Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Cross Industry Guidance on Operational Resilience

July 2025

Contents

Back to “Contents”

Version Control

Version No.	Purpose/change	Author	Date
0.0	Initial Publication of the Cross Industry Guidance on Operational Resilience post public consultation.	The Operational Resilience Team, Prudential Analytics and Inspections Directorate.	December 2020
0.1	General: Minor updates ensuring alignment with the Digital Operational Resilience Regulation and Directive (DORA). At the same time, to ensure regulatory simplification and clarity, the Central Bank has withdrawn its September 2016 Cross Industry Guidance in respect of Information Technology and Cybersecurity Risk Management.	Governance and Operational Resilience Management Division and Banking, Insurance & Payments Policy Division	July 2025
	Guideline 3: Updated to ensure that firms recognise that operational resilience and operational risk are distinct from each other, whilst acknowledging that there is alignment.		
	Guideline 4: Additional clarity included on critical or important business services based on industry feedback. Primarily, explaining that critical or important business services are external facing services that should have an identifiable external end user;		
	Guideline 5: Additional context included for the setting of their impact tolerances by emphasising that a breach of an impact tolerance would lead to 'irrecoverable consequences for customers, the firm and the wider financial system'		
	Guideline 9: This guideline has been updated to reflect DORA requirements and to clarify that those firms not currently subject to DORA are encouraged to take equivalent measures as part of their operational resilience programme.		

Back to "Contents"

A. Introduction

In keeping with the Central Bank of Ireland's ("the Central Bank") strategic commitment of strengthening our ability to maintain the resilience of the financial system[1], it is important to continue to address existing vulnerabilities and weaknesses, and mitigate risks in the financial system to ensure that it can better withstand future shocks and crises and to limit the impact of such events.

Since the publication of the first iteration of this Guidance, we have seen the gradual maturing of operational resilience frameworks within regulated financial service providers ("firms"). In addition, the financial services industry has experienced a number of significant shocks against a background of ongoing change to financial services, the technology that supports the delivery of those services, and the regulation that governs this important topic. While the core objective of this Guidance is to communicate to industry how to prepare for, respond to, and recover and learn from an operational disruption that affects the delivery of critical or important business services, this update has been informed by recent developments and valuable ongoing industry engagement.

The financial services industry operates in an increasingly complex and interconnected environment, facilitating the provision of services locally and internationally. In many cases, firms rely on international third party service providers to support their operations. Internationally, financial services firms have experienced challenges from various disruptive events including technology failures, cyber incidents, the COVID-19 pandemic and natural disasters, as well as geopolitical risks.

Financial sector regulation provides legislative and regulatory risk management, governance requirements, and guidelines to minimise the risk of disruptive events occurring. However, they provide limited direction on how to prepare for those disruptions when they do occur. The Central Bank of Ireland believes that sharing good practice and ensuring a common understanding of a pragmatic and

[1] Central Bank of Ireland - Our Strategy 2024

Back to "Contents"

proportionate approach to operational resilience will strengthen industry's ability to respond to and recover from such events.

This Guidance aims to enhance the operational resilience of firms and of the financial services sector as a whole mindful of the interconnections and interdependencies within the financial system that result from the complex and dynamic environment in which firms operate.

More specifically, the purpose of the Guidance is to:

- Communicate to the boards and senior management of firms the Central Bank's expectations with respect to the design and management of operational resilience;
- Emphasise board and senior management responsibilities when considering operational resilience as part of their risk management and investment decisions; and
- Require that the boards and senior management take appropriate action to ensure that their Operational Resilience Frameworks are well designed, are operating effectively, and are sufficiently robust. This should ensure that the risks to the firm's operational continuity do not transmit into the financial markets and that the interests of the customers and market participants are safeguarded during business disruptions.

The Guidance does not purport to address in detail every aspect of a firm's legal and regulatory obligations relating to operational resilience, and should be read in conjunction with the relevant legislation, regulations, and other guidance or standards issued by relevant industry bodies, supervisory authorities or the Central Bank. The Guidance does not supersede existing sectoral legislation, regulations, or guidance, but is intended to complement and support them. The Central Bank may update or amend the Guidance from time to time in light of future regulatory requirements.

Back to "Contents"

B. Definitions

Table 1 | Definitions

Term	Definition
Operational Resilience	The ability of a firm, and the financial services sector as a whole, to identify and prepare for, respond and adapt to, recover and learn from an operational disruption.
Business Service	A service that a firm provides to an external end user. Business services deliver a specific outcome or service to an identifiable user and should be distinguished from business lines or functions that are a collection of services and activities.
Critical or Important Business Service	A service provided by a firm to an external end user or market participant where a disruption to the provision of the service could cause material customer detriment; harm market integrity; compromise policyholder protection; or threaten a firm's viability, safety and soundness; or financial stability.
Outsourced Third Party Service Provider	Any third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, or providing services to a firm including under an outsourcing arrangement. This refers to both external third party service providers and intra-group service providers.
Impact Tolerance	Impact tolerances determine the maximum acceptable level of disruption to a critical or important business service.
Mapping	Mapping is the process of identifying, documenting and understanding the chain of activities involved in delivering critical or important business services. This incorporates the identification of all interdependencies and interconnections including people, processes, information, technology, facilities, and third parties service providers.
Scenario Testing	Scenario testing is the assessment of a firm's ability to remain within its impact tolerance for each of its critical or important

Back to “Contents”

	business services in the event of a severe, but plausible, disruption of its operations.
Board	It is acknowledged that some smaller, less complex firms may not have a board of directors. In these cases, where the term 'board' is used, it is intended to address the relevant management bodies or structures of these regulated firms.
ICT risk	ICT risk means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.

Back to "Contents"

C. Concept of Operational Resilience

The Central Bank considers operational resilience to be the ability of a firm, and the financial services sector as a whole, to identify and prepare for, respond and adapt to, recover and learn from an operational disruption.

An operationally resilient firm is able to recover its critical or important business services from a significant unplanned disruption, while minimising negative impacts and protecting its customers and the integrity of the financial system.

The first step in becoming operationally resilient is accepting that disruptive events will occur, and that these events will need to be managed effectively. A firm needs to have forward-looking plans that can be applied across a range of potential disruptions. A firm should proactively prepare to withstand and adapt to disruptions that will inevitably occur.

The Central Bank sees the management of a firm's operational risk and resilience as an aligned approach that is integrated into the firm's governance structures. Operational resilience is an evolution of operational risk and business continuity management and, as such, should be aligned with existing or developing frameworks in these areas.

Operational risk management is focused on minimising risk through development of controls that reduce the impact and probability of an operational event occurring. Operational resilience goes beyond this and promotes a deeper understanding of a firm's business and all the steps/activities involved in delivering its critical or important business services. It focuses on building capabilities to deal with risk events when they materialise, rather than purely focusing on building defences to prevent risk events from occurring.

This Guidance is complementary to the European Union's new Digital Operational Resilience Regulations (DORA), which focus on achieving a high level of digital operational resilience in firms. This Guidance will benefit and aid all firms (whether subject to DORA or not) in strengthening their operational resilience.

Back to "Contents"

Continuity of critical or important business services is an essential component of being operationally resilient, although operational resilience is much wider than just continuity and recovery. Operational resilience requires coordination between risk management, business continuity management (BCM), incident management, third party risk management, Information Communication Technology (ICT) risk management, and recovery and resolution planning.

A firm's operational resilience strategy should be cause agnostic and flexible enough to adapt to different types of disruption. Resilience is not about what happens to a firm, but rather, how a firm is able to withstand and respond to an incident when it does occur.

D. Value of Operational Resilience

An operational disruption can threaten the viability of individual firms, impact customers and other market participants, and ultimately affect financial stability. A firm needs to consider all of these risks when assessing the appropriate levels of resilience of the business services it provides. Operational resilience benefits the firm itself by strengthening its ability to remain a viable ongoing concern. At both an individual firm level and a sectoral level, operational resilience is critical to supporting services to customers and supporting the wider economy as well as safeguarding investors and consumers.

A resilient financial system is one that can absorb shocks rather than contribute to them. The financial system needs an approach to operational risk and resilience that includes preventative measures and the capabilities - in terms of people, processes, technology, and organisational culture - to recover and adapt when disruptions occur.

The increased dependence on technology, coupled with an accelerated pace of change has led to a rise in operational incidents across all sectors in recent years. This has brought to the fore the discussion around the need for firms to become more operationally resilient. Operational disruptions can result from man-made causes such as Information and Communications Technology (ICT) related

Back to "Contents"

threats (e.g. outages, cyber-attacks, change management issues); terrorist threats; civil disturbances; insider threats (e.g. internal arbitrage, insider trading); third party dependencies; and natural causes (e.g. storms, pandemics).

The COVID-19 pandemic exposed significant vulnerabilities in global business operations, underscoring the need for robust operational resilience. Organisations faced unprecedented disruptions to supply chains, workforce availability, and digital infrastructure, highlighting the critical importance of preparedness. In the post-pandemic era, companies are expected to prioritise operational resilience strategies to ensure continuity amid future crises, including cyber threats and economic instability. Regulatory bodies worldwide have also emphasised the need for resilient systems, especially in sectors like finance, healthcare, and logistics. As a result, operational resilience has become a cornerstone of long-term business sustainability and stakeholder trust.

In addition, changing customer behaviour is putting pressure on firms to enhance their digital offerings and has placed a different type of stress on how firms operate.

Focus on operational resilience is an opportunity to improve decision-making and value creation by targeting investment into the services that are critical or important to a firm and the economy, and focusing on services that could have the most material impact if unavailable.

E. International Alignment

The operational resilience landscape continues to evolve with new standards and consultations being proposed and/or published across multiple jurisdictions. In developing and maintaining this Guidance, the Central Bank engaged with our international regulatory colleagues and reviewed the more significant and innovative regulatory proposals across the European Union (EU), the UK, Asia, Australia, and the USA.

The more advanced principles include:

Back to “Contents”

- the Basel Committee on Banking Supervision's (BCBS) 'Principles for operational resilience'[2] ;
- the joint Bank of England (BoE), Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA) policy statement on their approach to operational resilience across the financial services sector[3] ; and
- the 'Digital Operational Resilience Act' (DORA)[4] .
- work is also underway in the International Association of Insurance Supervisors (IAIS) to develop an application paper on operational resilience objectives and toolkit.

Aspects of the various policy approaches may differ across jurisdictions, regulators are aligned on the fundamentals and core principles of operational resilience. However, they remain focused on ensuring that the risks to a firm's operational continuity, due to the firm's operational complexity and interconnectedness with the broader financial ecosystem, are not transmitted across the financial system and that the interests of the customers and market participants are safeguarded during business disruptions.

The US Federal Reserve Board (FRB), the UK's PRA, and the European Central Bank (ECB) have agreed coordinated statements on operational resilience, which have been issued to all Global Systemically Important Banks (GSIBs)[5] as well as non-GSIBs. In the statement, the authorities commit to actively work together to refine the approaches to operational resilience to ensure that they comprehensively consider risks as they evolve.

Operational resilience for the financial services sector does not, at present, benefit from one clear, detailed international standard. The Central Bank, in developing this Guidance, has sought to develop a holistic approach that aligns with the prominent international

[2] Basel Committee on Banking Supervision - Principles for Operational Resilience
[3] Bank of England - Operational resilience: Impact tolerances for important business services
[4] DORA, the Digital Operational Resilience Act Regulation EU 2022/2554 entered into force in January 2023 and applies from 17 January 2025 onwards. DORA introduced inter alia harmonised requirements for information and communication technology (ICT), risk management framework (RMF), incident reporting, and third-party risk management and testing
[5] European Central Bank - Statement regarding supervision cooperation on operational resilience

Back to "Contents"

thinking and that will allow firms with a presence in more than one jurisdiction the flexibility to develop an Operational Resilience Framework that can be applicable across all operations. The Central Bank will continue to monitor international developments and further enhance operational resilience across the financial services sector.

F. Scope of Application

The Central Bank is the competent authority in Ireland for the regulation and supervision of financial services firms across a variety of sectors and in line with the relevant sectoral legal requirements. We serve the public interest by maintaining monetary and financial stability while ensuring that the financial system operates in the best interests of consumers and the wider economy.

Operational resilience is important for individual firms, customers and the wider economy. Therefore, this Guidance should be considered by all regulated firms to ensure that they have adequate governance, systems and controls, processes and procedures, to enhance capabilities to deal with risk events when they materialise, thereby strengthening their ability to remain a viable ongoing concern when faced with operational disruptions.

This Guidance describes the Central Bank's expectations for an adequate and appropriate approach by firms to ensure that critical business services can survive disruption. Firms should follow this Guidance to understand the impacts of operational disruptions and prepare for them, to ensure that firms can respond and adapt to the disruptions to critical or important business services.

The Guidance is intentionally not prescriptive or at a granular level of detail to allow for a pragmatic application. As such, it is designed to be flexible and can be applied by all firms in a proportionate manner based on the nature, scale and complexity of their business.

Back to "Contents"

G. Implementation

It is the Central Bank's expectation that the boards and senior management of firms review the Guidance and adopt appropriate measures to strengthen and improve their Operational Resilience Frameworks and their effective management of operational resilience in line with this Guidance. Regulated firms should be able to demonstrate that they have applied this Guidance.

H. Supervisory Approach

The Central Bank's mission is to serve the public interest by safeguarding monetary and financial stability and by working to ensure that the financial system operates in the best interests of consumers and the wider economy. Our supervisory objectives are to protect consumers and financial stability by seeking to ensure that firms:

- Act in the best interests of consumers;
- Are financially sound and safely managed with sufficient financial resources;
- Are governed and controlled appropriately, with clear and embedded risk appetites, which drive an effective culture; and
- Have frameworks in place to ensure failed or failing providers go through orderly resolution.

The Guidance outlined in Schedule 1 seeks to enhance the Central Bank's regulatory framework by focusing firms' attention on their most critical or important business services and functions which, if disrupted, could cause prudential or consumer harm or have an impact on overall financial stability.

Back to "Contents"

The Central Bank expects boards and senior management of firms to review the Guidance and adopt appropriate measures to strengthen and improve their governance and risk frameworks and their effective management of operational resilience. A firm should be able to demonstrate that it has considered the supervisory expectations set out in this Guidance and developed a plan to meet the Guidance.

The Central Bank will utilise risk-based supervisory engagement to assess the core principles of operational resilience in firms and drive to enhance and mature operational resilience across the financial system. This will include an assessment of:

- Board ownership and accountability for the firm's operational resilience strategy and framework and the firm's ability to demonstrate a keen understanding of its critical or important business services. The Central Bank will look for evidence that the board is seeking the required information to enable it to understand the risk and resilience profile of the firm and make targeted investment decisions to support on-going resilience efforts;
- The firm's understanding of the delivery of its own critical or important business services, the people, the activities, information, technology, and third parties that support that delivery, and the criticality of those services to the wider financial system;
- A firm's ability to determine appropriate impact tolerances for its critical or important business services and that they test their ability to remain within those impact tolerances under severe but plausible scenarios; and
- The firm's consideration of third parties in its response and recovery processes and that they are aligned and tested for effectiveness.
- A firm should conduct and document an annual operational resilience self-assessment. These reviews should cover all aspects of the three pillars of operational resilience and be reviewed and approved by the board.

Back to "Contents"

The Central Bank will keep its regulatory framework and supervisory approach to operational resilience under review, based on our regulatory and supervisory experience and international developments. We are conscious that the regulatory framework within the EU is developing further, the introduction of DORA is one example. We believe that this Guidance is in line with international best practice and compatible with/complementary to DORA and the 'Directive on Security of Network and Information Systems' (NIS2). Our aim is to align and update the intended outcomes of our supervisory approach with the operational resilience policy developments as they evolve.

Schedule 1: Operational Resilience Guidelines

Introduction

The overarching principle of operational resilience is the acceptance that disruptions will occur and that firms need to be prepared to respond accordingly and have measures in place to limit the impacts. A firm needs to ensure that they have prepared effectively, and have the flexibility to withstand, absorb, respond, adapt, recover and learn from disruptions with minimal impact on their critical or important business services.

Approaching operational resilience through a business service lens encourages a firm to prioritise what is critical or important to their firm and the financial system and to understand the interconnections and interdependencies involved in delivering those services. Ultimately, this will allow firms to determine the wider impact a disruption will have on the services that it provides.

A firm should take ownership of its own operational resilience and prioritise based on the potential impacts to itself, its customers and financial stability.

The core principles of any Operational Resilience Framework are:

Back to "Contents"

- Board and senior management ownership of the Operational Resilience Framework;
- The identification of critical or important business services; and all activities, people, processes, information, technologies and third parties involved in the delivery of these services;
- The setting of impact tolerances for each of these identified services, and the testing of the firm's ability to stay within those impact tolerances during a severe but plausible operational disruption scenario; and
- The continuous review of how a firm responded and adapted to disruptive or potentially disruptive events so that lessons learned can be incorporated into operational improvements to continually enhance the operational resilience of the firm.

Three Pillars of Operational Resilience

The Central Bank Guidance is built around three pillars of Operational Resilience:

- Identify and Prepare
- Respond and Adapt
- Recover and Learn

These three pillars support a holistic approach to the management of operational resilience and related risks and create a feedback loop that fosters the perpetual embedding of lessons learned into a firm's preparation for operational disruptions.

Back to "Contents"

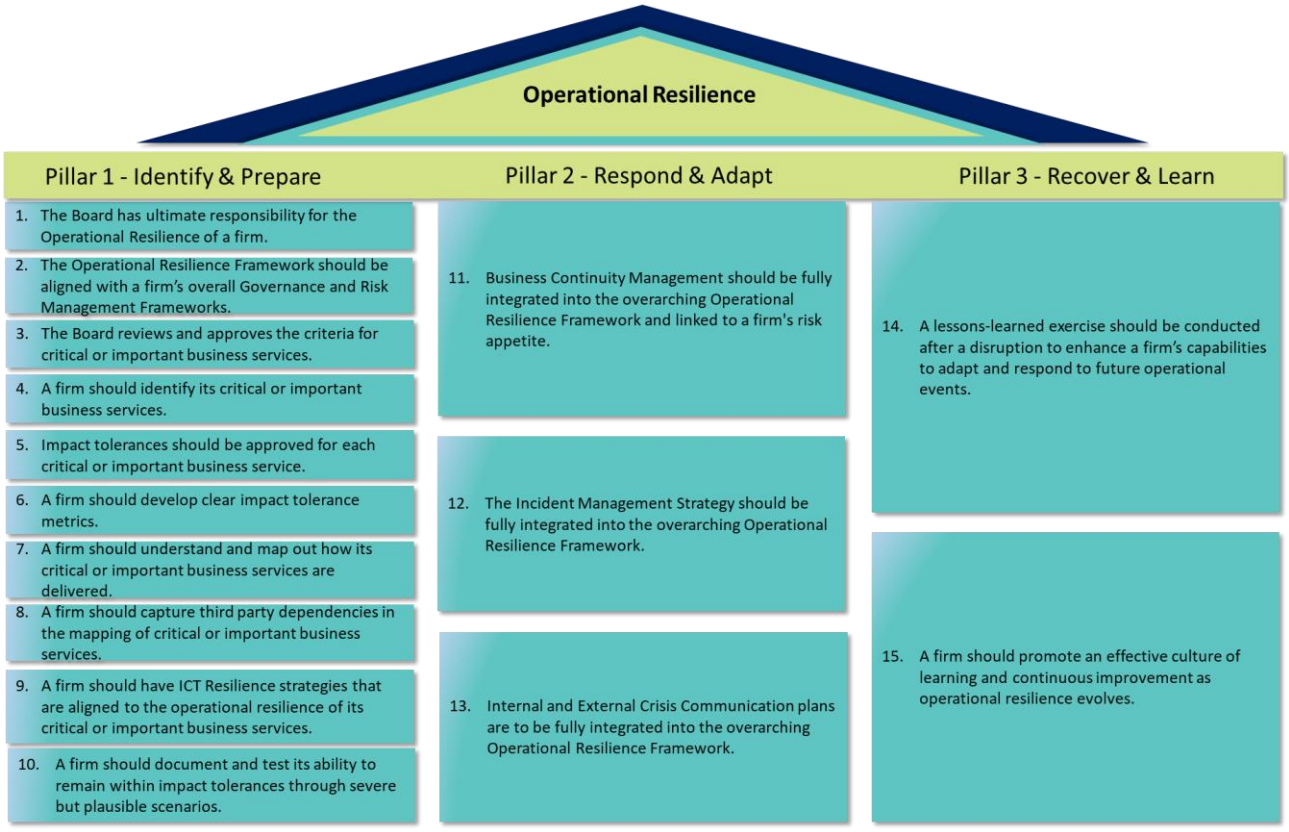

Figure 1: The Three Pillars of Operational Resilience

Back to "Contents"

Pillar 1: Identify and Prepare

1 Governance

Guideline 1:

The Board has ultimate responsibility for the Operational Resilience of a firm.

A firm's board has the ultimate responsibility for the approval and oversight of the firm's Operational Resilience Framework. Leadership from the top down should ensure that resilience is intrinsically built into a firm's strategic decisions and should allow boards to prioritise activities and target investment towards making critical or important business services more resilient. A top down approach to operational resilience creates a uniform process flow and enhances clarity on the responsibilities throughout the organisation to conduct business within approved impact tolerances.

All board members should have sufficient understanding to provide effective oversight and challenge of the firm's operational resilience. Senior management should have the financial, technical and other resources needed in order to support the firm's overall operational resilience efforts under the oversight of the board.

The board and senior management should have accurate and adequate oversight of resilience activities, trends and remediation measures, which should allow the board to make the business decisions regarding investments and risk exposure. A firm should provide formal operational resilience management information ("MI") to its board on a regular basis and in the event of a disruption. The operational resilience MI should be embedded into the existing reporting structure in an adequate, meaningful and timely manner. Escalation routes should be established for when vulnerabilities are identified or when an unexpected disruption occurs.

The board has responsibility for the approval of the Operational Resilience Framework and approval of the critical or important business services, impact tolerances, business service maps, scenario testing to ascertain the firm's ability to remain within impact tolerances, and communications plans. The board should review the components of the Operational Resilience Framework at least

Back to "Contents"

annually, through a documented self-assessment to confirm that there are no undetected developing weaknesses.

The board should oversee senior management assessments of the components of the Operational Resilience Framework. The board is responsible for review, challenge and approval of the assessments of its critical or important business services, impact tolerances, business service maps and scenario analysis annually and/or as part of the lessons learned exercise after a disruption has occurred.

The actions a firm takes to improve operational resilience, including through its investment decisions, should be prioritised based on factors such as the potential impact of disruptions, time criticality and progress required to be able to remain within impact tolerances.

Guideline 2:

The Operational Resilience Framework should be embedded within a firm's overall Governance and Risk Management Frameworks.

A firm should utilise its existing governance and risk management structures when implementing an effective Operational Resilience Framework. A firm will need to ensure that its existing governance frameworks and committee structures include responsibilities with respect to operational resilience.

The Central Bank views operational resilience and operational risk as separate but aligned disciplines. Firms are expected to manage these disciplines through distinct yet aligned frameworks, where operational resilience focuses on identifying the most critical services and guides response during disruptions, and operational risk focuses on the management and control of risks that could impact operations. Operational resilience is an evolution of operational risk, providing a holistic firm-wide approach to managing disruptions to critical or important business services. A firm should develop a documented Operational Resilience Framework aligned with its Operational Risk and Business Continuity Frameworks.

Operational resilience should be strategically implemented across the business by senior management throughout the Operations, Risk and Finance pillars. As operational resilience draws from elements of

Back to "Contents"

business continuity, third party risk management, ICT risk management, incident management, and wider aspects of operational risk management, a holistic approach is essential if a firm is to enhance the resilience of its business services, regardless of the type of disruption. The three-pillar approach to operational resilience aligns all of these elements into an effective Operational Resilience Framework.

2 Identification of Critical or Important Business Service

Guideline 3:

The Board reviews and approves the criteria for critical or important business.

The starting point for any firm in enhancing its operational resilience is to set the criteria for defining its critical or important business services. It is the responsibility of the board to approve clearly defined and documented criteria to determine how business services are classified as critical or important.

The criteria should enable a firm to identify its critical or important business services and prioritise them in the event of a disruption. This should be achieved by considering the impact a disruption to a critical or important business service would pose to its external end users through three lenses: (i) impact on customer, (ii) impact on firm's viability, safety and soundness and (iii) impact to overall financial stability.

The criteria for the identification of critical or important business services should be reviewed and approved by the board annually or at the time of implementing material changes to the business that would involve additional critical or important business services.

Guideline 4:

A firm should identify its critical or important business services.

Once a firm has set its criteria, the firm should identify its critical or important business services and functions. Traditionally, firms have focused on protecting individual systems, processes and functions rather than looking at the complete end-to-end chain of activities

Back to "Contents"

required to deliver a particular business service. Operational resilience challenges a firm to rethink how it views its operations and puts in place measures to protect its most critical business services and to ensure the continued delivery of those services to external end users or market participants throughout a disruption.

Critical or important business services are external facing and should have an identifiable external end user. Whereas, processes, functions and business lines are internal facing and may form part of the chain of activities that support the delivery of a service. A firm should leverage its existing business functions' knowledge when identifying and prioritising their critical or important business services. As critical or important business services will differ between individual firms and sectors, firms should take an outcomes based approach to identification of these services. Ultimately, it will be the responsibility of the board to review and approve all business services classified as 'critical' or 'important' on at least an annual basis.

Critical or important business services should be identified to enable a firm to (i) clearly determine impact tolerances based on maximum acceptable levels of disruption, (ii) perform mapping of the end-to-end delivery of the business service, including any dependence on third parties, and (iii) to perform tests based on severe but plausible scenarios.

Furthermore, a firm should consider whether the number of critical or important business services is proportionate to the nature, scale and complexity of its business.

3 Impact Tolerances

Guideline 5:

Impact tolerances should be approved for each critical or important business service.

A firm should develop impact tolerances for each of its critical or important business services on the assumption that disruptive events will happen. The purpose of an impact tolerance is to determine the maximum acceptable level of disruption to a critical or important business service.

Back to "Contents"

Impact tolerances should be set at the point at which disruption to the firm's business service would pose, or has the potential to pose, a risk to the firm's viability, safety and soundness, would impact wider financial stability or could cause material detriment to customers. The breach of an impact tolerance of a critical or important business service may indicate to the firm that the impacted service has irrecoverable consequences for customers, the firm and the wider financial system.

Impact tolerances should be used as a planning tool for a firm rather than as a tool to measure regulatory compliance. Impact tolerances will enable a firm to understand its level of operational resilience in the event of an unplanned disruption. Impact tolerances are designed to determine the schedule by which a firm should be able to restore the delivery of critical or important business service after a disruption has occurred.

Impact tolerances need to be tested against severe but plausible scenarios to determine their appropriateness; i.e. to determine whether the firm is able to stay within the defined impact tolerances during a disruption.

The Central Bank expects a firm's board to review and approve impact tolerances at least annually, or following a disruption, to ensure they remain fit for purpose.

While impact tolerances should be aligned to a firm's risk appetite, impact tolerances are a separate and distinct tolerance measurement. Risk appetite focuses on the impact and probability of a risk event occurring and is typically set with reference to a firm's strategic goals. Risk appetite is 'the aggregate level and types of risk an organisation is willing to assume within its risk capacity to achieve its strategic objectives and business plan'[6].

Impact tolerances assume that the risk event has already crystallised and, therefore, the probability element of risk appetite is removed. When a disruption has impacted a critical or important business service the risk appetite will have already been breached.

Impact tolerances are a standard that a firm should be able to remain within and which the board and senior management should use to

[6] Financial Stability Board - Principles for An Effective Risk Appetite Framework

Back to "Contents"

drive improvements to their operational resilience. Firms have the flexibility to determine impact tolerances for their critical or important business services, including leveraging any appropriate pre-determined and approved criteria as part of other practices. For example, this may include processes used for Business Impact Analysis (BIA), Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) and Maximum Tolerable Outage (MTO) where these metrics, measure the disruption of single points of failure that feed into the delivery of a critical or important business service.

Guideline 6:

A firm should develop clear impact tolerance metrics.

A firm should set at least one impact tolerance metric for each of its critical or important business services. Impact tolerance metrics need to be clear and measurable, and can be both qualitative and quantitative. To achieve this, they should reference specific outcomes and measurements. A firm should be able to determine the outcome if the impact tolerances are exceeded.

At a minimum, there should be a time-based metric indicating the maximum acceptable duration a critical or important business service can withstand a disruption. A time-based metric ensures that a firm focuses its response to a disruption on the continuity of its critical or important business service.

To be prepared to withstand more than one type of disruption a firm should consider having additional impact tolerance metrics, which for example, could be based upon:

- the maximum tolerable number of customers affected by a disruption;
- the maximum number of transactions affected by a disruption; or
- the maximum value of transactions impacted.

This is not an exhaustive list, and firms should set and approve impact tolerance metrics based on their specific critical or important business services taking into account the nature, scale and complexity of the firm.

Back to “Contents”

4 Mapping of Interconnections and Interdependencies

Guideline 7:

A firm should understand and map out how its critical or important business services are delivered.

To ensure that a critical or important business service can remain within its impact tolerance(s), a firm needs to understand how the services are delivered and how each service can be disrupted. A firm will need to understand the chain of activities that contribute to the delivery of each of its critical or important business services in order to be able to identify any critical or single points of failure, dependencies, or key vulnerabilities.

A firm should identify, document and map the necessary people, processes, information, technology, facilities, and third parties service providers required to deliver each of its critical or important business services. This exercise should be undertaken collaboratively across the business to ensure comprehensive mapping.

Mapping should be conducted at a level of detail that enables the identification of the resources that contribute to the delivery of each stage of the service and their importance. A firm should understand how these resources blend and work in combination to deliver the critical or important business service. A firm should identify which business units own each resource and from where it is provided.

The approach and level of granularity of mapping should be sufficient for a firm to identify vulnerabilities and key dependencies, and to support testing of its ability to stay within the assigned impact tolerances for each critical or important business service.

Comprehensive mapping of a service will enable a firm to pinpoint vulnerabilities in how critical or important business services are being delivered and determine where recovery and resolution plans can be leveraged. Examples of such vulnerabilities could include concentration risk, single points of failure, key person risk, and inadequate substitutability of resources.

Guideline 8:

A firm should capture third party dependencies in the mapping of critical or important business services.

Back to “Contents”

The increasing complexity of firms' operating models, and the increased reliance on third party service providers (TPSP) for the delivery of key elements of their critical or important business services, can often result in a firm being dependent on a multitude of resources across many different third party providers, including other regulated firms, for the delivery of critical or important business services.

A complex network of external interconnections and interdependencies increases the risks related to the use of third parties. If a disruptive event occurs anywhere within this network of interconnected activities, the firm can be impacted, even if the event did not occur within its own systems. A complicated network of outsourced activities reduces visibility over potential vulnerabilities in the delivery of critical or important business services. This can hamper a firm in preparing for an operational disruption and therefore, capturing these dependencies as part of the mapping process will be a key tool in managing operational disruptions.

Boards and senior management should be cognisant of the fact that when entering into outsourcing arrangements they are creating a dependency on a third party for the resilience of their firm. A firm should manage its dependencies on relationships, including those of third parties involved in the delivery of critical or important business services. Dependencies should be clearly identified and detailed in the mapping of critical or important business services. A firm's critical or important business services should be able to remain within impact tolerances, including when they rely on TPSPs. A firm should undertake due diligence in respect of its TPSPs prior to entering into an outsourcing arrangement, to ensure that third party arrangements have appropriate operational resilience conditions that enable the firm to remain within its impact tolerances.

A firm should ensure that legally binding written agreements are in place with third parties that detail how the critical or important services will be maintained during a disruption and how an exit strategy if/when the service cannot be maintained is executed. A firm should also take into account the geographical location of the third party, which may impact on the provision of service depending on the nature or location of the event.

Back to "Contents"

A firm should also be aware of any chain outsourcing that exists for all its critical or important business services and should manage and monitor accordingly. Chain outsourcing can complicate the effective management of the critical or important business service and a firm should have clear written agreements in place regarding any chain outsourcing that may impact the provision of a critical or important business service.

This Guideline should be read in conjunction with the Central Bank's "Cross Industry Guidance on Outsourcing"[7]. In respect of ICT services provided by a third party, firms subject to DORA must ensure compliance with the provisions relating to the management of third party risks. Firms that are not subject to DORA should consider that the application of the measures described in that regulation represent good practice.

5 ICT Resilience

Guideline 9:

A firm should have ICT Resilience strategies that are aligned to the operational resilience of its critical or important business services.

Information and communications technology (ICT) is a key driver and enabler of most firms' business models and as such the resilience of the technology infrastructure and the protection of its ICT assets should be an integral to any Operational Resilience Framework.

A firm should ensure that its ICT systems and dependencies are appropriately managed to ensure a high level of digital operational resilience and support the overall operational resilience of the firm.

The European Union has established the Digital Operational Resilience Act (DORA) to bring together provisions addressing digital operational resilience across all European financial sectors in a consistent manner. The Central Bank recognises the requirements of DORA as representing good ICT risk management, incident management, testing, third party and information sharing practices for all financial entities to ensure both the resilience of individual firms and the financial sector as a whole.

[7] Central Bank of Ireland - Cross Industry Guidance on Outsourcing

Back to "Contents"

Firms should identify those information and ICT assets supporting their critical and important business functions, and thus supporting their critical and important business services as described in this Guidance. In doing so, firms should develop an understanding of the various roles and dependencies in relation to the management of ICT risk and should maintain a register of ICT third-party service providers in order to support the mapping under guidelines 7 and 8 of this Guidance.

As part of ensuring their operational resilience, the Central Bank expects that firms that are not directly subject to DORA should nevertheless consider introducing equivalent measures as part of their operational resilience in line with the nature, scale and complexity of their operations, and, in respect of their ICT risk management framework, consider at least DORA's Simplified Risk Management Framework[8].

6 Scenario Testing

Guideline 10:

A firm should document and test its ability to remain within impact tolerances through severe but plausible scenarios.

A firm should test its ability to remain within its impact tolerances for every critical or important business service through severe but plausible scenarios. Testing can only be effective once clear and detailed maps have been developed for critical or important business services.

In carrying out the scenario testing, a firm should identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to delivery of the firm's critical or important business services in those circumstances. Mapping facilitates the identification of an individual firm's idiosyncratic risks and allows for the development of appropriate testing.

The nature and frequency of testing should be proportionate to firm size and complexity. A flexible approach allows a firm to carry out scenario testing at an appropriate level to identify vulnerabilities

[8] The Simplified Risk Management Framework under Chapter II of DORA is defined in Article 16 of DORA and in Title II of the Commission Delegated Regulation (EU) 2024/1774.

Back to "Contents"

within the chain of activities of their critical or important business services. A firm that implements change more regularly should undertake more frequent testing. This should at least be completed annually for all firms. A firm should consider various testing methods such as paper based or simulation testing on a number of critical or important business services.

A scenario test should identify any vulnerabilities or reliance on third parties. The results of which should focus investment in the resolvability of a vulnerable element, determine alternative channels of delivery or identify the elements that can be substituted if disrupted. Additionally, the results can identify areas where an increase in capacity is required, a reduction in manual intervention, where staff need appropriate training, and what outsourcing arrangements need to be reviewed.

A firm should design a test plan and document the scope of the exercise, the steps taken or considered during the exercise, and should capture and act upon the lessons learned from the exercise. This will provide greater assurance that a firm has adequate contingency plans in place to identify and prepare for, respond and adapt to, recover and learn from an operational disruption.

A firm's board should review the results of all scenario testing carried out on critical or important business services. If scenario testing identifies a situation where impact tolerances may be breached, then it would be the responsibility of the board and senior management to take action to improve the resilience of the business service and focus investment, where needed. The design and implementation of remediation plans are the responsibility of senior management and the results of the remediation plans should be reviewed and approved by the board thereafter.

Pillar 2: Respond and Adapt

7 Business Continuity Management

Guideline 11:

Business Continuity Management should be fully integrated into the overarching Operational Resilience Framework and linked to a firm's risk appetite.

Back to "Contents"

Continuity of business services is an essential, forward-looking, component of being operationally resilient. While operational resilience is much broader than traditional business continuity management (BCM) and recovery, approved business continuity plans should be utilised as part of the holistic response to a disruption.

Where traditional BCM focuses on single points of failure, such as individual systems, people or processes, operational resilience goes a step further by determining how these single points of failure have the potential to affect the end-to-end delivery of critical or important business services.

When a disruption occurs to a firm's critical or important business services, the Business Continuity Plan (BCP) should be enacted as part of the response process. For BCM to be aligned with the Operational Resilience Framework, the BCPs should be tested through severe but plausible scenarios and include any third party interdependencies or interconnections. To respond effectively to a disruption, an integrated BCP should incorporate invocation processes, impact analyses, recovery strategies, training programmes and crisis management programmes to guide the management of a disruption and limit the impact.

A firm should adopt a holistic approach to BCM by mapping critical or important business services (discussed in section 4) and develop a recovery plan in line with approved impact tolerances[9].

Key personnel should be identified and have completed the necessary training. Training and awareness programmes should be customised based on specific roles to ensure that staff can effectively execute contingency plans when responding to a disruption.

Where interdependencies on third parties for the delivery of critical or important business services have been identified, it should be verified that these arrangements have appropriate operational resilience conditions to ensure the firm can remain within its impact tolerances. The arrangements should be reviewed and tested at least annually. The firm should consider identifying the dependencies that can be substituted in the event of an unexpected disruption.

[9] With regard to BCM management of ICT functions, the Central Bank invites firms to consider good practices such as DORA's requirements in relation to ICT business continuity management.

Back to "Contents"

8 Incident Management

Guideline 12:

The Incident Management Strategy should be fully integrated into the overarching Operational Resilience Framework.

Incident management is an essential component of being operationally resilient. Operational resilience requires a firm to have an approach to incidents that covers the full life cycle of an event, from the classification of incidents that trigger approved response procedures, to testing the incident management procedures and reflecting on lessons learned from the occurrence of incidents.

For incident management to be aligned with the Operational Resilience Framework, a firm should develop and implement response and recovery plans and procedures to manage incidents that have the potential to disrupt the delivery of critical or important business services. When responding to an incident, the incident management plans should be developed to consider how a disruption can affect a firm's risk appetite and impact tolerance metrics.

A firm should maintain an inventory to support the firm's response and recovery capabilities that includes the incident response and recovery steps followed during a disruption, internal and third party resources potentially impacted, and communication plans followed.

Incident response and recovery procedures should be reviewed, tested and where relevant updated at least annually. Root causes should be identified and managed to prevent the serial recurrence of incidents. Lessons learned from previous incidents, including incidents experienced by others, should be reflected when updating the incident management program and learnings from incidents should be considered as part of scenario testing. A firm's incident management program should manage all incidents impacting or potentially impacting the firm.

In respect of major ICT-related incidents in line with the Digital Operational Resilience Act (DORA), firms subject to DORA should ensure compliance with the Regulations provisions on ICT-related incident management, classification and reporting.

Back to "Contents"

9 Communication Plans

Guideline 13:

Internal and External Crisis Communication plans should be fully integrated into the overarching Operational Resilience Framework.

A crisis communication plan should be developed either as part of a firm's Operational Resilience Framework or contained in the BCM/recovery plans to communicate effectively during a disruption.

A key part of an effective crisis communications plan is the identification and preparation of key resources and experts that can be leveraged when a disruption occurs. By doing so, this will aid the mitigation of the harm caused during a disruption.

The firm should develop internal and external communication plans and stakeholder maps that can be implemented during a disruption. The internal communication plan should contain escalation routes on how to communicate with key-decision makers, operational staff and third parties if necessary. The external communication plan should outline how the firm will communicate with their customers, stakeholders and regulators during a disruption.

Pillar 3: Recover and Learn

10 Lessons Learned Exercise and Continuous Improvement

Guideline 14:

A lessons learned exercise should be conducted after a disruption to a critical or important business service to enhance a firm's capabilities to adapt and respond to future operational events.

A firm should conduct a lessons learned exercise after any disruption to a critical or important business service. This includes any potential material disruption to a third party provider that feeds into the delivery of a critical or important business service.

The lessons learned exercise should utilise the information gathered as part of the incident management or disaster recovery process. The decisions and recovery processes determined to be appropriate throughout the incident management process should form the basis of the lessons learned exercise.

Back to "Contents"

A lessons learned exercise allows a firm to reflect on the three-pillar approach to operational resilience and allows for a feedback loop into the first two pillars that encourages improvement in how a firm prepares for and recovers from disruptions.

A firm should have predetermined criteria or questions that form the basis of the lessons learned exercise. These questions should identify deficiencies that caused a failure in the continuity of service and these deficiencies should be addressed as a matter of priority. Specifically, at a minimum, the following should be considered:

- How and why the incident occurred;
- The identified vulnerabilities;
- The impact on the delivery of critical or important business services;
- Whether the risk controls, decisions and recovery processes and communications were appropriate; and
- The speed of recovery and whether the impact tolerances are adequate.

The lessons learned exercises should define effective remediation measures to redress deficiencies and failure in the continuity of service. Doing so will allow a firm to agree remedial actions and adjust any impact tolerances, if determined. This should all be contained within a self-assessment document and presented to the board, as outlined in the next Guideline.

Guideline 15:

A firm should promote an effective culture of learning and continuous improvement as operational resilience evolves.

Continuous improvements to operational resilience requires a firm to learn from its experiences as changes to its operational approaches, or technology infrastructure mature over time. This should not only occur after a disruption has occurred but should form part of ongoing operational resilience governance discussions.

A firm should promote an effective culture of learning and continuous improvement as operational resilience evolves. Operational resilience needs to be a fundamental element of any

Back to “Contents”

strategic decision taken by a firm. Any changes to strategy or the business model should be considered through a business service lens. A firm should determine the impact of strategic changes on the delivery of critical or important business services or any of the chain of activities that have been documented as part of the mapping exercise.

A firm should document and update written self-assessments highlighting how it meets current operational resilience policy requirements on at least an annual basis. These reviews should cover all aspects of the three pillars of operational resilience, from the identification of critical or important business services through to lessons learned exercises and ensure that no emerging vulnerabilities are overlooked.

The self-assessment should detail the rationale for determining all criteria from the Identify and Prepare pillar. For example, a firm should evaluate the current list of critical or important business services and state why each has been identified, with reference to regulatory expectations. A similar process, detailing the firms' approach to impact tolerances, mapping and scenario testing, should be applied to determine whether current practice meets regulatory guidelines.

Back to "Contents"

Schedule 2 - Glossary

Table 2 | Glossary

Acronym	Meaning
BCBS	Basel Committee for Banking Supervision
BCM	Business Continuity Management
BCP	Business Continuity Plan
BoE	Bank of England
DORA	Digital Operational Resilience Act (EU) 2022/2554
ECB	European Central Bank
EU	European Union
FCA	Financial Conduct Authority
FRB	Federal Reserve Board
GSIB	Global Systemically Important Bank
ICT	Information and Communications Technology
MI	Management Information
NIS2	Second Directive on Security of Network and Information Systems (EU) 2022/2555
TPSP	Third Party Service Provider
PRA	Prudential Regulatory Authority

Back to “Contents”

T: +353 (0)1 224 5800
E: publications@centralbank.ie
www.centralbank.ie

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem