guiding principles to help structure an appropriate response. Such principles might include:

- an expression of **care and concern**
- a demonstration of **control** over the situation
- an indication of **alternative services** and redress arrangements
- a **commitment** to improve.

Communications as an integral part of operational resilience

The changes the DP introduces may require many firms and FMI to enhance their communications planning and preparations.

An important aspect will be to ensure communications are an integral part of overall operational resilience capabilities and subject to the same governance and assurance processes. This will require specific training of communications teams and operational functions and including the communications team in all strategic and operational crisis management activities.

This will establish defined and rehearsed communications plans and procedures, including full consideration of any necessary surge capacity alongside stakeholder mapping and an understanding of vulnerable stakeholders relevant to the business services affected. These should be tailored to specific scenarios and cover key aspects such as pre-considered actions for customer redress.

The operational resilience approach will need to involve communications specialists and confirm the message and suitability of communications channels, such as website, social media, telephone and call centres, when operating under adverse conditions.

Communications planning should focus on the who, who to and the how, as well as assumptions such as expected increase in call volumes, website hits and suspected fraud cases.

5. Scenario testing

Scenario testing is a key part of operational resilience. It builds and demonstrates capability to respond and recover within pre-defined impact tolerance levels.

The DP highlights the importance of using well-developed severe but plausible scenarios. Adoption of this will lead to a step-change in the nature and extent of operational resilience testing and reporting.

Broaden testing scenarios

Scenario testing as part of business continuity and disaster recovery often focuses on generic unavailability scenarios affecting a single asset. For example, the unavailability of an office or IT system.

There is some utility in this but these tests are often limited in scope and demonstrate a capability to recover those assets within a relatively known and pre-planned environment.

The DP, however, advocates that firms and FMI should expand scenario testing to consider a broader range of severe but plausible scenarios to understand if they can, even under stressed conditions, meet the outcome-based objectives set in their impact tolerance statements.

These should consider the vulnerabilities - for example concentrations and single-points-of-failure - identified in the mapping of the business service, whose disruption could quickly become amplified. The cyber stress tests initiated by the FPC indicate the severity that might be expected in operational resilience scenario tests.

Develop a scenario testing approach

The scope of a test is unlikely to focus on a single plan or recovery measure. Several contingencies should be deployed together as part of an operational resilience toolkit, such as extraordinary workarounds alongside more conventional business continuity and disaster recovery procedures, to meet impact tolerances.

Similarly, there is unlikely to be one test or simulation that can validate all contingencies across a business service at the same time.

Instead, firms and FMI should provide aggregated assurance that their testing:

- is focused on the right parts of the organisation – important business services
- uses appropriate scenarios – severe but plausible and relevant to any vulnerabilities identified in the service
- measures success against the agreed impact tolerances.

Scenario testing for operational resilience can, and often, includes a simulation exercise to validate operational resilience arrangements.

We believe that even paper-based analysis of operational resilience capabilities against such scenarios and impact tolerances will be a valuable step forwards. This could take the form of a summary document describing the:

- test scenario used
- business services impacted, within the scope of the test
- impact tolerance statements that apply
- sequence of operational resilience contingency measures deployed in this scenario such as business continuity plans, alternate processing arrangements, communications plans, delegated authority arrangements
- degree to which those measures, individually and collectively meet the applicable impact tolerance statements, including identified gaps
- date each of the above measures were last tested, individually or collectively.

Measure success – can impact tolerances be met?

Testing impact tolerances in this way will help firms and FMI to push their services to the brink of their impact tolerance thresholds.

Firms will understand whether operational dependencies are resilient and recoverable, including if alternative processing options or workarounds are feasible and sustainable. This will confirm the breadth of functional support needed for recovery and determine if investment in resilience measures is appropriate, or where risk may need to be accepted.

Some firms and FMI already perform dynamic tests and exercises that use a range of scenarios but the success criteria for operational resilience testing has been broadly underdeveloped to date. There is also a notable lack of an industry standard to provide guidance on desirable approaches and outcomes.

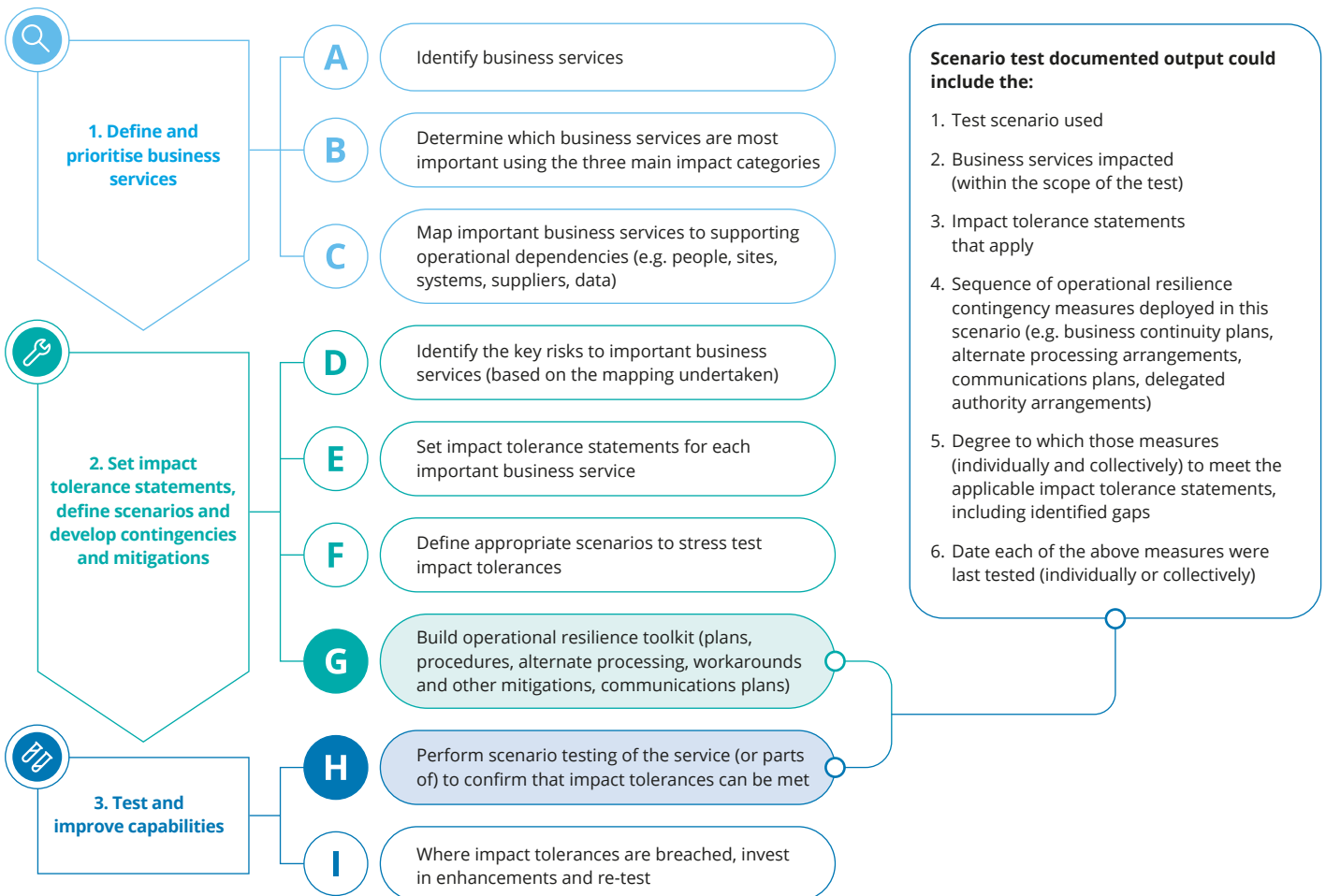
Since the authorities advocate the integration of operational resilience and operational risk, many firms may look to the Basel III 'principles for sound stress testing practices and supervision' to understand how to implement the scenario testing aspect of the DP. The Basel III principles establish a clear benchmark and objectives to determine the success of stress-testing, which may set a desirable standard for operational resilience.

“Some firms and FMI already perform dynamic tests and exercises that use a range of scenarios but the success criteria for operational resilience testing has been broadly underdeveloped to date.”

Summary

We have explored five opportunities to develop and enhance operational resilience capabilities based on the direction set out in the DP. Below, we summarise the steps to implement them.

Figure 6. Implementing the key aspects from the DP



Next steps

The DP introduces a number of potentially important changes for the financial services sector's approach to operational resilience. By looking at these changes now, accountable executives can set the foundations early for responding to future regulatory developments. They will also better understand where and how to invest in operational resilience.

In the longer-term, there may be implementation challenges that accompany a new regulatory framework on operational resilience. It is anticipated that a consultation paper on the matter will be released in Autumn 2019, and that a supervisory framework will start to be applied mid-to-late 2020.

Throughout that journey, the regulatory authorities are likely to modify parts of their approach in response to stakeholder feedback and make the framework practical to apply to a broad range of firms and FMI.

The DP, however, introduces a number of opportunities that will better enable firms and FMI to prepare for, respond to, recover and learn from high-impact events, as well as realise sensible efficiencies and make better investment decisions by adopting a top-down, business services based approach.

The direction of intent is clear, and while there may be some adjustments and greater illustration of key points, there is a strong case for firms and FMI to act now, rather than wait. This is particularly important to inform the debate.

Initial steps may include:

- a gap analysis of your current approach to the areas highlighted in this paper
- consideration of the definition of business services within your organisation
- develop more detailed impact consideration and criteria for harm done
- develop example impact tolerance statements
- consider potentially severe, but plausible scenarios.

Early assessment of the likely scale of changes needed and the plan, resources and budget required to do this is recommended, as execution will need to start no later than 2020.

Contacts

As leaders and pioneers in resilience and crisis management over the last 10 years, we have a depth and breadth of expertise and are well placed to help firms and FMI understand the complexities and nuances involved in building operational resilience.

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



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



David Strachan
Partner
Head of EMEA Centre for
Regulatory Strategy
+44 20 7303 4791
dastrachan@deloitte.co.uk



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



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



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



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



Charles Barlow
Senior Manager
Reputation, Crisis & Resilience
+44 20 7303 5189
cbarlow@deloitte.co.uk



Lucy Jones
Manager
Reputation, Crisis & Resilience
+44 20 7303 4656
lujones@deloitte.co.uk



Notes



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2019 Deloitte LLP. All rights reserved.

Designed and produced by 368 at Deloitte. J18297