Matheson

November 2022

Operational Resilience Toolkit

CONTENTS Page No

1 Introduction

The financial services industry has experienced several unexpected and disruptive events in recent years, namely: technology failures; the COVID-19 pandemic; and natural disasters, among others. The industry is also operating in an increasingly complex and interconnected environment, where many firms now rely on outsourced services providers ("**OSPs**") inside and outside of Ireland to support their operations.

This increased dependence on multiple service providers, coupled with an accelerated increase in technology use has led to a rise in operational incidents and disruptions across all sectors of the industry.

While risk management processes and governance arrangements focus on preventing the occurrence of disruptive events, the concept of operational resilience focusses on an acceptance that certain incidents are unpreventable. Operational resilience encourages firms to be cognisant of possible points of failure and to prepare for how to react when such a disruption does occur.

In light of this, the Central Bank of Ireland (the "**Central Bank**") published the Cross-Industry Guidance on Operational Resilience in December 2021 (the "**Guidance**").[1] The objective of the Guidance is to advise financial services providers (referred to in the Guidance as "firms") on how to prepare for, respond to, recover and learn from an operational disruption that affects the delivery of critical or important business services.

At an EU level, the Digital Operational Resilience Act ("**DORA**") is aiming to harmonise digital resilience frameworks to ensure firms can adapt to ICT related disruptions. DORA sets out a number of objectives intended to strengthen firms' operational and digital resilience in light of increased cyber threats.

We hope you find the Matheson Operational Resilience Toolkit useful and that it becomes your go to resource for Operational Resilience going forward. We recommend that this Operational Resilience Toolkit be reviewed by firms alongside our earlier Outsourcing Toolkit (available here).

Should you have any queries in respect of the materials included in the Matheson Operational Resilience Toolkit, please do not hesitate to contact your usual Matheson contact, or one of the contacts listed below.

1. https://www.centralbank.ie/publication/consultation-papers/consultation-paper-detail/cp140---cross-industry-guidance-on-operational-resilience

Contacts

Darren Maher
Partner | Head of Financial Institutions Group
T +353 1 232 2398
E darren.maher@matheson.com

Gráinne Callanan
Partner | Financial Institutions Group
T +353 1 232 8211
E grainne.callanan@matheson.com

Caroline Kearns
Partner | Financial Istitutions Group
T +353 1 232 2421
E caroline.kearns@matheson.com

Elaine Long
Partner | Financial Institutions Group
T +353 1 232 2694
E elaine.long@matheson.com

Dualta Counihan
Partner | Asset Management and Investment Funds Group
T +353 1 232 2451
E dualta.counihan@matheson.com

Philip Lovegrove
Partner | Asset Management Investment Funds Group
T +353 1 232 2538
E philip.lovegrove@matheson.com

Barry O'Connor
Partner | Asset Management and Investment Funds Group
T +353 1 232 2488
E barry.oconnor@matheson.com

Claire Scannell
Professional Support Lawyer
T +353 1 232 2759
E claire.scannell@matheson.com

Joe Beashel
Partner | Financial Institutions Group
T +353 1 232 2101
E joe.beashel@matheson.com

Niamh Mulholland
Partner | Financial Institutions Group
T +353 1 232 2061
E niamh.mulholland@matheson.com

Louise Dobbyn
Partner | Financial Institutions Group
T +353 1 232 2094
E louise.dobbyn@matheson.com

Tara Doyle
Partner | Head of Asset Management and Investment Funds Group
T +353 1 232 2221
E tara.doyle@matheson.com

Shay Lydon
Partner | Asset Management and Investment Funds Group
T +353 1 232 2735
E shay.lydon@matheson.com

Michelle Ridge
Partner | Asset Management and Investment Funds Group
T +353 1 232 2758
E michelle.ridge@matheson.com

Karen Reynolds
Partner | Commercial Litigation and Dispute Resolution Department
T +353 1 232 2759
E karen.reynolds@matheson.com

Should you require further information in relation to the material contained in this Toolkit, please get in touch with a member of the team at the contact information above or your usual Matheson contact. Full details of Matheson's Financial Institutions group together with further updates, articles and briefing notes written by members of these teams, can be accessed at www.matheson.com

2 Central Bank Perspective

The Guidance defines Operational Resilience as:

> "*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.*"

The overarching principle of operational resilience is the acceptance that disruptions will occur and that firms should be prepared to respond accordingly. An operationally resilient firm is one that can recover critical or important business services from a significant and unplanned disruption, with minimal impact to customers and the integrity of the financial system.

To meet this standard, the Guidance has set out 15 guidelines under three pillars, which aim to provide firms with a holistic roadmap for ensuring they are operationally resilient.

2.1 Scope

The Guidance applies to all regulated financial service providers, ie, all persons who carry on a business of providing one or more financial services in Ireland.[2]

2.2 Deadline and Ultimate Responsibility for Implementation

The board and senior management of firms hold the ultimate responsibility for reviewing the Guidance and adopting appropriate measures to improve firms' operational resilience frameworks.

The Central Bank expects firms to implement this guidance within two years of the Guidance issuing, ie, by **December 2023**.

2 Section 2 of the Central Bank Act 1942.

3 Applicable Legal / Regulatory Requirements

While primary legislation imposes obligations on firms regarding operational resilience, the guidelines issued by regulators are generally more prescriptive on the steps they should take to ensure they are in compliance with their operational resilience obligations. However, the Central Bank states that its operational resilience Guidance is "*intentionally not prescriptive*", in order to allow firms to apply the Guidance in a manner proportionate to the nature, scale and complexity of their business.

In light of this, this Toolkit serves as a roadmap which allows firms to identify how the Guidance applies to their business and the practical steps they can take to comply with it.

The Central Bank advises firms to read the Guidance in conjunction with the relevant legislation, regulations, and other guidance or standards issued by the relevant industry bodies and supervisory authorities. Accordingly, we have collated certain legislation and guidance relevant to specific firms listed below, and provide links to relevant sources for ease of reference.

GUIDANCE FOR FIRMS
European and Irish legislation
▪ European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 – Irish implementation of the EU Directive on Security of Network and Information Systems ("**NIS2**")
International Standards for Operational Resilience
▪ Basel Committee on Banking Supervision's Principles for Operational Resilience ▪ Bank of England, Prudential Regulatory Authority and Financial Conduct Authority Joint Policy Statement on Operational Resilience across the Financial Services Sector
Central Bank Guidance
▪ Central Bank Cross Industry Supervisory Expectations in relation to Outsourcing Governance Arrangements, Risk Management Controls and Business Continuity Practice 2018 ▪ Central Bank Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks 2016
Incoming EU Regulations
▪ Proposed Digital Operational Resilience Act ("DORA")
Other
▪ Financial Stability Principles for an Effective Risk Appetite Framework 2013 ▪ Central Bank Consumer Protection Code 2012

4 Checklists

The checklists below set out the minimum expectations of the Central Bank during and after an operational disruption (the "**Checklists**").

The Checklists correspond with the Central Bank's Three Pillar Structure. These Checklists take firms through the full cycle of operational resilience, from identifying critical or important services and their vulnerabilities, to testing and implementing procedures, to reflecting on lessons learned from the occurrence of a disruption.

Pillar 1: Identify and Prepare [Preparing for inevitable disruptions]

i) Governance (Guidelines 1 and 2);

ii) Identification of Critical or Important Business Services (Guidelines 3 and 4);

iii) Impact Tolerances (Guidelines 5 and 6);

iv) Mapping of Interconnections and Interdependencies (Guidelines 7 and 8);

v) ICT and Cyber Resilience (Guideline 9);

vi) Scenario Testing (Guideline 10);

Pillar 2: Respond and Adapt [Responses during a disruption]

vii) Business Continuity Management (Guideline 11);

viii) Incident Management (Guideline 12);

ix) Communication Plans (Guideline 13); and

Pillar 3: Recover and Learn [Learning from disruptions]

x) Lessons Learned Exercise and Continuous Improvement (Guidelines 14 and 15).

Operational Resilience Checklists

1 Governance

No	Requirement	Guidance	✓
Guideline 1: The board has ultimate responsibility for the operational resilience of a firm. To meet this standard, the board and firms can take the following steps:			
1.	**Ultimate Responsibility - Board**	A firm's board has ultimate responsibility for the approval and oversight of the firm's Operational Resilience and Operational Resilience Framework ("**ORF**"). This includes responsibility for: ▪ creating a uniform operational resilience process; ▪ prioritising activities that improve operational resilience; and ▪ targeting investments towards making important or critical business services more resilient.	☐
2.	**Board Responsibility - Oversight and Governance**	The Central Bank expects all board members to have a sufficient understanding of the firm's ORF to be able to provide effective board oversight and scrutiny of the firm's operational resilience. In ensuring effective oversight, the board should: ▪ ensure senior management have the financial, technical and other resources needed to support the firm's overall operational resilience; ▪ oversee senior management assessment of the ORF; and ▪ prioritise actions for improving operational resilience according to factors such as potential impact of disruptions, time criticality, and progress required to be able to remain within impact tolerances. It is essential that all board members have a sufficient understanding of the ORF, rather than being satisfied that the board as a whole has sufficient knowledge.	☐
3.	**Board Responsibility – Approvals**	The board is responsible for approving and reviewing: ▪ the ORF; ▪ 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.	☐
4.	**Annual Review**	The board should review the ORF at least annually to confirm there are no undetected developing weaknesses.	☐
5.	**Board Responsibility – Post-Disruption Review**	After a disruption occurs, the board should review, challenge and approve assessments of the firm's: ▪ critical or important business services; ▪ impact tolerances; ▪ business service maps; and ▪ scenario analysis.	☐

6.	**Trend Knowledge**	▪ Ensure board and senior management have accurate, adequate oversight of resilience activity, trends and remediation measures.	☐
7.	**Information Management**	Senior management should: ▪ provide the board with formal operational resilience management information ("**MI**") on a regular basis and in the event of a disruption; ▪ embed MI into existing reporting structures; and ▪ establish escalation routes in the event of identifying a vulnerable area or the occurrence of an unexpected disruption.	☐

Guideline 2: The Operational Resilience Framework should be aligned with a firm's overall Governance and Risk Management Frameworks.
To achieve this, firms can take the following steps:

8.	**Existing Structures**	Firms must: ▪ utilise existing governance and risk management structures when implementing the ORF; and ▪ include operational resilience related responsibilities in existing governance frameworks and committee structures, if not already present.	☐
9.	**Holistic Approach**	Firms must: ▪ develop a documented ORF aligned with the firm's Operational Risk and Business Continuity Frameworks (see Checklist 7); or ▪ incorporate these risk areas into one holistic framework.	☐
10.	**Senior Management Responsibility**	Senior management are responsible for implementing operational resilience across the firm and throughout its operations, risk and finance pillars, with particular regard for: ▪ business continuity; ▪ third party risk management; ▪ ICT and cyber risk management; ▪ incident management; and ▪ any wider aspects of operational risk management applicable to the firm.	☐

2. Identification of Critical or Important Business Service

The Guidance defines a critical or important business service as 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.

No	Requirement	Guidance	✓
Guideline 3: The board reviews and approves the criteria for critical or important business services. To achieve this, firms can take the following steps:			
1.	**Role of criteria**	Before identifying the firm's critical or important business services, set the criteria regarding: ▪ what constitutes a critical or important business service for the firm; and ▪ where there is more than one, the priority ranking of the firm's critical or important business services.	☐
2.	**Selecting Criteria**	Consider the risk a disruption poses to: ▪ customers; ▪ firm viability, safety and soundness; and ▪ overall financial stability.	☐
3.	**Board Responsibilities**	The board is responsible for: ▪ approving clearly defined and documented criteria for classifying business services critical or important; and ▪ reviewing identification criteria annually or at the time of implementing material changes to the business, where change involves additional critical or important business services.	☐
Guideline 4: A firm should identify its critical or important business services. To achieve this, the board, senior management and firms can take the following steps:			
4.	**Ultimate Board Responsibility - Review**	The board must be designated with responsibility for reviewing and approving all business services classified as critical or important on at least an annual basis.	☐
5.	**Applying the criteria**	Once the firm sets the criteria, identify all the firm's critical or important business services. A firm can achieve this by: ▪ reviewing its operations as a complete end-to-end set of activities required to deliver a particular business service; ▪ leveraging its existing business functions' knowledge; and / or ▪ taking an outcomes based approach to identifying and prioritising services.	☐

6.	**Result of Identification**	Following identification, the firm should be able to: ▪ clearly determine impact tolerances based on maximum acceptable levels of disruption; ▪ perform mapping of the end-to-end delivery of the business service, including any dependence on third parties; and ▪ test based on severe but plausible scenarios.	☐
7.	**Risk Ratio**	Consider whether the number of critical or important business services identified is proportionate to the nature, scale and complexity of the firm's business.	☐

3. Impact Tolerances

An impact tolerance determines the maximum acceptable level of disruption to a critical or important business service, helping a firm to understand its level of operational resilience in the event of an unplanned disruption.

No	Requirement	Guidance	✓
Guideline 5: Impact tolerances should be approved for each critical or important business service. To achieve this, firms can take the following steps:			
1.	**Assume Disruption**	Develop impact tolerances for each critical or important business service on the assumption that disruptive events will happen	☐
2.	**Using Impact Tolerances**	Set impact tolerances at the point at which disruption to the firm's business service would pose, or have the potential to pose, a risk to the firm's viability, safety and soundness, to financial stability or could cause material detriment to customers.	☐
		Use impact tolerances as a planning tool for a firm rather than as a tool to measure regulatory compliance. They can be used to determine the schedule by which a firm should be able to restore the delivery of critical or important business service after a disruption occurs.	☐
3.	**Testing**	Test impact tolerances against severe but plausible scenarios to determine their appropriateness.	☐
		A key consideration is whether the firm is able to stay within the defined impact tolerances during a disruption.	☐
4.	**Board Responsibility - Review**	Review and approve impact tolerances at least annually or when a disruption occurs. Focus the review on determining if the original approved impact tolerances are still fit for purpose.	☐
5.	**Align to Risk Appetite**	Align to firm's risk appetite, but be mindful that impact tolerances remain a separate and distinct tolerance measurements to risk appetite.[3]	☐
6.	**Use of Pre-Existing Resources**	Leverage any appropriate pre-determined and approved criteria as part of other practices for use in impact tolerance testing. This may include processes used for: ▪ Business Impact Analysis; ▪ Recovery Time Objectives; ▪ Recovery Point Objectives; and ▪ Maximum Tolerable Outage, where these metrics that measure disruption of single points of failure feed into the delivery of a critical business service	☐

3 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.

Guideline 6: A firm should develop clear impact tolerance metrics To achieve this, firms can take the following steps:			
7.	**Criteria**	Impact tolerance metrics: ▪ need to be clear and measurable; ▪ should reference specific outcomes and measurements; ▪ can be qualitative and quantitative; ▪ should allow the firm to determine the outcome if the impact tolerances are exceeded; and ▪ should focus the firm's response to a disruption on the continuity of critical or important business services.	☐
8.	**Minimum requirements**	Have a time-based metric at a minimum. A time-based metric indicates the maximum acceptable duration a critical or important business service can withstand a disruption.	☐
9.	**Additional metrics**	To be prepared to withstand more than one type of disruption, firms should consider having additional impact tolerance metrics, such as: ▪ the maximum tolerable number of customers effected by a disruption; ▪ the maximum number of transactions affected by a disruption; or ▪ the maximum value of transactions impacted.	☐
10.	**Business specific metrics**	Set and approve additional impact tolerance metrics based on the firm's specific critical or important business services and the firm's nature, scale and complexity.	☐

4. Mapping of Interconnections and Interdependencies

No	Requirement	Guidance	✓
Guideline 7: A firm should understand and map out how its critical or important business services are delivered. To achieve this, firms can take the following steps			
1.	**Mapping Exercise**	List the firms' critical or important business services as identified from Checklist 2.	☐
		Identify and document the following that are necessary for the delivery of each service: ▪ people; ▪ processes; ▪ information; ▪ technology; ▪ facilities; and ▪ third party service providers and OSPs necessary for the delivery of the service	☐
		Map each stage of the service and note for each stage which services contribute to its delivery.	☐
		Identify which stage each service contributes to the delivery of.	☐
		Rank the order of priority of the services identified.	☐
2.	**Questions to consider during the exercise**	▪ How are the services delivered? How do they work together to deliver the service? ▪ How can each service be disrupted? Are there any single points of failure, any dependencies, any vulnerabilities? ▪ Which business units own which resource? ▪ From where is each service provided? Having answered the above questions, firms should be in a position to identify where recovery and resolution plans can be leveraged.	☐
3.	**Collaborative Approach**	To ensure comprehensive mapping, undertake the mapping exercise collaboratively across the firm. At least one representative of each relevant department in the firm should contribute to the questions in Action 2 above. Relevant departments or representatives may include: ▪ ICT and Security; ▪ Risk; ▪ Liaisons with OSPs; and ▪ Departments involved in the delivery of critical or important business services for the firm.	☐

Guideline 8: A firm should capture third party dependencies in the mapping of critical or important business services To achieve this, firms can take the following steps:			
4.	**Board and Senior Management Responsibility – Third Party Risk**	Boards and senior management are responsible for: ▪ managing relationships with external service providers; and ▪ recognising that when entering an outsourcing arrangement, they are creating a dependency on a third party for firm resilience.	☐
5.	**Mapping Exercise**	Clearly identify and detail any dependencies in the mapping exercise for Guideline 7.	☐
6.	**Due Diligence**	Prior to entering into an outsourcing arrangement, undertake due diligence in respect of the potential OSP.[4]	☐
7.	**Due Diligence – Key Considerations**	Will the third party's resilience conditions enable the firm to remain within its impact tolerances? Will the geographical location of the third party impact on the provision of services in the event of a disruption?	☐
8.	**Third Party Agreements**	Where arrangements with third parties exist, in addition to ensuring that the arrangements are in compliance with the Central Bank's Cross-Industry Guidance on Outsourcing, the agreements should detail: ▪ how critical or important services will be maintained during a disruption; ▪ the exit strategy where / if the service cannot be maintained; and ▪ any geographical or service specific provisions.	☐

4 For further practical steps here, see the Matheson Outsourcing Toolkit.

5. ICT and Cyber Resilience

No	Requirement	Guidance	✓
Guideline 9: A firm should have ICT and Cyber Resilience strategies that are integral to the operational resilience of its critical or important business services. To achieve this, firms can take the following steps:			
1.	**Standard**	A firm is responsible for ensuring its information and communication technology is: ▪ robust and resilient; and ▪ subject to protection, detection, response and recovery programmes in line with industry best practice.	☐
2.	**Mapping**	Identify where technology is part of the delivery of a critical or important business service.	☐
3.	**Third Parties**	Where IT systems or technology resources are provided by a third party, take the necessary steps outlined in Checklist 4.	☐
4.	**Testing**	Test the identified systems regularly as part of IT security, cyber-security and resilience testing, using severe but plausible scenarios. Focus testing on ensuring the continuity of critical or important business services during severe disruptions.	☐
5.	**Ongoing Intelligence**	Develop on-going threat intelligence and situational awareness programmes within the firm to: ▪ feed into the operational resilience programme; and ▪ align with the firm's IT risk management, IT security management, IT incident management and IT continuity/disaster recovery programmes.	☐
6.	**Alignment with Other Guidance**	Read this Guideline in conjunction with: ▪ the Central Bank's 'Cross Industry Guidance in respect of Technology and Cybersecurity Risks; ▪ the EBA Guidelines for ICT and Security Risk Management; ▪ the EIOPA Guidelines for ICT Security and Governance; ▪ NIS2; and ▪ the forthcoming DORA.	☐

6. Scenario Testing

No	Requirement	Guidance	✓
Guideline 10: A firm should document and test its ability to remain within impact tolerances through severe but plausible scenarios To achieve this, firms can take the following steps:			
1.	**Scope**	Test the firm's ability to remain within its impact tolerances for every critical or important business service identified in Checklist 2.	☐
2.	**Carrying out testing**	Identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to the firm's business and risk profile.	☐
		Use data from mapping exercises in Guidelines 7 and 8 to identify the firm's individual idiosyncratic risks and develop more appropriate testing.	☐
		Consider various testing methods such as paper based or simulation testing on a number of critical or important business services.	☐
3.	**Frequency**	Complete scenario testing at least annually. Frequency of testing should be proportionate to firm size and complexity. A firm that implements change more regularly should undertake more frequent testing.	☐
4.	**Testing Results**	A scenario test will identify any vulnerabilities or reliance on third parties. These results should: ▪ focus investment in the resolvability of a vulnerable element; ▪ determine alternative channels of delivery; and ▪ 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 is possible; ▪ staff need appropriate training; and ▪ outsourcing arrangements need to be reviewed.	☐
5.	**Lessons Learned Exercise**	Provide the Central Bank with greater assurance that the firm has adequate contingency plans in place for operational disruption by: ▪ designing a test plan; ▪ documenting the scope of the exercise, the steps taken or considered during the exercise; and ▪ capturing and acting upon the lessons learned from the exercise.	☐

6.	**Board Responsibility – Response to Testing Results**	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, the board and senior management are responsible for taking action to improve the resilience of the business service and focusing investment where needed.	☐
7	**Senior Management Responsibility – Remediation Plans**	Senior management are responsible for executing the design and implementation of any remediation plans.	☐
8	**Board Responsibility – Review and Approval of Remediation Plans**	The board should review and approve the results of any remediation plans following their design and implementation by senior management.	☐

7. Business Continuity Management

No	Requirement	Guidance	✓
Guideline 11: Business Continuity Management ("BCM") should be fully integrated into the overarching ORF and linked to a firm's risk appetite. To achieve this, firms can take the following steps:			
1.	**Existing Resources**	Utilise already approved business continuity plans ("**BCPs**") as part of the holistic response to a disruption.	☐
2.	**BCM as distinct from OR**	Be mindful that 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.	☐
3.	**Alignment with ORF**	Align BCM with the ORF by: ▪ testing the pre-approved BCPs through severe but plausible scenarios. Include any third party interdependencies or interconnections in these tests; ▪ mapping critical or important business services per Guidelines 7 and 8; and ▪ developing a recovery plan in line with approved impact tolerances.	☐
4.	**On Disruption of a Critical or Important Business Service**	Enact BCP as part of response process.	☐
		Develop the integrated BCP to incorporate: ▪ invocation processes; ▪ impact analyses; ▪ recovery strategies; ▪ training programmes; and ▪ crisis management.	☐
		Ensure the BCP can guide management through a disruption and limit its impact.	☐
5.	**Staff Preparedness**	Identify key personnel and ensure they complete any necessary training for executing contingency plans.	☐
		Customise training and awareness programmes based on specific roles.	☐
		Ensure all staff are aware of contingency plans and their role in effectively executing them to respond to a disruption.	☐
6.	**Third party interdependency**	Where interdependencies on third parties for the delivery of critical or important business services have been identified: ▪ verify that these arrangements have appropriate operational resilience conditions to ensure the firm can remain within its impact tolerances; ▪ review and test the arrangements at least annually; and ▪ consider identifying the dependencies that can be substituted in the event of an unexpected disruption.	☐

8. Incident Management

No	Requirement	Guidance	✓
Guideline 12: The Incident Management Strategy should be fully integrated into the overarching Operational Resilience Framework To achieve this, firms can take the following steps:			
1.	**Scope**	A firm's incident management strategy should: ▪ cover the full life cycle of an event, from classification to testing to reflecting on lessons learned; and ▪ manage all incidents impacting or potentially impacting the firm.	☐
2.	**Potential incidents**	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.	☐
3.	**Incident response**	When responding to an incident, develop the incident management plans so they consider how a disruption can affect a firm's risk appetite and impact tolerance metrics.	☐
4.	**Inventory**	Maintain an inventory to support the firm's response and recovery capabilities that includes: ▪ incident response and recovery steps followed during a disruption; ▪ internal and third party resources potentially impacted; and ▪ communication plans followed.	☐
5.	**Procedure Review - Frequency**	Review, test and update incident response and recovery procedures at least annually.	☐
6.	**Root Causes**	Identify and manage the root causes of specific incidents to prevent their serial recurrence.	☐
7.	**Lessons Learned**	When updating the incident management program reflect on lessons learned from previous incidents, including incidents experienced by OSPs or other firms. Consider learnings from incidents as part of scenario testing.	☐

9. Communication Plans

No	Requirement	Guidance	✓
Guideline 13: Internal and External Crisis Communication plans should be fully integrated into the overarching ORF To achieve this, firms can take the following steps:			
1.	**Holistic Approach**	Develop the firm's crisis communication plan either as part of: ▪ the ORF; or ▪ the BCM / recovery plans.	☐
2.	**Key Resources and Experts**	Identify and prepare the key resources and experts that can be leveraged when a disruption occurs, in order to mitigate the harm caused during a disruption.	☐
3.	**Resources to implement during a disruption**	Key resources during a disruption should include: ▪ internal communication plans; ▪ external communication plans; and ▪ stakeholder maps.	☐
4.	**Content of internal communication plan**	Include escalation routes on how to communicate with: ▪ key-decision makers; ▪ operational staff; and ▪ third parties and OSPs, if necessary.	☐
5.	**Content of external communication plan**	Outline how the firm will communicate with the following parties during a disruption: ▪ customers; ▪ stakeholders; and ▪ regulators.	☐

10. Lessons Learned Exercise and Continuous Improvement

No	Requirement	Guidance	✓
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. To achieve this, firms can take the following steps:			
1.	**Frequency**	Conduct a lessons learned exercise after any disruption to a critical or important business service, including any potential material disruption to a third party provider that feeds into the delivery of a critical or important business service.	☐
2.	**Lessons Learned - Objectives**	Utilise the information gathered as part of the incident management or disaster recovery process.	☐
		Reflect on the three-pillar approach to operational resilience.	☐
		Use the information gathered to create a feedback loop into the first two pillars that encourages improvement in how a firm prepares for and recovers from disruptions.	☐
3.	**Basis**	The decisions and recovery processes determined to be appropriate throughout the incident management process should form the basis of the lessons learned exercise. Establish 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.	☐
4.	**Conclusions and Remedies**	Define effective remediation measures to redress deficiencies and failure in the continuity of service. Agree on remedial actions. Adjust any impact tolerances if determined.	☐
5.	**Self-Assessment Document**	Collate the information in the steps above within a self-assessment document.	☐
		Present the documents and its findings to the board at least annually.	☐

Guideline 15: A firm should promote an effective culture of learning and continuous improvement as operational resilience evolves. To achieve this, firms can take the following steps:			
6.	**Continuous improvements**	Incorporate learning from the exercises in Guideline 14 into the firm's ongoing operational governance discussions.	☐
7.	**Learning Culture**	Promote an effective culture of learning and continuous improvement as operational resilience evolves.	☐
8.	**Strategy decisions**	Consider any changes to strategy or the business model considered through a business service lens.	☐
		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.	☐
9.	**Self-assessment - Content**	Document and update written self-assessments highlighting how the firm meets current operational resilience policy requirements. These reviews should: ▪ cover all aspects of the three pillars of operational resilience; and ▪ ensure no emerging vulnerabilities are overlooked; ▪ detail the rationale for determining all criteria from Pillar 1; and ▪ determine whether the firm's current practices meet regulatory guidelines.	☐
10.	**Frequency**	Carry out and document these self-assessment exercises at least annually.	☐

Matheson

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Renrose Dock,
Cork, T23KW81

T: +353 21 465 8200
E: cork@matheson.com

LONDON
1 Love Lane
London EC2N 7JN
England

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
200 Park Avenue
New York, NY 10166
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
530 Lytton Avenue
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
156 2nd Street
San Francisco CA 94105
United States

T: +1 650 617 3351
E: sf@matheson.com