Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Feedback Statement – Consulatation Paper 140: Cross Industry Guidance on Operational Resilience

December 2021

Contents

Introduction

The Central Bank of Ireland's (the Central Bank's) consultation paper (CP140) on the *Cross Industry Guidance on Operational Resilience* (the Guidance) outlined the Central Bank's proposed approach and perspectives in relation to how the financial sector should prepare for, respond and adapt to, and recover and learn from, an operational disruption that affects the delivery of critical or important business services.

Stakeholders were invited to provide feedback on the proposals and to comment on whether the guidelines included the key elements necessary for effective operational resilience, and whether there are the other areas that should be covered in the proposals or in future guidance.

Sixteen responses were received from stakeholders, including regulated financial service providers (RFSPs), representative bodies, industry consultancies, and third service providers, over a three-month consultation period from 9 April to 9 July 2021.

Respondents generally welcomed the consultation and agreed that the Guidance includes the core elements of an effective Operational Resilience Framework. They acknowledged that that the Guidance represents a reasonable and pragmatic approach to operational resilience for financial entities, and is presented in a clear and structured manner.

While the feedback related to a number of sections within the Guidance, the majority of the comments revolved around the following themes:

1) Proportionality;
2) International Alignment;
3) Governance and Board Ownership;
4) Critical or Important Business Services;
5) Mapping of Outsourced Service Providers (OSPs);
6) Impact Tolerances and Metrics; and
7) Scenario Testing.

The feedback was generally constructive and provided us with a greater understanding of how the Guidance might be interpreted or applied across the different financial sectors. A significant proportion of the comments related to the need for proportionality given the wide range of firms operating in the Irish financial sector, and the need to ensure that, as

international regulation evolves in this space, the Central Bank's approach is able to adapt accordingly. Most of these comments do not affect the content of the Guidance itself but have been included in this Feedback Statement to evidence how we welcome and addressed that feedback.

After considering all the feedback, the finalised Guidance remains largely unchanged from that consulted upon. Where changes have been made, they do not alter the intent or purpose of the guidelines but instead provide additional context to remove any perceived ambiguity or provide additional reassurance about how the Guidance will be applied. The key guidelines where additional context has been added are:

- Guideline 2 to more accurately reflect the need for alignment between the Operational Risk and Operational Resilience Frameworks rather than incorporating frameworks into each other;
- Guideline 4 to confirm that that the number of critical or important business services should be proportionate to a firm's business model and not solely determined by the size of the firm;
- Guideline 5 & 6 to clarify that impact tolerance metrics can be both qualitative and quantitative and that firms may leverage appropriate existing approved processes as part of the development of impact tolerances; and
- Guideline 8 to further align the expectations of this Guidance with those of the *Cross Industry Guidance on Outsourcing*.

The Central Bank is grateful for the time and effort of the stakeholders that responded to the consultation. This Feedback Statement summarises the material responses along with the Central Bank's comments and decisions in relation to the relevant guideline.

The Feedback Statement is structured such that the overarching themes of proportionality and international alignment are addressed first, with the remaining feedback and responses presented under the headings of the three pillars of operational resilience and in the order of the guidelines under those pillars. Each section details the expectation of the relevant guideline, the feedback received in relation to that Guideline, and how the Central Bank has addressed the comments in the finalised Guidance.

The Feedback Statement is published to promote an understanding of the policy development process within the Central Bank and is not relevant to assessing compliance with regulatory requirements.

Governance and Operational Resilience Division

Central Bank of Ireland

1 December 2021

General Responses

Proportionality

Section F of the Guidance 'Scope of Applications', explains that the Guidance applies to all RFSPs but that the Central Bank expects the Guidance to be applied in a proportionate manner depending on the nature, scale and complexity of the firm.

Feedback:

The majority of the responses received related to the concept of Proportionality. Respondents generally endorsed the flexibility in the design of the Central Bank's approach to operational resilience and the fact that the Guidance is intended to be applied by firms in a proportionate manner based on the nature, scale and complexity of their business.

However, respondents sought reassurance that the finalised Guidance will retain such a flexible and proportionate approach and that this approach would apply to the individual components of the Operational Resilience Framework detailed throughout the guidelines.

Furthermore, reassurance was sought that the Central Bank will maintain a risk-based approach to the supervision of operational resilience and that this supervisory model would continue be part of the Central Bank's proportionate approach to the application of the Guidance.

Central Bank Response:

Under Section F of the finalised Guidance, 'Scope of Application', the Central Bank confirms that the Guidance is designed to be flexible and should be applied by firms in a proportionate manner based on the nature, scale and complexity of their business. The Guidance is intentionally not prescriptive or at a granular level of detail, to allow for a pragmatic application by firms. This promotes a flexible approach to applying the operational resilience guidelines and allows a firm's board to make judgements on its idiosyncratic risks and business services.

The Central Bank has retained this approach in relation to all components of an Operational Resilience Framework throughout the finalised Guidance.

In section H, 'Supervisory Approach', the Central Bank confirms that it will utilise risk-based supervisory engagement to assess the core principles of operational resilience in firms and to drive enhanced and mature operational resilience across the financial system.

International Alignment

In Section A of the Guidance, the Central Bank details that the Guidance does not supersede existing sectoral legislation, regulations, or guidance but is intended to complement and support them.

In Section E of the Guidance, the Central Bank details that it will continue to monitor international developments after the issuance of this Guidance and further enhance operational resilience across the financial services sector.

Feedback:

Respondents welcomed the fact that the Central Bank's holistic approach to operational resilience aligns with prominent existing international operational resilience policies. They agreed that it makes sense to adopt a flexible and pragmatic approach that can be utilised by global firms with operations in multiple jurisdictions, particularly where other jurisdictions have already implemented operational resilience policies.

Respondents acknowledged that the Covid-19 pandemic highlighted the need for further global consistency and coordination in relation to operational resilience. Respondents noted that the value of adopting a cross-sectoral approach in developing global operational resilience principles is that financial institutions can be flexible when adapting to challenging circumstances and when adapting the guidelines to their respective business models.

Respondents sought reassurance that the Guidance will continue to align with the international direction of travel on operational resilience policy, to ensure global entities do not have to comply with inconsistent or conflicting policies in the different jurisdictions in which they operate. Multiple respondents referenced the forthcoming European Digital Operational Resilience Act (DORA), highlighting how several elements of this proposed regulation align with the principles set out in the Central Bank's Guidance and requested reassurance that the Central Bank's approach will remain aligned with this regulation as it evolves.

Central Bank Response:

As outlined in the 'International Alignment' section (Section E) of the Guidance, the Central Bank acknowledges that the regulatory landscape for operational resilience is still evolving with new standards and consultations being proposed and/or published across multiple jurisdictions. While aspects of the various policy approaches may differ across jurisdictions, global regulators are aligned on the fundamentals and core principles of operational resilience and have committed to actively working together to refine the approaches to ensure they comprehensively consider risks and issues as they evolve.

In developing these guidelines, the Central Bank engaged with our international regulatory colleagues and examined existing and forthcoming operational resilience policy across several jurisdictions to ensure that our Guidance was aligned in principle with the general international thinking in this space. The Central Bank is committed to continuing to monitor international developments and to engage on these regulatory issues to ensure that our approach continues to follow best international practice.

The Central Bank notes that 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 the relevant industry bodies, supervisory authorities, or the Central Bank.

The Central Bank notes that the Guidance is in line with international best practice and compatible with/complementary to DORA. Further detail in relation to alignment with DORA is addressed below in the response to the feedback relating to ICT & Cyber Resilience.

Specific Responses

Pillar 1

Governance

Guideline 1 expects that the board has ultimate responsibility for the operational resilience of a firm. This includes approval of the Operational Resilience Framework and all of the related components. Guideline 1 requires the board to review these components, at least annually.

Guideline 2 articulates the relationship between a firm's Operational Risk and Operational Resilience Frameworks and recognises the aligned objectives of both frameworks.

Feedback:

In relation to Governance, several respondents commented on the level of board involvement in the approval and oversight of the Operational Resilience Framework and asked for clarity on the expectations in relation to incorporating the Operational Risk Framework into the Operational Resilience Framework.

Respondents felt there is an over emphasis on the direct involvement of the board, but agree that the board should have overarching ownership of the Operational Resilience Framework.

Board Ownership

- Respondents questioned the expectations of the board detailed throughout the Guidance, and in particular, whether the board should 'own' the approval of the Operational Resilience Framework components. Respondents sought clarity on the appropriateness of the board having an oversight role and senior management or sub-groups carrying out the assessments of the components of the Operational Resilience Framework.
- Respondents expressed concerns with the review timeline of "at least annually", stating that it has the potential to indicate that these actions could be taken more than once a year.
- Respondents suggested that the proposed Guidance had the potential to blur the lines between the role of the non-executive directors and that of senior management with respect to oversight of the Operational Resilience Framework, and suggested that this would require additional workload and greater time commitment by the directors.

- A concern was raised regarding small firms, sole-traders and firms with voluntary boards or no board structure in place. Respondents asked for clarification regarding how these firms can comply with the Guidance, and suggested that stringent compliance with the Guidelines will be challenging.

Operational Risk and Operational Resilience Framework Alignment

- Further clarity was sought concerning the relationship between the Operational Risk and Operational Resilience Frameworks. A number of respondents suggested that the Operational Risk Framework to be aligned with the Operational Resilience Framework rather incorporated into it, as per the wording in the consultation paper. Respondents also suggested that firms be permitted flexibility to maintain separate frameworks, or provide one holistic framework, depending on business models, or the size and scale of the firm.

Central Bank Response:

Board Ownership

As stated in Guideline 1, a firm should view operational resilience as 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. The Central Bank considers the board's involvement in the approval of the Operational Resilience Framework, and all of its components, to be fundamental to incorporating operational resilience into the discussion of the firm's strategic objectives. The Central Bank has aligned itself with international thinking on this area.

Due to the significance of critical or important business services for the firm, its customers, and wider financial stability, the board needs to be ultimately responsible for reviewing and approving the firm's strategic approach to operational resilience, which would be articulated through the Operational Resilience Framework. Senior management are responsible for implementing the Operational Resilience Strategy.

The Central Bank has considered the feedback received and intends to proceed with the proposal as set out in Guideline 1 in relation to the board having ultimate responsibility for the operational resilience of the firm.

The review frequency is important for a firm to be able to confirm that there are no undetected or developing operational weaknesses. The Central Bank expects that, where the risk environment has remained unchanged, this should be a straightforward process but this will encourage the board to remain aware of the operational resilience landscape.

The Central Bank has considered the feedback received and additional context has been added to Guideline 1 to reinforce the objective of the review process.

Operational Risk and Operational Resilience Framework Alignment

The Central Bank views operational resilience, as an evolution of operational risk and business continuity management and, as such, considers that a firm's approach to operational resilience should align with its approach to operational risk and business continuity management. The Central Bank recognises that firms need flexibility in how they structure their management of these different, but related, activities but also acknowledges that they all are working towards the same strategic objective of making the firm more resilient against the impact of operational disruptions. Therefore, after considering the feedback received, additional context has been added to Guideline 2 to emphasise their aligned objectives. Where the consultation paper stated that Operational Risk and Operational Resilience should be *'enacted through one consistent framework'*, this has been revised in the finalised Guidance to state that they should be 'enacted through aligned frameworks'. In addition, where the consultation paper stated that a firm should develop a documented Operational Resilience Framework *'incorporating the Operational Risk and Business Continuity Frameworks'*, this now states that it should be *'aligned with the Operational Risk and Business Continuity Frameworks'*.

Additional context was also included in Guideline 2 to state that 'The three pillar approach to operational resilience aligns all of these elements (business continuity, third party risk management, ICT & cyber risk management, incident management, and wider aspects of operational risk management) into an effective Operational Resilience Framework.'

In response to the feedback received regarding small firms, sole-traders and firms with voluntary boards or no board structure in place, the Central Bank considers the definition of a board as per Section B of the Guidance to be appropriate. 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. Therefore, these firms should take a proportionate approach in terms of their nature, scale and complexity.

Identification of Critical or Important Business Services

Guideline 3 expects the board to approve clearly defined and documented criteria to determine how business services are classified as critical or important.

Guideline 4 expects that a firm should identify its critical or important business services based on criteria approved by the board. Only services that are provided by a firm to an external end user or participant where a disruption to the provision of the service could cause material customer detriment; harm market integrity; threaten policyholder protection, a firm's viability, safety and soundness, or financial stability are categorised as 'critical or important'.

Feedback:

Most respondents welcomed and supported the flexible approach to determining critical or important business services and acknowledged that this approach allows firms to take their unique business models and risk profiles into consideration. However, there are areas where respondents sought further clarity, particularly in regards to the criteria for identifying critical or important business services.

Criteria for Critical or Important Business Services

- Respondents requested that the Central Bank provide further clarity on the criteria that RFSPs should use to designate critical or important business services or to provide examples in the finalised Guidance.
- Respondents asked if the criteria implies that a service can be considered either 'critical' or 'important', and whether firms will be expected to document their rationale for why certain services are not deemed either critical or important.
- Respondents requested further clarity on the inclusion of internal services (for example, payroll and cash management services) that could be deemed critical or

important, or if firms should explicitly exclude internal services that could affect resilience.

- Respondents noted that the size of a firm might not always be indicative of the number of critical or important business services, which should be identified, or the importance of those critical or important business services.

Central Bank Response:

The Central Bank has intentionally set the definition of critical or important business services at a high level to allow firms and sectors the flexibility to use their own judgement in identifying their critical or important business services.

The Central Bank has purposely included both the terms 'critical' and 'important' in the definition to emphasise that it is not only the business services that are critical from a financial system/financial stability perspective that we are concerned about making more resilient, but also business services that are critical or important to the viability of the firm itself. This terminology of 'critical or important' also aligns to other regulatory developments in this area, including the forthcoming DORA regulations.

The Central Bank has considered the feedback received and intends to proceed with the criteria of a critical or important business service as set out in Guideline 3 of the Guidance.

The Central Bank encourages boards and senior management to make judgements in the selection of their critical or important business services based on the definition in the Guidance. Critical or important business services will differ between individual firms and sectors as firms take an outcomes-based approach to the identification of these services. Determining whether a service is critical or important takes into account both an individual firm's safety and soundness and its impact on wider financial stability. The Central Bank expects this to differ between firms and sectors. The Central Bank determines that an inclusion of a list of critical or important business services has the potential to exclude certain sectors and influence the judgment of firms.

The Central Bank agrees that the number of critical or important business services should be proportionate to a firm's business model and idiosyncratic risks and not solely determined by the size of the firm. After considering the responses received,

the Central Bank has amended Guideline 4 to reflect this adjustment. Where the consultation paper stated that *'It is likely that larger firms will identify a larger number of critical or important business services than smaller firms'*, the finalised guidelines have removed that statement and instead states that *'a firm should consider whether the number of critical or important business services is proportionate to the nature, scale and complexity of its business.'*

As defined in Section B and further detailed in Guideline 4, a business service delivers a specific outcome to an identifiable external end user (e.g., a customer or market participant). An internal service that forms part of the chain of activities required to deliver a critical or important business service to an external end-user should be captured in the mapping exercise. An internal service would not be considered a business service on its own.

The Central Bank has considered the feedback received, in relation to internal services being included in the criteria of critical or important business services, and intends to proceed with the definition as set out in Section B of the Guidance.

Setting Impact Tolerances

Guideline 5 sets out the Central Bank's expectations in relation to impact tolerances. A firm should develop impact tolerances for each of its critical or important business services. The impact tolerance should articulate the maximum acceptable level of disruption for that critical or important business service. The firm's board should review and approve the impact tolerances at least annually, or when a disruption occurs.

Guideline 6 sets out the Central Bank's expectations for firms to develop clear and measurable impact tolerance metrics for each of their critical or important business services. At least one impact tolerance metric should be set for each critical or important business service.

Feedback:

Respondents supported the use of impact tolerances, and acknowledged that this approach aligns with international principles on operational resilience. However, respondents requested further clarity on how to apply the Central Bank's expectations.

Examples

- Several respondents requested examples of non-financial impact tolerance metrics, including both qualitative and quantitative metrics. They also felt the provisions of examples across different industry types would be beneficial. Some respondents also suggested that detail was required on whether the Central Bank expects specific minimum tolerance levels for particular services.
- Respondents agreed that time-based metrics are important, but stated that they may not always be the dominant factor. A number of respondents have asked the Central Bank to provide more examples of non-time based impact tolerances in the final guidelines, and clarity on how non-time based metrics would work in practice.

Leveraging Established Processes

- A number of respondents asked for clarity on how the Guidance on impact tolerances compares to a business impact analysis (BIA) or similar oriented approaches.

- Respondents noted that it is important to recognise firms may already have board approved impact criteria scales in place as part of their existing risk frameworks. Respondents expect to see a degree of alignment between the factors used to set these criteria scales and the factors used set impact tolerances. Allowing firms to leverage off existing relevant criteria should reduce the complexity of this process for firms.

Central Bank Response:

As per Guideline 5, the Central Bank expects firms to set and approve impact tolerances and metrics in a proportionate manner, allowing flexibility for firms to set the impact tolerances and metrics that are appropriate for individual firms' critical or important business services. The Guidance is intentionally not prescriptive or at a granular level of detail to allow for a pragmatic application.

Due to the difference in the nature and scale of external end users, firms may have different impact tolerances for similar critical or important business services. The Central Bank determines that the board should use its judgement while leveraging existing business knowledge when determining impact tolerances and therefore, adding additional examples would not add value across all the firms in scope.

The Central Bank confirms that impact tolerances can be both qualitative and quantitative. The definition of impact tolerances in Section B has been revised to

reflect the scope of potential metrics and this change has been also reflected in Guideline 6. In the consultation paper, the definition of an impact tolerance was that *'impact tolerances quantify the maximum acceptable level of disruption to a critical or important business service'* and in the finalised Guidance this has been amended to *'impact tolerances determine the maximum acceptable level of disruption to a critical or important business service'*.

Time-based impact tolerance metrics are necessary to ensure there are contingency plans in place to limit the extent of disruptions to each critical or important business service. Firms should focus their response on the continuity of their critical or important business services in the event of a disruption. This has been reflected in Guideline 6 and additional context has been added to the finalised Guidance.

The Guidance provides firms the flexibility to identify, set criteria and develop impact tolerances most appropriate to the firm, based on their individual business models and risk exposures. Firms may leverage appropriate existing approved processes as part of the development of impact tolerances. 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 disruption/recovery of individual systems/processes or single points of failure that feed into the delivery of a critical business service. This has been reflected in Guideline 5 and additional context has been added to the finalised Guidance stating that firms have flexibility when determining impact tolerances, *'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 that measure disruption of single points of failure that feed into the delivery of a critical business service.'*

Mapping

Guideline 7 sets out the importance of mapping out the complete chain of activities, including the people, processes, information, technology, facilities and third parties, that are required to deliver a firm's critical or important business service. This is critical in order for a

firm to fully understand and identify any critical single points of failure, dependencies, or key vulnerabilities.

Guideline 8 sets out the Central Bank's expectations regarding third party arrangements, and the need to capture third party dependencies in the mapping of critical or important business services.

Feedback:

Overall, respondents acknowledged that mapping is a vital component of an Operational Resilience Framework and understand the importance of having comprehensive service maps. Respondents agree that firms should monitor and encourage their Outsourced Service Providers (OSPs) to enhance their level of operational resilience to ensure they are prepared in the event of a disruption to a critical or important business service.

Third Party Dependencies

- Respondents expressed challenges in ensuring that an OSP has "at least equivalent" levels of operational resilience, particularly when situated in a different jurisdiction.
- Respondents noted that where there is significant use of third-party service providers, it may not be possible to identify all elements (people, processes, technology, facilities, third party services providers (TPSPs) and information required to deliver each of its critical or important business services) provided by the OSP to an equivalent level as the firm.

Alignment with Outsourcing Guidelines

- Respondents acknowledged that Guideline 8 should be read in conjunction with the Central Bank's *Cross Industry Guidance on Outsourcing* but asked for further guidance on how these two papers inter-link, and how firms should seek to adopt CP138 with CP140.

Resourcing

- A number of respondents noted that an increased level of resources will be required to complete the mapping component of an Operational Resilience Framework. Respondents feel this area maybe overly burdensome on smaller firms and the principle of proportionality should be considered by the Central Bank in the finalised guidelines.

Central Bank Response:

As detailed in Guideline 8, the Central Bank expects boards and senior management to ensure that any third party arrangements have appropriate levels of operational resilience to ensure that the firm can remain within its defined impact tolerances.

The Central Bank has considered the feedback received in respect to the levels of operational resilience expected of an OSP that feeds into the delivery of a critical or important business service. In order to further align the expectation in the Cross Industry Guidance on Operational Resilience with *the Cross Industry Guidance on Outsourcing*, the stated expectation for an OSP to have *"at least, equivalent'* levels of operational resilience has been modified. Additional context has been added to Guideline 8 that states *'a firm should undertake due diligence in respect of its OSPs 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.'* This change reinforces the overall approach of flexibility and ensures that the board uses its judgement in deciding if the level of operational resilience of an OSP is appropriate to enable the firm to remain within its impact tolerances.

The Central Bank emphasises that these guidelines should still be read in conjunction with the *Cross Industry Guidance on Outsourcing*.

An understanding of the chain of activities that contribute to the delivery of each of a firm's critical or important business services is essential for an operationally resilient firm. Comprehensive mapping of a critical or important business service will enable a firm to pinpoint vulnerabilities and determine where recovery and resolution plans can be leveraged, taking into account the nature, scale and complexity of a firm. Mapping should be conducted at a level of detail that enables the firm to identify the resources that contribute to the delivery of each stage of the critical or important business service. The Central Bank understands that the level of resources required to complete this mapping may be higher for some firms, but it is expected firms will take an approach that reflects the nature, scale and complexity of its business.

ICT & Cyber Resilience

Guideline 9 emphasises the significance of having a resilient ICT & Cyber Framework and the importance of identifying where ICT is part of the chain of activities in delivering a critical or important business service.

Feedback:

Respondents agree that the ICT & Cyber Risk strategy is an important component of an Operational Resilience Framework and that it should be aligned with the pending principles from DORA and NIS2.

International Alignment

- A number of respondents requested that the finalised Guidance align with the forthcoming international ICT and Cyber Resilience principles, making particular reference to DORA, NIS2, guidance published by the European Union Agency for Cybersecurity (ENISA), or other European and global bodies.

Guidance on ICT and Cyber Resilience

- Several respondents stated there is very little guidance on ICT and Cyber Resilience. The Central Bank's Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks, mentioned in paragraph 6.5 of the consultation paper, was published in 2016 and respondents requested more up-to-date guidance that reflects the current technological landscape.

Central Bank Response:

As detailed in the International Alignment section above, the Central Bank notes that this Guidance is in line with international best practice and compatible with and complementary to DORA. The Central Bank will continue to update and align the intended outcomes of our supervisory approach with relevant international operational resilience policy developments as they evolve.

The Central Bank has determined that there are no contradictions between this Guidance and the forthcoming DORA regulation. There are however, many elements of DORA that, when applied, will require firms to build greater resilience into their critical or important business service and thus align with the intended outcome of these guidelines. The Central Bank confirms that it will continue to monitor

international developments after the issuance of this Guidance, including any updates to ICT & Cyber Resilience best practices.

The Central Bank's Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks was published 2016 at a time when there was little formal supervisory guidance on this topic. Since then, however, the EBA published its Guidelines on ICT and Security Risk Management[1] in November 2019 and the EIOPA published its Guidelines on ICT Security and Governance[2] in October 2020. The EBA Guidelines establish requirements for credit institutions, investment firms and payment service providers (PSPs), while the EIOPA guidelines apply to insurance and reinsurance undertakings. Both of these guidelines supersede the Central Bank's 2016 Guidance but do not contradict anything in that Guidance. In addition, the forthcoming DORA will add further regulatory requirements for financial services firms and critical ICT service providers when it comes into effect.

The Central Bank has considered the feedback received and intends to proceed with the requirements of Guideline 9 while assuring firms that we will continue to align with the forthcoming DORA.

Scenario Testing

Guideline 10 sets out the Central Bank's expectations regarding operational resilience scenario testing. Firms should document and test their ability to remain within impact tolerances through severe but plausible scenarios. The guideline allows a firm the flexibility to carry out scenario testing at an appropriate level to identify vulnerabilities within the chain of activities of their critical or important business services.

Feedback

Overall, respondents noted the importance of scenario testing and agree that firms need to test their ability to remain within impact tolerances through severe but plausible scenarios.

Scope of Testing

[1] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
[2] https://www.eiopa.europa.eu/media/news/eiopa-finalises-guidelines-information-and-communication-technology-security-and_en

- Respondents requested further clarity on the scope of testing and the different components of operational resilience scenario testing. Respondents provided feedback signifying that it would be implausible to test all scenarios, and have therefore requested guidance on the generation of scenarios for testing.

Examples

- Respondents requested the that Central Bank to provide examples of good and poor practices, with further requests on design criteria, scenario testing outputs, the process of setting impact tolerances for testing, and expectations of timelines for deployment of remediation plans.

Local entity requirements

- Respondents queried where responsibilities lay in terms of group and local entities. Respondents feel that while critical services are normally determined at group level, the majority of the work and analysis will be done in principle at group level, including scenario testing, with specifics for the local subsidiary.

Remediation Plans

- Respondents commented that the responsibility for the approval of remediation plans arising from scenario testing should rest with senior management, while the board should have an oversight and review role.

Central Bank Response:

Scenario testing involves identifying an appropriate range of adverse circumstances of varying nature, severity and duration relevant to a firm's business and risk profile, and considering the risks to the delivery of the firm's critical or important business services in those circumstances. A firm should test its response plans against these circumstances and determine the impact on its critical or important business services as a result. The mapping exercise should facilitate the identification of an individual firm's idiosyncratic risks and allows for the development of appropriate testing.

The Guidance is intentionally not prescriptive or at a granular level of detail on what or how a firm should determine or conduct scenario testing, to allow for a pragmatic application depending on the nature, scale and complexity of the firm's business. Having considered the feedback, the provision of direct examples and specific criteria

for scenario testing goes against the flexible nature of the guidelines. The expectation is that a firm should design a test plan appropriate to the individual firm.

The Central Bank does not expect all scenarios to be tested, but does expect firms to use their own judgment and consider scenarios that the individual firm deems severe but plausible for its business and that could potentially impact its critical or important business services. A firm that implements change more regularly should undertake more frequent testing. The Central Bank has considered the feedback received and intends to proceed with the proposal as set out in Guideline 10 in relation to scenario testing.

In respect of international firms with entities in multiple jurisdictions, there is an expectation that a local entity will have to determine its own critical or important business services, particularly in the context of the Irish economy. On a wider scale, local entities should understand how they feed into the delivery of group level critical or important business services. Local entities should take ownership of the components of the Operational Resilience Framework at a local level, including scenario testing.

There is an expectation that a firm's board should review the results of all scenario testing carried out on critical or important business services, particularly in relation to impact tolerances that have been breached, either during scenario testing or in the event of a real life disruption. The design and implementation of the remediation plans should be the responsibility of senior management and the results of the remediation plans should be reviewed and approved by the board thereafter. Having considered the feedback received, additional context has been added to Guideline 10 to reflect this.

Pillar 2

Business Continuity Management & Incident Management

Guideline 11 sets out the Central Bank's expectations regarding the integration of Business Continuity Management (BCM) into the overarching Operational Resilience Framework.

Further, Guideline 12 sets out the Central Bank's expectations regarding the integration of the firm's Incident Management strategy into the overarching Operational Resilience Framework.

Feedback:

Respondents generally accepted that Business Continuity Management (BCM) and Incident Management should be aligned with the Operational Resilience Framework and did not identify any material unintended consequences that might arise from aligning BCM and Incident Management strategies with the overarching Operational Resilience Framework.

Clarification of terms

- Respondents requested further clarity on the expectations of small firms and sole traders who may not currently have BCM arrangements in place.
- Several respondents asked for further clarity on terms referenced in the Guidance, particularly, in regards to defining the phrases Disaster Recovery Planning, Incident Management, and Crisis Management. Respondents queried if Disaster Recovery Planning is the same as Business Continuity Planning (BCP).
- A number of respondents have requested that the guidelines include more detail concerning the relationship between Operational Resilience, BCM, Incident Management and Disaster Recovery Strategy development.

Central Bank Response:

As detailed in Guidelines 11 and 12, the Central Bank encourages all firms to develop and maintain a BCP and Incident Management process that outlines procedures and instructions a firm must follow in the event of a disruption. Firms are encouraged to use already established reporting lines.

In response to feedback requesting clarity on specific terms used within the guidelines, the Central Bank will not be providing standalone definitions in the

finalised Guidance. While these terms have generally consistent meaning across industries, there may be slight variations between sectors. It is therefore expected that BCM, Incident Management and Disaster Recovery processes should be managed in line with the relevant and appropriate industry standards and governing regulations.

BCM and Incident Management should be aligned with the Operational Resilience Framework. Alignment occurs through BCM planning and the identification of single points of failure within a process that could also affect the end-to-end delivery of a critical or important business service. When responding to an incident, the Incident Management plans should be leveraged to consider how a disruption could affect a firm's impact tolerance metrics in relation to critical or important business services. Firms should continuously improve their incident response and disaster recovery plans by incorporating the lessons learned from previous incidents.

Communication Plans

Guideline 13 sets out the Central Bank's expectation regarding internal and external communication plans and stakeholder maps, which should be implemented to communicate effectively during a disruption.

Feedback:

Respondents were supportive of the development of internal and external communication plans and stakeholder maps, which should be implemented in the event of a disruption.

- Respondents noted that some firms may already have clearly defined reporting lines in place, and agreed that a firm should be expected to inform relevant stakeholders in a timely manner and for most firms this will already be part of the process.
- Respondents suggested that given the unpredictability of disruptive events, firms would welcome confirmation from the Central Bank that communication plans should be developed at a high-level that can be built upon when a disruptive event occurs.

Central Bank Response:

The Central Bank expects a firm to develop communication plans and stakeholder maps at a level that is proportionate to the firm in terms of nature, scale and complexity. An individual firm should have both internal and external communication plans at a level of granularity the firm deems to be appropriate. Firms may already have communication plans in place as part of other processes and requirements, and the Central Bank expects firms to leverage from existing communications plans already established.

The Central Bank has considered the feedback received and intends to proceed with the proposal as set out in Guideline 13 in relation to communication plans.

Pillar 3

Lessons Learned & Continuous Improvements

Guideline 14 requires a firm to look inward and determine what it learned after a disruption to a critical or important business service and how it will adapt and respond to future events.

Guideline 15 requires a firm to promote an effective culture of learning and continuous improvement as operational resilience evolves. This will promote operational resilience as a fundamental element of any strategic decision taken by a firm.

Feedback:

Respondents supported the Central Bank's proposal regarding lessons learned exercises and promoting an effective culture of learning.

- Respondents requested additional guidance on the self-assessment documentation, what should be included and how it should be documented.
- Some respondents suggested that a lessons learned exercise should only be conducted after a material disruption rather than all disruptions.
- In relation to presenting the lessons learned exercises, redress measures and self-assessment documentation to the board upon completion, respondents noted that this is putting a time constraint on the presentation of management information (MI) to the board.

Central Bank Response:

A lessons learned exercise allows a firm to reflect on their approach to operational resilience and allows for a feedback loop that encourages improvement in how a firm prepares for and recovers from disruptions. The minimum considerations for the development of a lessons learned exercise are included in Guideline 14. The Central Bank has considered the feedback received and intends to proceed as proposed, with the addition of including "identified vulnerabilities", where possible, as part of a lessons learned exercise. The list has been provided to encourage firms to identify deficiencies but is a non-exhaustive list allowing for a flexible and proportionate approach to developing lessons learned exercises across sectors.

The Central Bank determines that any disruption to a critical or important business service warrants a documented lessons learned exercise due to the potential a

disruption could have on a firm and the wider economy. Any identified vulnerabilities should be reported to the board to inform its judgment on the firm's level of operational resilience.

The Central Bank notes that the board has ultimate responsibility for the operational resilience of a firm and should be aware of any vulnerabilities in the continuity of service. The board and senior management should have accurate and adequate oversight of resilience activity, trends and remediation measures, which allows them to make the business decisions regarding investments and risk exposure. A firm should provide formal operational resilience MI to its board on a regular basis and in the event of a disruption. The frequency and depth of the reports should be done in a proportionate manner.

Next Steps

Operational resilience will remain a key objective of the Central Bank going forward. In keeping with the Central Bank's strategic commitment of strengthening our ability to maintain the resilience of the financial system, 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.

The Central Bank will publish the finalised *Cross Industry Guidance on Operational Resilience* in conjunction with this Feedback Statement and intends to use this as the foundation for engagement with firms on the evolution of their operational resilience strategies.

The expectation is for firms to begin to design their Operational Resilience Frameworks in line with this cross industry guidance and to begin dialogue at board level around the current level of operational resilience maturity in their firm. The Central Bank will continue to engage with individual firms as part of its supervisory engagement to assess firms' progress in implementing the requirements of this Guidance.

T: +353 (0)1 224 6000
E: OpResilience@centralbank.ie
www.centralbank.ie

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem