

# Operational resilience – the challenges and pitfalls for mutuals

**Andy Tomkinson FBCI**

**Associate Director, Operational  
Resilience, Business Risk Services  
Grant Thornton UK LLP**



# Operational Resilience:

## “The ability to absorb shock and bounce back”

### Flip Sides of the Same Operational Resilience Coin

- **Risk Management**

Treat Inherent risks (likelihood and impact) but always left with residual risks



- **Response**

(Emergency Response, Crisis Management, Business Continuity and IT Disaster Recovery, Business Resumption to BAU) Mitigates residual risks

# Operational Resilience simplified



# Joint objectives and approach

Financial Conduct Authority  
[FCA]

CP19/32 Banks, building societies, investment firms, Solvency II firms, e-money, securities, exchanges, payments

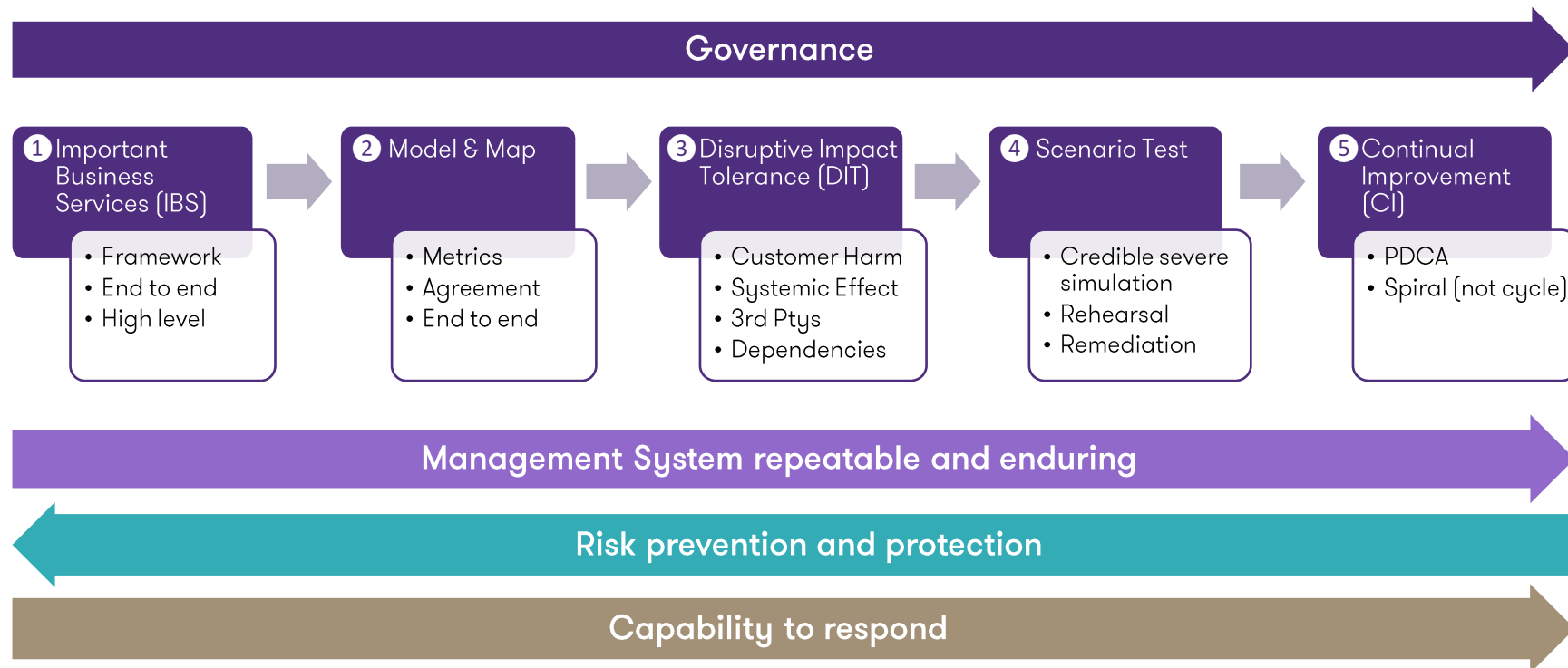
Prudential Regulation Authority  
[PRA]

CP29/19 Banks and Insurers  
CP30/19 Outsourcing

Bank of England  
[BoE]

Central Counterparties  
Payment systems  
Central securities depositories

# Operational Resilience sample programme



# Scope items

## Risk control matrix

Governance	<ul style="list-style-type: none"> <li>• Scope Policy Programme Manual Oversight RACI</li> </ul>
Important Business Services	<ul style="list-style-type: none"> <li>• Process Mapping</li> <li>• Dependency Modelling</li> <li>• IT Systems Integration</li> </ul>
Disruptive Impact Tolerance	<ul style="list-style-type: none"> <li>• Analysis</li> <li>• Agree Results</li> <li>• Inform Plans</li> </ul>
Preventative Controls	<ul style="list-style-type: none"> <li>• Risk Appetite</li> <li>• Inherent Risk</li> <li>• Risk treatment Plan</li> <li>• Regulatory Risk</li> </ul>
3rd Parties	<ul style="list-style-type: none"> <li>• Procurement</li> <li>• Monitoring</li> <li>• Exit Strategies</li> </ul>
Response & Recovery	<ul style="list-style-type: none"> <li>• Emergency Response Plan</li> <li>• Incident Management Plan</li> <li>• Crisis Management Plan</li> <li>• Business Continuity Plans</li> <li>• IT Disaster Recovery Plans</li> </ul>
Stress Testing	<ul style="list-style-type: none"> <li>• Awareness</li> <li>• Training</li> <li>• Rehearsals/Exercises</li> <li>• DR Tests</li> </ul>
Continual Improvement	<ul style="list-style-type: none"> <li>• Continual Improvement process PDCA</li> </ul>















**CUSTOMER HARM**

**SYSTEMIC EFFECT**

**SUPPLY CHAIN FAILURE**  
**3<sup>RD</sup> PTY MSP/OSP**

# Scope

Evaluate the adequacy of the design, controls and operating effectiveness considering the following areas:

 <b>Corporate mission, vision, values</b>	Strategic intent of the organisation underpinned by corporate culture regarding Operational Resilience
 <b>Corporate risk appetite and governance</b>	A governance framework and risk appetite has been established that enables and supports the approach to operational risk management across the organisation.
 <b>Important Business Services</b>	Identify Important business Services by mapping services that could cause external harm to customers, markets and the supply chain
 <b>Policy and Programme</b>	Policy statement from top management providing direction for the annual programme of repeatable and enduring activities in order to develop, establish, maintain, monitor, review and continually improve Operational Resilience
 <b>Mapping</b>	End to end process mapping and dependency modelling of business processes supported by resources and technology
 <b>Disruptive Impact Tolerance incl 3rd Ptys</b>	Analysis of all process and functions, product and services to measure disruptive impact tolerance over time and by dependency including outsourced and managed service partners.
 <b>Relative criticality and thresholds</b>	The priority order and sequence of critical assets agreed and understood so they can be protected by inherent risk controls and effectively react, continue and recover should a residual risk event occur.
 <b>Risk treatment plans, Response plans</b>	Inherent risk management controls are implemented to reduce vulnerability and response plans (emergency response, crisis management, business continuity and IT disaster recovery) are tried and tested to mitigate residual risk.
 <b>Awareness training and rehearsals</b>	Everyone is aware of their part in the culture to mitigate risk and respond to incidents, layers of training are delivered according to need and those skills and capabilities are rehearsed in simulations
 <b>Scenario stress testing</b>	Disruptive Impact Tolerance is proven and managed by plausible yet severe end to end rehearsals of the preventative risk management and the reactive response capability leading to remediation and improvement
 <b>Assurance audit and continual improvement</b>	The governance framework, documents and records and capability is assured and findings are closed in a formal process of continual improvement.
 <b>Leadership, oversight, reporting and MI</b>	Leadership in crisis, oversight in business as usual and documented standing agenda items for Operational Resilience provides management information on where to focus effort to reduce risk and improve response.

# Recycle BCM: Concept and principles

The definition of BCM is to continue or recover what is agreed as critical (from the BIA) to an acceptable level within an agreed time. This includes technology from an ITDR perspective. The underpins development toward operational resilience where treating risks to important business services is equally as important as responding to disruptive impacts.

1. Awareness of the concept of BCM
  - That the principle of BCM is to analyse what is critical in order to focus on the priorities, this is driven by a top down approach where criticality is agreed strategically.
  - Once critical products and services are agreed BCM delivers two elements risk and response

## a. RISK

Inherent risk controls where prevention is better than cure

## b. RESPONSE

Response where residual risk requires an effective reaction

2. Risks are treated proactively. The response is reactive and comprises a sequence of steps through time. Each step requires a documented, tried and tested plan at the appropriate level (Executive, Management, Workforce);

BEFORE	Seconds to minutes AFTER:	Minutes to hours AFTER:	Hours to days AFTER:	Weeks to months AFTER:
Inherent risk treatment	Emergency response	Crisis management	Business continuity & IT disaster recovery	Resume business as usual

3. There is a difference between the governance and administration of the BCMS and the actual capability in the plans (and response teams).

## Governance and Administration of the BCM Lifecycle

Policy, programme, manual  
Analysis (BIA and RA)  
Design & Implementation (RTP)  
Validation & Embedding (Awareness, training, rehearsals)

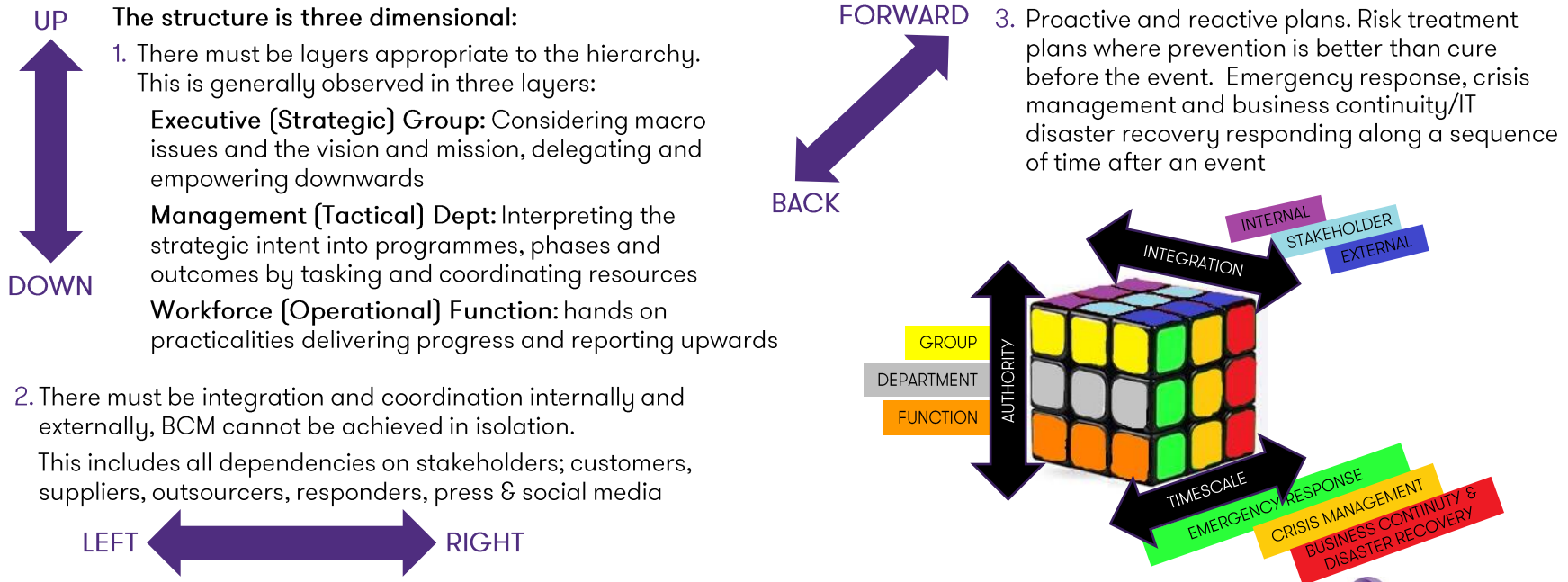
## Practical capability

Emergency response plan  
Crisis management plan  
Business continuity plans  
Disaster recovery plans



# BCM response restructured to OR

BCM and ITDR are essential elements of doing business today. Covid19 has been a real life example of how a risk can have far reaching effects. In response to Covid19, the UK Government has intervened to help businesses across the UK, however organisations should not rely upon this level of support for every catastrophic event. Organisations must be ready to prevent risk and have an effective response which is structured in alignment with good practice other multi-national corporations. Structure can be visualised like a Rubik's Cube.



# What do you have already?

## Business Continuity & Disaster Recovery

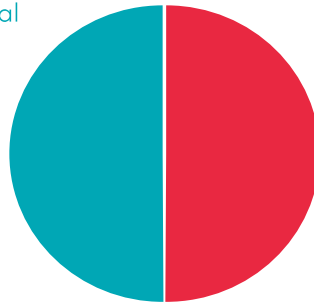
If you have a business continuity management system (BCMS) you should already have the following cycle broken into the components on two sides:

The governance and administration (In blue)

The response plans (In red)

### GOVERNANCE

Policy, Programme, Manual  
Business Impact Analysis  
Risk Assessment  
Awareness, Training  
Rehearsals  
Continual Improvement  
Embedded into culture



### RESPONSE

Emergency Response Plan  
Crisis Management Plan  
Business Continuity Plan  
Disaster Recovery Plan

### Areas of weakness in the BCMS:

It is owned centrally so there is insufficient RACI in the business functions.

The BIA is based on risks not business criticality so the plans are incorrectly scenario based

The BIA does not align ITDR and BCP metrics leading to an expectation gap

The plans are merged into one gigantic document containing the policy, BIA and plans which is difficult to navigate

Human factors are not considered

Risk treatment is rarely implemented

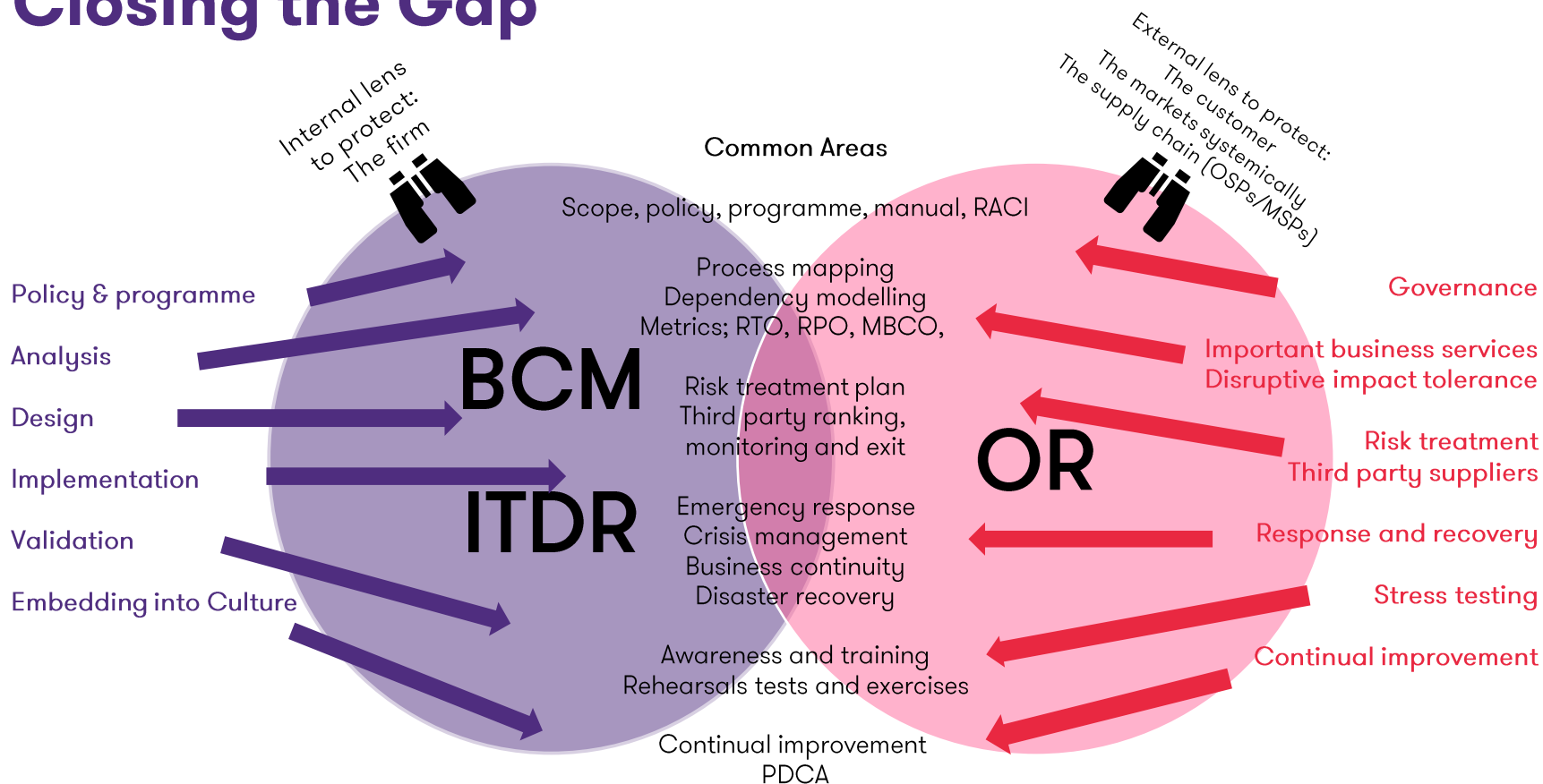
3<sup>rd</sup> parties are excluded

Continual improvement is informal if documented at all

Rarely rehearsed, rarely DR tested

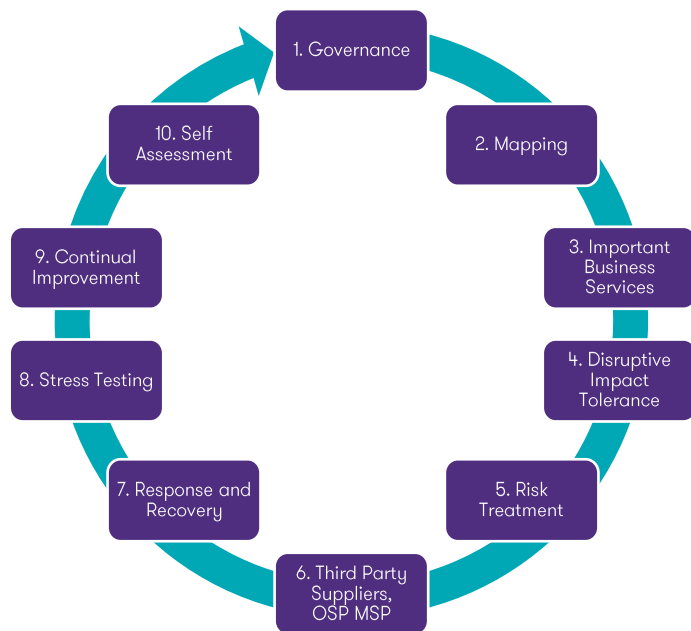
Quite rightly BCM looks a protecting the organisation (people assets profitability, reputation)

# Closing the Gap



# Our approach

## Industry guidance: Ten steps toward Operational Resilience



Step	Processes
1 Governance	Scope, policy, programme, manual, governance, oversight and RACI (Responsible, Accountable, Consulted and Informed). Annual attestation, OR Framework and Target Operating Model
2 Mapping	End to end process mapping and dependency modelling of business processes supported by resources and technology
3 Important Business Services	Identify Important business Services by mapping services that could cause external harm to customers, markets and the supply chain
4 Disruptive Impact Tolerance	Setting impact tolerances and metrics to measure relative criticality from the end to end of each important business service
5 Risk Treatment	Implementation of a risk control to protect against vulnerability or prevent a risk to an important business service
6 Third Party Suppliers, OSP, MSP	Ranking, monitoring and exit strategies for key suppliers, outsourced service partners and managed service providers
7 Response and Recovery	Reactive plans for emergency response, incident management crisis management business continuity and disaster recovery
8 Stress Testing	Plausible but severe scenarios rehearsed in a simulation leading to risk reduction, improved capability and better plans.
9 Continual Improvement	Plan-do-check-act spiral of discovery, investigation, root cause analysis, remediation, re-testing and close
10 Self Assessment	Provide Board level assurance on the status of compliance to the Operational Resilience Regulations.

# Key challenges

## Key challenges to operational resilience in financial services organisations

- 1. Benchmarking:** The vast majority of firms have written a scope, policy or strategy and designed a framework as a programme which is being implemented as a work in progress. This accounts for an estimated 80% between the more and less advanced, well short of the leaders 5% who have implemented. The trailing edge firms haven't started yet. They are aware but due to conflicting priorities such as Covid, Brexit, Libor etc have not the resources, motivation or inclination. It is estimated that this accounts for 15% of firms which are likely to miss the first deadline.
- 2. Misunderstanding the perspective:** The business continuity perspective is internal. Business continuity quite rightly protects the firm, but the operational resilience perspective is external; to protect the customer, the markets and the supply chain. It is a challenge to judge internal business continuity critical processes such as Payroll that is not an important business service from the customer's perspective. The regulator is looking for mapping and disruptive impact tolerance from end to end process that focuses on the three external risks of; customer harm, market instability or supply chain domino effect. Payroll clearly isn't part of that critical path of activities.
- 3. Definitions are too complex:** The point of resilience is twofold; 'To absorb shock and bounce back'. Absorb shock, by proactive risk management and bounce back, by reactive response plans. Many firms focus only on the reactive response plans. The regulatory view is that prevention is better than cure, therefore risk treatment is an equal to response plans.
- 4. Resourcing:** Only one person has been tasked to design the framework and then implement it. Successful business continuity is where the ownership of activities such as an annual business impact analysis or an annual scenario based rehearsal or the authorship of the BC Plans is owned by the business function (not the central resource). Operational resilience has to be owned by the business functions too.
- 5. Third parties:** Procurement and monitoring existing vendors, outsourcers and partners is generally subject to an annual review, an approved suppliers list and a check and balance of the contract performance, costs, SLAs and KPIs. Operational resilience is broader and more focussed. The existing annual monitoring is fine except for those few [often only the top 3-5 suppliers] that could cause customer harm, market instability or supply chain domino effect. For those Operational resilience is looking for more frequent and broader monitoring. Operational resilience looks at liquidity, fourth party suppliers, staff morale/skills retention or attrition, merger or acquisition, where monitoring could trigger an alarm (risk management context) and the invocation of an exit strategy.
- 6. Stress testing:** Linked to risk based scenarios and parameters from disruptive impact tolerance. Few firms use plausible but severe simulations to rehearse their response capability. To meet the regulations it is certainly not a fire drill or evacuation. Desktop exercises is a step along the maturity scale but ultimately an annual rehearsal should be multi-layer, involve external parties and be as realistic as possible. Few firms, less than 20% facilitate realistic exercises.
- 7. Continual improvement** - operational resilience calls out continual improvement. That is the upward spiral of Plan-Do-Check-Act. The majority of firms do not have a documented procedure following the steps of continual improvement; discovery, investigation, root cause analysis, remediation, testing/re-assessment, closure.



How Grant Thornton supports in the development of resilience and assurance frameworks:

1. We are agile.
2. We understand the art and science of Operational Resilience.
3. We keep it simple, real and appropriate.
4. We are a team supported by a corporation.
5. We are inclusive (and can't do this in isolation)
6. We know 'practice makes perfect'.
7. We know this is a spiral of continual improvement.

# Questions?



# Thank you for joining us today



**Andy Tomkinson**

Associate Director, Operational Resilience,  
Business Risk Services

Grant Thornton UK LLP

T +44 (0) 161 214 6306

E [Andy.D.Tomkinson@uk.gt.com](mailto:Andy.D.Tomkinson@uk.gt.com)



---

[grantthornton.co.uk](https://grantthornton.co.uk)

© 2021 Grant Thornton UK LLP.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.