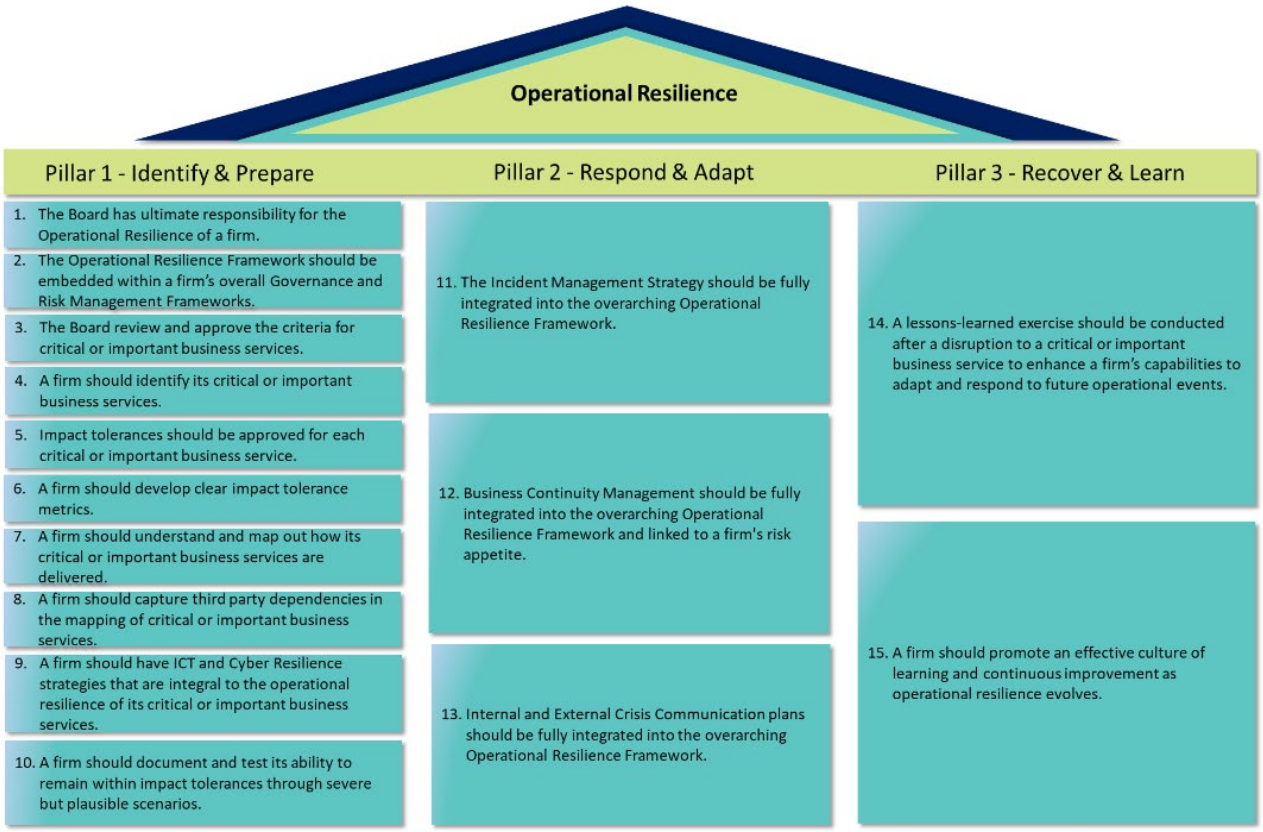
CP-140 Cross Industry Guidance on Operational Resilience

Central Bank of Ireland, December 2021 released a Consultation Paper, CP140 on Operational Resilience for Financial Institutions.

This guidance paper comments to the preparedness of financial institutions to continued operations with regard to events that may occur that impact on its continuing operations and or ability to deliver member services.

“The objective of this guidance is to communicate to industry how to prepare for, respond to, recover and learn from an operational disruption that affects the delivery of critical or important business services.”

Operational risk management is focused on minimising risk, through development of controls that reduce the impact and probability of an operational event occurring. 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 - to remain a viable ongoing concern, absorb shocks rather that contribute to them, to recover and adapt when disruptions occur.



Consultation on Cross Industry Guidance on Operational Resilience

Central Bank of Ireland

Operational Resilience Framework Governance Model:

An Operational Resilience Framework Governance Model is a structured and systematic framework that establishes the principles, policies, roles, and processes for overseeing and managing operational resilience within an organisation.

The model encompasses the entire lifecycle of operational resilience, including risk assessment, business impact analysis, incident response, and continuous improvement. The governance model ensures alignment with organisational objectives, regulatory requirements, and industry best practices.

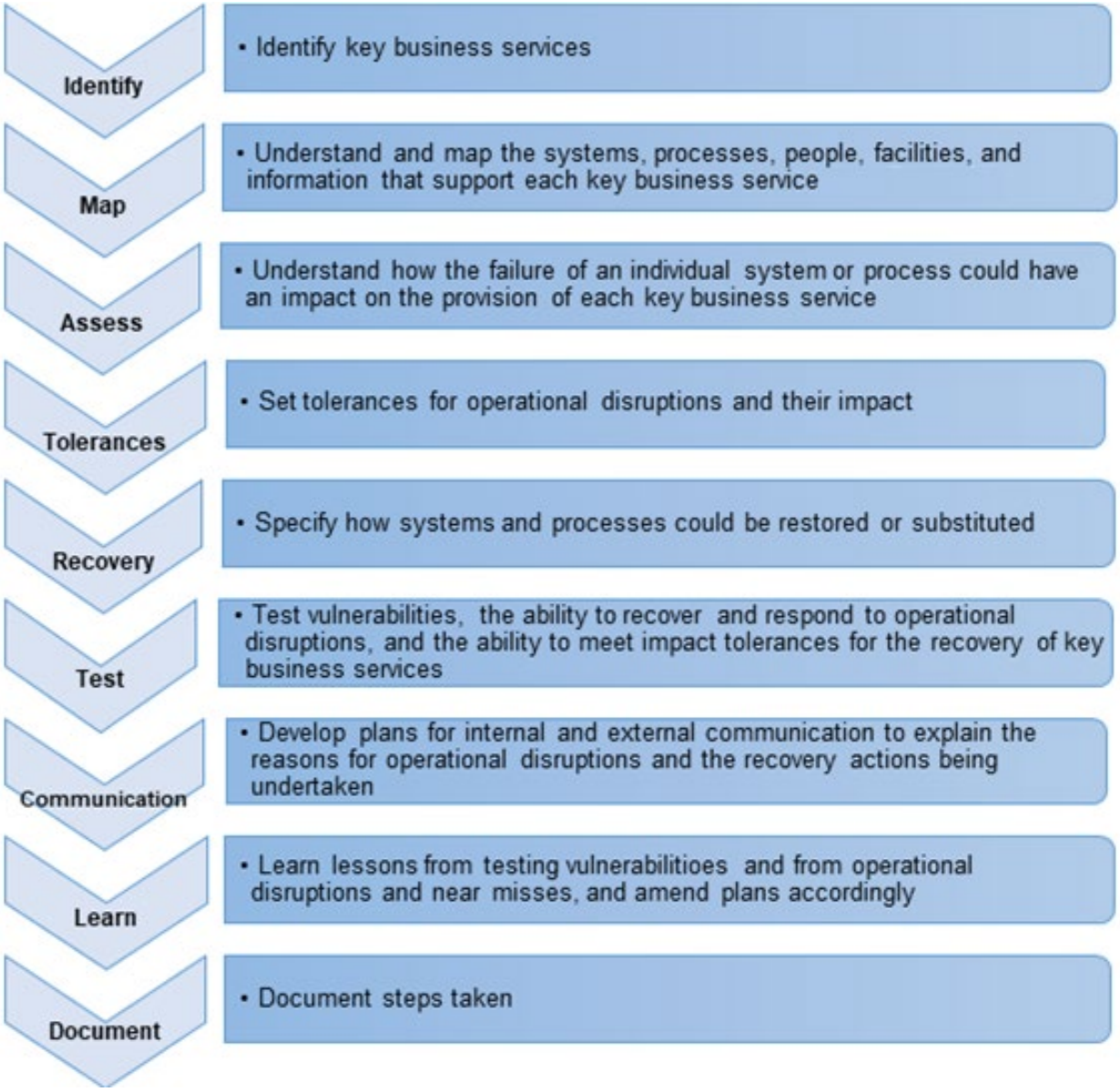


Table B - Operational Resilience Framework Process

Core Principles for Building an Operational Resilience Framework:

Identify Critical Business Services:

- Determine which services are critical or important for your organisation.
- Look beyond organisational structure and focus on activities that deliver specific outcomes to end users (e.g., loan processing, fund transfers).

Set Impact Tolerances:

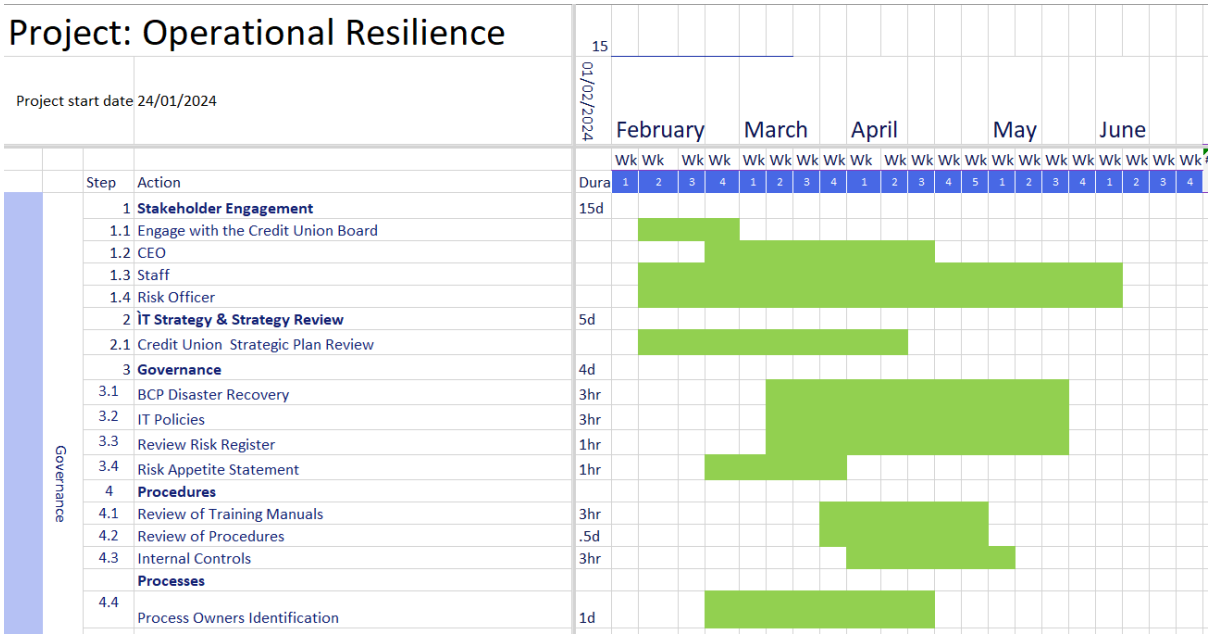
- Define acceptable levels of impact for each critical service.
- Understand how much disruption your organisation can tolerate without severe consequences.

Map Resource Interdependencies and Connectivity:

- Identify dependencies between resources (people, technology, data, facilities, suppliers).
- Understand how disruptions in one area affect others.

Scenario Testing:

- Conduct scenario-based tests to assess your organisation's response to operational disruptions.
- Test your ability to recover critical services and learn from the experience.



Project Plan for Operational Resilience

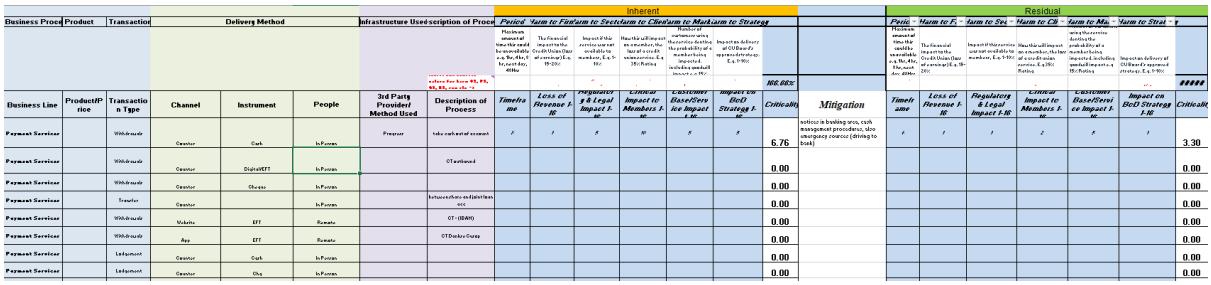
CP-140 Cross Industry Guidance on Operational Resilience Framework Document Register

Step 1	Identify and Prepare- **Action**	**Identified Document**
Governance	The Operational Resilience Framework should be aligned with a firm's overall Governance and Risk Management Frameworks	Risk Register Policies Engagement with staff, BOD and key stake holders Development & agreement of this process
Identification of Critical or Important Business Service	A firm should identify its critical or important business services.	Process Owners Information document Review of Training Manuals Progress Training/Release Documentation
Impact Tolerances	Impact tolerances should be approved for each critical or important business service.	Business Impact Assessment document
Impact Tolerances	A firm should develop clear impact tolerance metrics	Business Impact Assessment document
Mapping of Interconnections and Interdependencies	A firm should understand and map out how its critical or important business services are delivered.	Process Owners Information document
Outsourced Service Provider' Due Diligence	A firm should capture third party dependencies in the mapping of critical or important business services.	Due Diligence Outsourcing Reviews of OSP
ICT and Cyber Resilience	A firm should have ICT and Cyber Resilience strategies	BCP
Scenario Testing	A firm should document and test its ability to remain within impact tolerances through severe	Scenario testing

Steps Involved

Operational Resilience revolves understanding the key process of the organisation. This journey starts at determining your Business Process, impact to member services, organisation, market and duration that this process can be unavailable before it affects the member.

Our framework then reviews the major policies – Business Continuity Plan, IT Policies, Risk Appetite for the organisation.

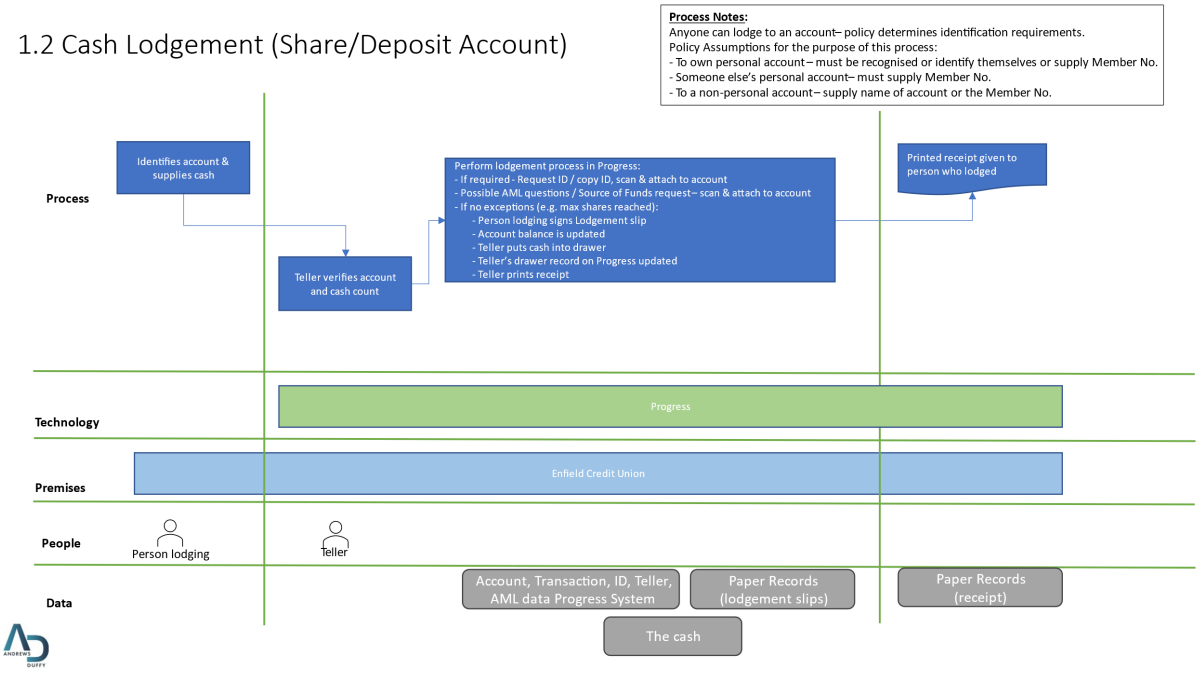


Business Impact Assessment Framework

	Description	Frequency	Board of Directors	Committee	Management	Sponsor	Risk Officer	Staff	Outsourced Service Providers
Pillar 1 Identify and Prepare	The Board reviews and approves the criteria for critical or important business services.	Yearly	(A)	(R)	(R)	(C)	(C)	(I)	
	Operational Resilience Framework aligned with a firm's overall Governance and Risk Management Frameworks	Yearly	(A)	(R)	(R)	(C)	(C)	(I)	
	The Board reviews and approves the criteria for critical or important business services	Yearly	(A)	(R)	(R)	(C)	(C)	(I)	(I)
	A firm should identify its critical or important business services.	Bi - Annual	(A)	(R)	(R)	(C)	(C)	(I)	(I)
	Impact tolerances should be approved for each critical or important business service.	Bi-Annual	(A)	(C)	(C)	(A)	(C)	(I)	(I)
	A firm should develop clear impact tolerance metrics.	Yearly	(A)	(R)	(R)	(C)	(C)	(I)	

	A firm should understand and map out how its critical or important business services are delivered.	Yearly, or as required	(A)	(R)	(R)	(C)			
	A firm should capture third party dependencies in the mapping of critical or important business services. Review 3rd Party SLA's	Yearly	(A)	(C)	(R)	(C)	(R)	(I)	(I)
	A firm should have ICT and Cyber Resilience strategies that are integral to the operational resilience of its critical or important business services.	Bi-Annual	(A)	(C)	(R)	(C)	(R)		
	A firm should document and test its ability to remain within impact tolerances through severe but plausible scenarios.	Scenario testing every quarter	(A)	(C)	(R)	(C)	(R)		

RACI Matrix for Operational Resilience



Process Map for Lodgement of a Member into their Credit Union account

Develop of Process maps to understand

- The internal process
- Technology involved to provide that service
- People involved
- Data involved (how it is processed)

Robust internal and external communication strategies to allow organisations to act quickly and effectively to reduce potential harm. The business continuity plan, as part of this document details the internal and external communication plans including Crisis Management.

Scenario	Communication Plan	
People Risk		
• Human Errors		
• Fraud / unethical behaviour		
• Talent Risk (key staff leaving)		
• Risk Culture		
Process Risk		
• Failure of internal business processes		
• Product design		
• Process failures		
• Resilience risk – failure to put resources into this framework		
System Risk (Technology)		
• Internal System failure/disruption		
• Connectivity		
• Information system failure		
• Backup systems		
• Technology Risks		

Communication Plan

5.1.5 Potential computer system recovery incident – premises not affected

✓	**Action**	
	A computer failure incident will be reported to the Manager/Emergency Planning Officer together with available known information.	
	The manager/computer administrator seeks advice from their IT supplier on cause, effect, actions required and options available.	
	If a Cyber Attack is suspected contact Insurance Provider	

	The IT Supplier prepares an outline operational recovery plan (verify last good backup tapes, time of this backup, work completed since last good backup, paper audit trails required to re-process work, establish downtime requirement (if any), management and resourcing of credit union operation during recovery process.	
	Manager identifies risks as a result of the incident and risks associated with the planned recovery approach	
	Manager/computer administrator to review plan with IT supplier and to establish what operational impacts will apply (if any)	
	Manager finalises approach and implements recovery plan (in conjunction with IT supplier and recovery team as appropriate)	
	IT supplier performs their duties as required and as agreed	
	Manager/computer administrator maintains regular contact with IT supplier until recovery process is complete and the credit union operation is stabilised	
	Manager directs and supervises credit union tasks to complete the recovery process (including any back-posting if necessary)	
	IT supplier performs necessary tests to validate recovery process is successful	
	Manager and designates perform appropriate user tests to validate the recovery process is successful	
	Manager/computer administrator sign-off that the recovery process is complete and successful and agree any necessary follow-up actions (including the planning and authorisation for preventative maintenance)	
	Complete the Recovery Progress Activity Log.	