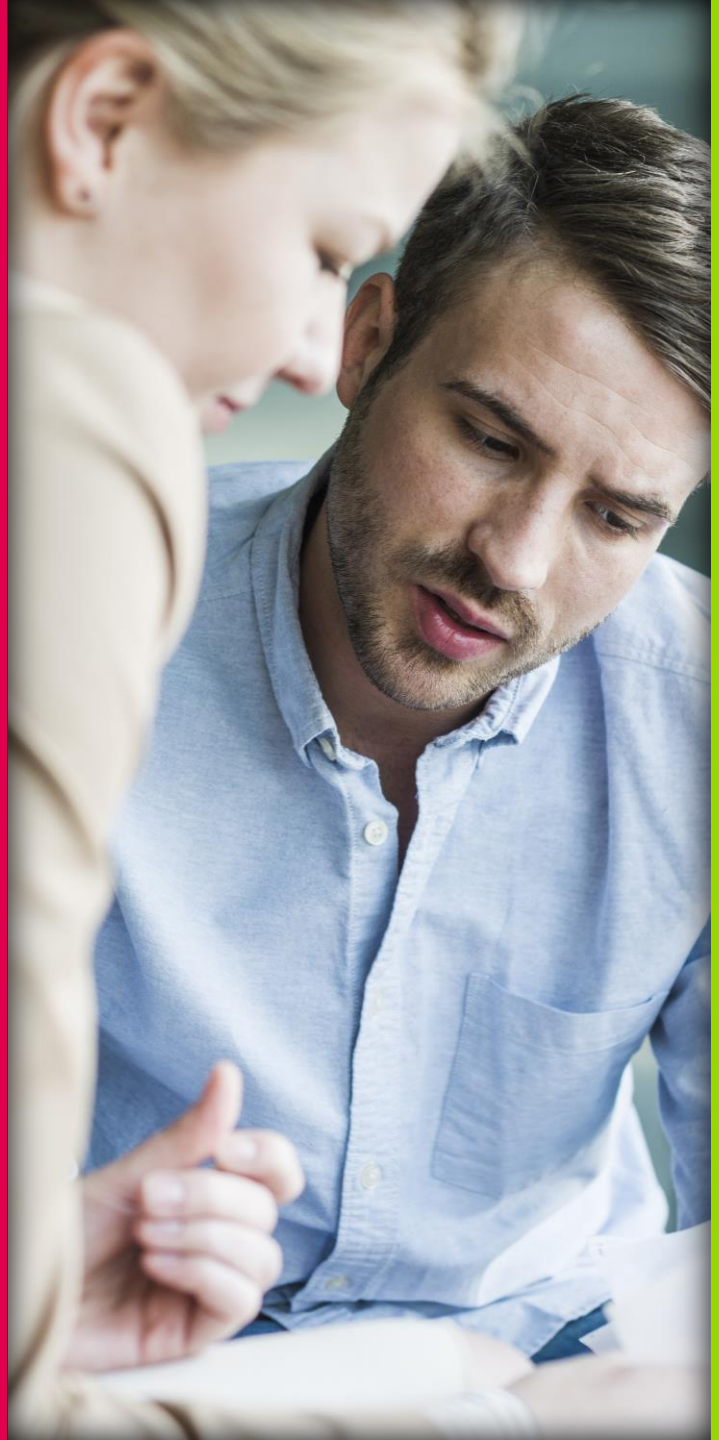
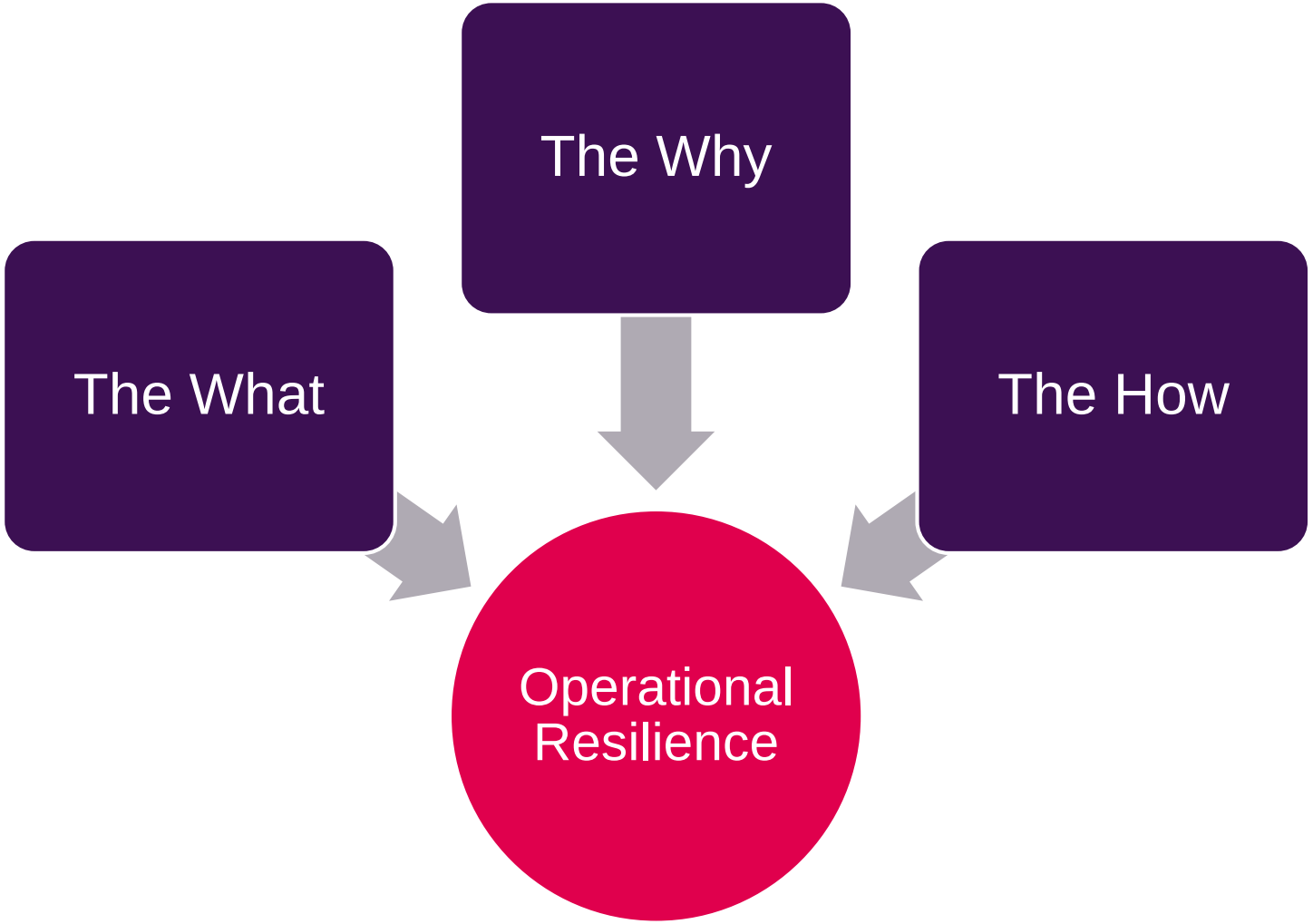
Developing an Operational Resilience Framework

MICHELLE O'DONOGHUE – DIRECTOR



We're by your side

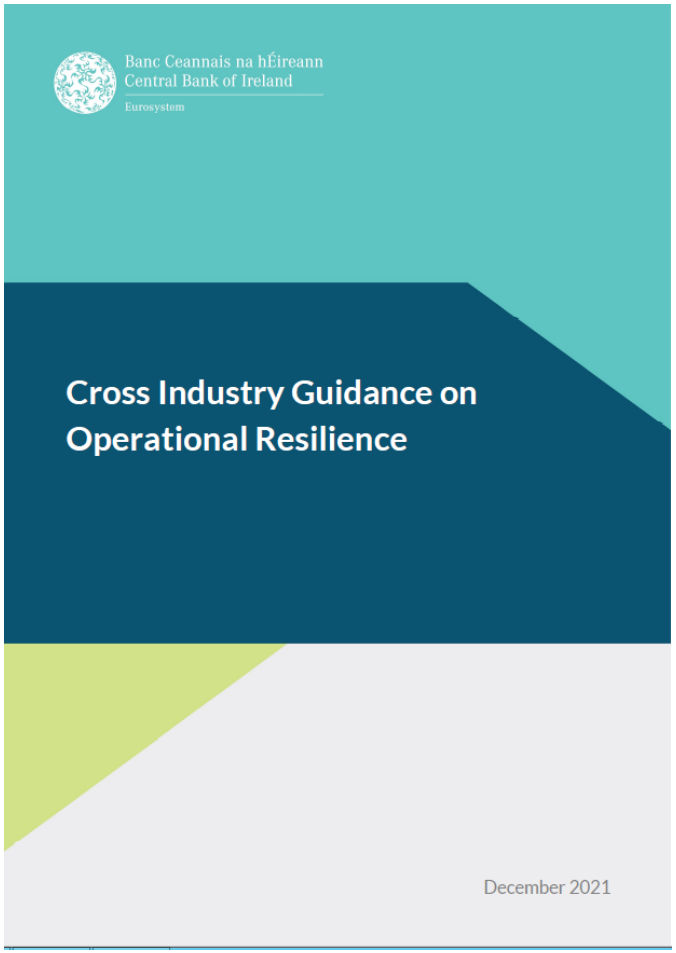
Agenda



Operational Resilience

Operational Resilience – The What

- Initially CP140 issued in April 2021
- Final guidance issued in December 2021
- Part of the CBI's strategy to continue to address vulnerabilities and weaknesses in the financial system so as to address future shocks/crisis



Operational Resilience – The What

The ability of a credit union (and the wider financial services sector) to identify, prepare, respond and adapt to, recover and learn from an operational disruption

Operational Resilience – The What

- Resilient organisations are capable of absorbing shocks – includes people, processes, technology and culture
- Needs clear governance oversight and input from the management team
- Is a multi-discipline approach involving all stakeholders and is becoming increasingly important following Covid-19

Operational Resilience – The What

- It is more holistic than traditional business continuity planning
- Traditional BCP = single point of failure
- Focus is on multi-point failures and how to respond to these
- Looks at putting a mechanism in place to respond to risks as they arise

Operational Resilience

Operational Resilience – Why?

"There are 4 steps to achievement – plan purposefully, prepare prayerfully, proceed positively, pursue persistently"

William A Ward

RBK

Operational Resilience – Why?

- Covid-19 has been hugely disruptive – what will be the next business disruptor?
- An increased reliance on IT means greater cyber exposure
- Credit Union members want digital – physical branches are less attractive to Gen Z's
- More credit unions are outsourcing – this brings its own challenges
- Operational resilience is becoming a strategic priority

Operational Resilience – Why?

- No business is immune to disruption – what resilience is trying to do is to move the dial
- Less of trying to prevent the disruption
- More of trying to respond to and learn from the disruption
- Proactive rather than reactive
- If Credit Unions (and the sector) can become more resilient, they can plan better and make more informed decisions

Operational Resilience – Why?

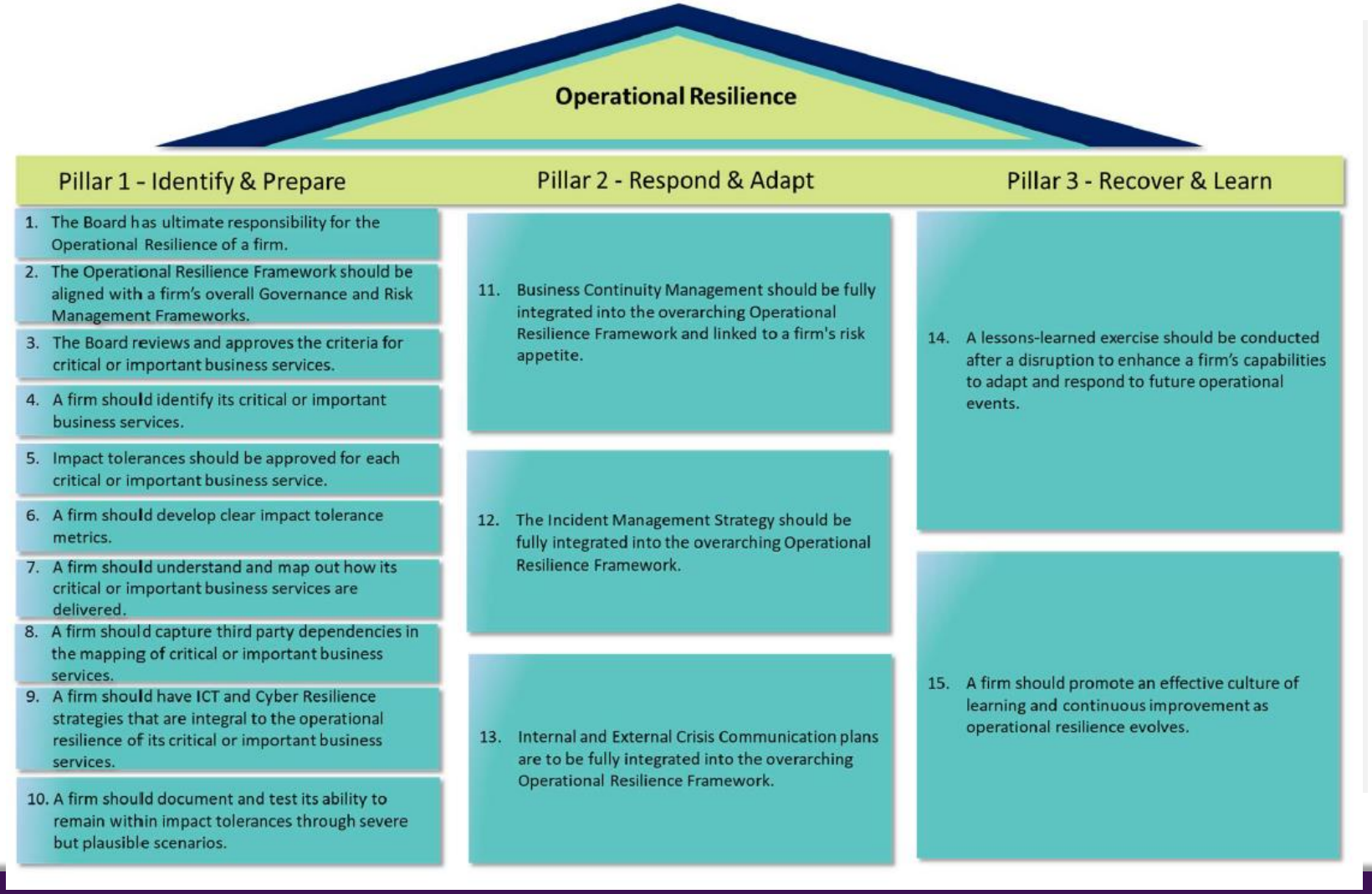
- CP140 was published in April 2021 and final guidance was issued in December 2021
- Communicates the CBI's expectations in relation to the design and management of operational resilience
- Outlines that the Board and Senior Management are responsible
- Requires action – 2 year implementation plan
- Will form part of the CBI's supervisory visits going forward

Operational Resilience

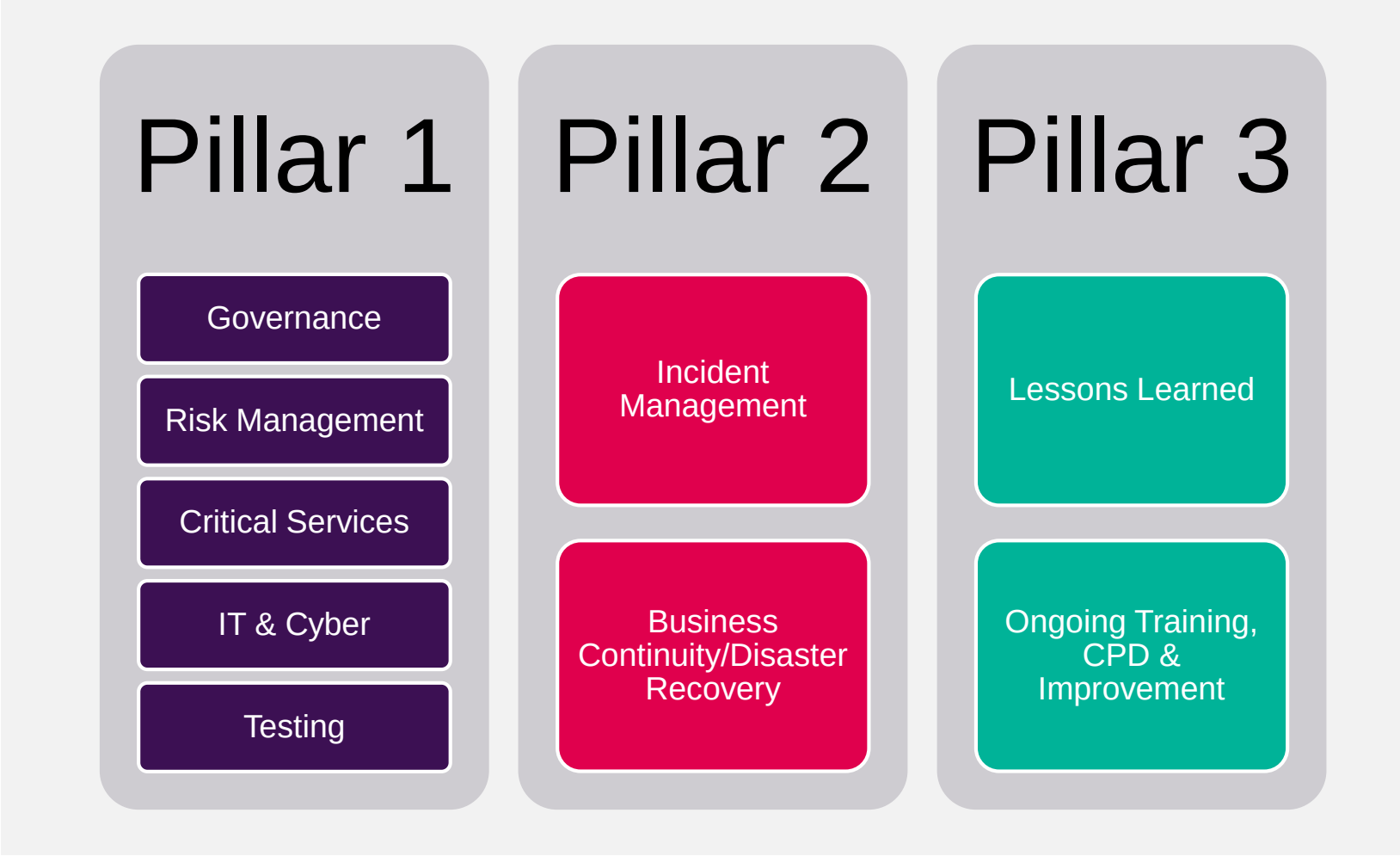
The Three Pillars of Operational Resilience

- Core principles of the framework are:
  - Board and senior management own the framework
  - Requires identification of critical business services and activities – this includes people, processes, technologies and third parties involved in delivery of the services
  - Requires the establishment of impact tolerances and testing via plausible scenarios
  - There should be continuous review and improvement
- 3 Pillars in the framework with 15 guidelines
  - Identify and prepare
  - Respond and adapt
  - Recover and learn

The Three Pillars of Operational Resilience



The Three Pillars



Pillar 1: Governance

- Operational Resilience must form part of the Strategic Planning process
  - Stated policy and objectives are needed as to how resilience will be measured and increased
- This OR Strategy should be used to develop management information for reporting to the Board
  - Existing capabilities, gaps and a plan to address these
- Board should ensure that senior management have sufficient time and resources to implement and support the framework

Pillar 1: Risk Management

- Operational resilience is an extension of operational risk
- The OR framework should be integrated into the existing risk function
- Layers on top of operations, finance and risk to enhance these functions
- Feeds into Business Continuity, IT, Outsourcing and Cyber planning
- Alignment with functions and strategically implemented

Pillar 1: Critical Services

- Set criteria to determine what is critical – impact on customers, financial stability and viability, safety
- Map out the critical services using the documented criteria – Business Impact Analysis is a good starting point
- Identify:
  - People affected
  - Systems required – core and ancillary
  - Maximum acceptable outage time – how long can you stay offline?
  - Recovery point – last nights backup tapes?
  - Impact after a pre-determined time, e.g. 24, 48 or 72 hours

Pillar 1: IT & Cyber

- Information security should be central to the operational resilience framework
- The integrity of the data as well as availability and attitudes to information security need to be considered
- The mapping of critical business processes should include where technology is most required
- These systems should be tested regularly for weaknesses and vulnerabilities

Pillar 1: Testing

- The guidance requires “testing through severe but plausible scenarios”
- Need to know what to test – easy to say things like severe weather, network failure, Wifi Outage **BUT**
- Testing will only work if the critical services and people impacted have been properly identified
- If there are frequent changes, the testing needs to be more regular
- The scenario testing should include escalation, e.g. might start with loss of comms but progress to loss of building

Pillar 2: BCP & Incident Management

- BCP is already a requirement under the Act
- This is enacted as part of the response to a business interruption
- For a BCP to form part of the operational resilience framework it needs to be tested – severe but plausible
- Consider what testing is completed currently
- Does the testing include looking at reliance on third parties?
- How ready are these third parties to respond to a disruptive event

Pillar 2: BCP & Incident Management

- Incident management has 5 elements:
  - Prepare
  - Identify
  - Respond
  - Recover and
  - Review
- Not every incident needs to become a crisis
- Proper incident management will follow the life cycle of the disruptive event
- Meaning that potentially big business disruptors can be stopped early to avoid escalation
- Resilient organisations will do a post incident review and look to see what can be improved

Pillar 3: Ongoing Learning and Improvement

- When “normal” state is returned, a lessons learned exercise needs to be completed
- Look at what information was gathered as part of the disruption:
  - Did the plan work?
  - What decisions were taken?
  - Did people know what to do?
  - Did we respond quickly?
  - Were there vulnerabilities that we hadn’t anticipated
  - What would we do differently?
- Experiences should be shared so that all involved can learn
- Not about assigning blame – continuous improvement for the “real thing”

Key Considerations: People

- Key person dependency is a real risk in operational resilience
- Succession planning is key **but**
- What about an event which is caused by that key person:
  - Vacancy in a PCF role – CEO, Finance, Regulatory function, Board
- Where plans include using internal resources, does that person have appropriate skills and training to undertake the role?
- Current labour market shortages may protract the recruitment process
- Alternatives may need to be considered…

Key Considerations: Outsourcing

- While outsourcing is important there can be a dependency on that provider – e.g. banking platforms
- The dependencies on these providers should be included in the mapping of critical activities
- Outsourcing due diligence and ongoing SLA reviews should cover the outsourced providers own BCP arrangements
- Ensure there is a robust SLA in place

Key Considerations: BCP

- Consider how often the BCP itself is tested
- Many Credit Unions are only testing the backup tapes – not sufficient
- Consider a tabletop walkthrough:
  - Evacuation and move to the DR site
  - Failing over the IT systems to the backup
  - Simulated data breach/cyber attack
  - Switching from IT back to paper
  - Diverting phones/internet/backup generators
  - Employee engagement and communication plan

Key Considerations: 10 Point Plan

1. Develop the operational resilience policy – including MI and KPI reporting
2. Identify critical business activities including the people and the technology
3. Include Information Security in the assessment at #2
4. Define the impact tolerances and develop a plan
5. Review and update the BCP to ensure it is fit for purpose
6. Develop a crisis management plan
7. Test the plans
8. Don’t forget outsourced providers
9. Undertake a look back and learn
10. Review and update annually

What will it look like?

Concluding thoughts

Concluding thoughts

- 18 months left to implement – time to act now to be ready
- Important to identify critical activities but do you know what they are?
- Where are the key person dependencies?
- Is the Business Impact Analysis detailed enough?
- Is the existing BCP comprehensive enough?
- Is there enough rigorous testing?
- This is progress – not perfection

Questions

Thank you

Michelle O'Donoghue
Director
T: +353 9064 80600
E: modonoghue@rbk.ie

@RBK
@RBKCA
@RBK
www.rbk.ie

We're by your side