airmic LIVE

airmic

airmic LIVE

Today's Objectives:

- What operational resilience means, and what the role of the risk manager should be in helping to achieve it.
- What resilience means to an Executive or Board.
- How organisations are implementing operational resilience and what 'enough resilience' looks like.

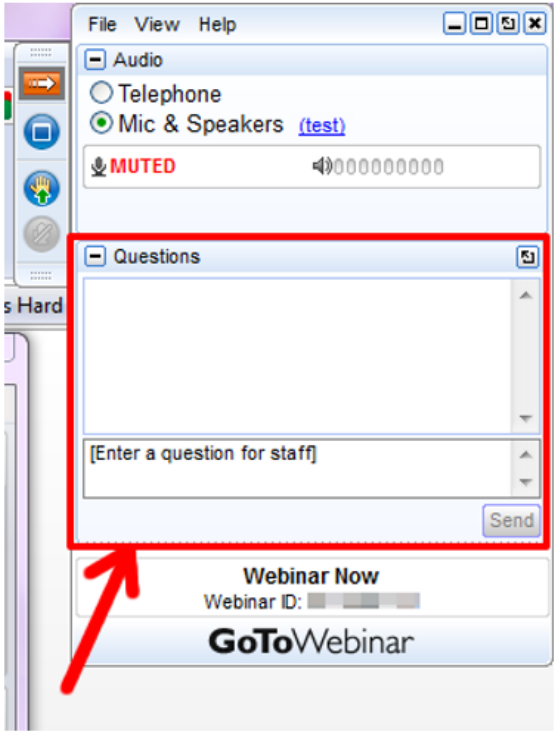
airmic

airmic LIVE

How to ask questions during the webinar

Use the questions panel in the GoToWebinar console

If the console is not visible, click the orange arrow to expand it



MARSH

Operational Resilience

December 2020

MARSH & McLENNAN COMPANIES

The Emergence of Operational Resilience

1. **Board accountability for critical infrastructure:** General lack of board-level ownership for IT risk.
2. **IT expertise on the board:** Limited technology expertise on the board.
3. **IT risk appetite:** Weaknesses in the way risk appetite was applied and a lack of comprehensive mapping of resilience requirements.
4. **Maturity of the three lines of defence:** Was relatively weak with a poor delineation between first line and second line activities.
5. **Resilience scenarios:** Were not far reaching enough to capture high impact events, or to reflect concentration risk and dependencies on shared infrastructure.
6. **Contractors:** Weaknesses in oversight of third-party IT providers; despite the growing reliance.

RECEIVED
21 OCT 2015

Financial Conduct Authority
25 The North Colonnade
Canary Wharf
London
E14 5HS

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

Rt Hon Andrew Tyrie MP
Treasury Committee
14 Tothill Street
London
SW1H 9NB

19 October 2015

Dear Andrew,

RE: Review of critical infrastructure and technology resilience

Thank you for your letter dated 28 September 2015 in which you ask a number of questions related to the joint review on critical infrastructure recently conducted by the FCA and the PRA.

By way of background, this is called the 'Dear Chairman II Exercise' (DCE-II). It was carried out as a follow up to the first Dear Chairman Exercise (DCE-I) which was conducted by the FSA in response to the June 2012 IT incident at the Royal Bank of Scotland.

DCE-I sought to understand the levels of resilience and the banks' exposure to technology risk. The high level themes from this review were:

- insufficient oversight of technology at Board level;
- weaknesses in the firms' 3-Lines-Of-Defence model and IT risk management arrangements; and
- improvements required to disaster recovery (DR) capabilities

DCE-II [covered the seven largest UK deposit-takers and] assessed the improvements to technology resilience since the first exercise. Whilst DCE-II has been conducted as a joint FCA and PRA exercise, each regulator has focused on topics relevant to their statutory objectives. The objective of DCE-II from an FCA perspective was to assess whether operational resilience, across the banks in scope, is adequate to mitigate the risk of significant customer detriment and prevent adverse market implications resulting from a major IT failure.

Our answers to your questions are based on the FCA's findings from DCE-II and the feedback provided to the seven firms. The PRA has issued separate feedback letters to the firms

Source:
https://www.parliament.uk/globalassets/documents/commons-committees/treasury/Correspondence/Letter-from-Tracey-McDermott-FCA-to-Treasury-Chair-19-10-15.pdf

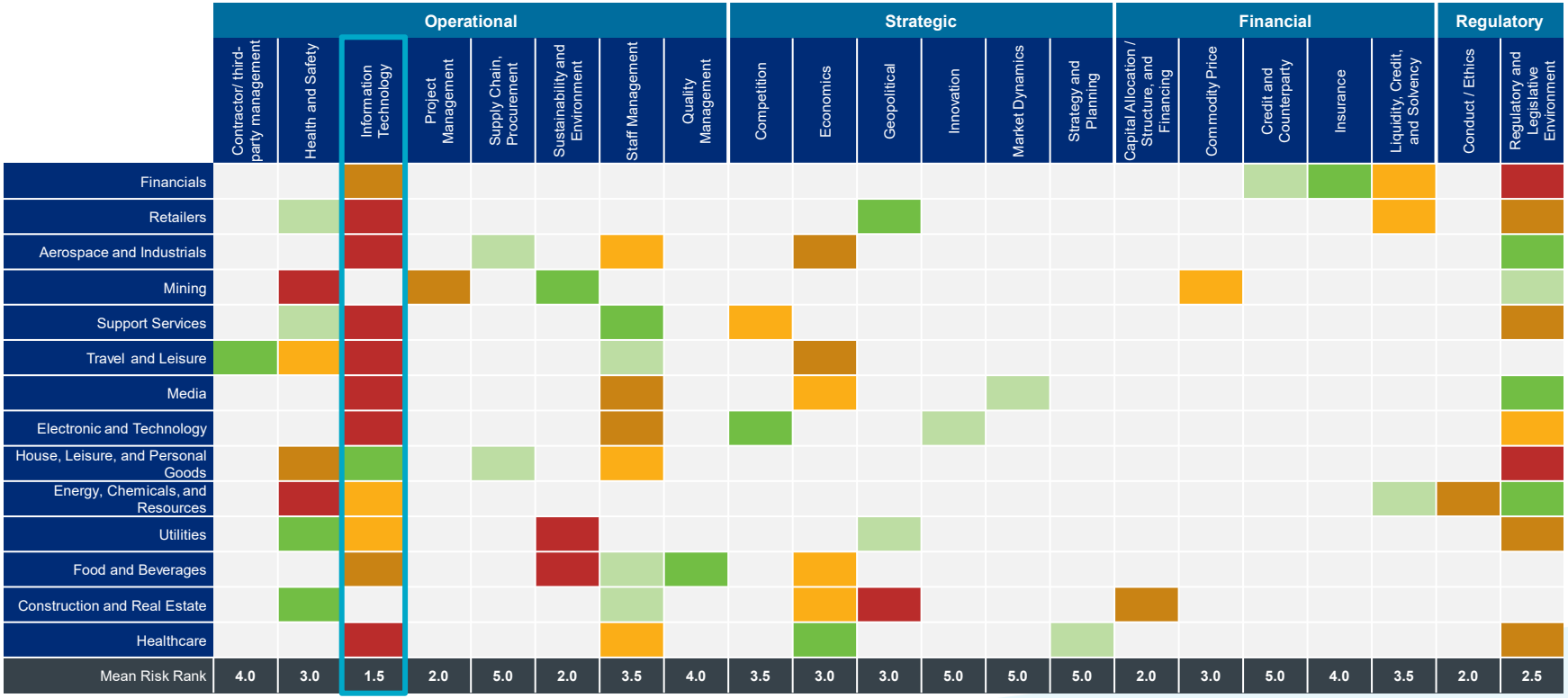
Components of an Operational Resilience Approach

1. Deliver resilience at a business service level, to minimise customer disruption.
2. Define a board's tolerance to disruptions.
3. Use scenarios to test resilience.
4. Assume disruptions will happen and plan accordingly.
5. Build a faster response to disruptions and communicate.

Implies

- Resilience is a board issue.
- Improved focus on customer outcomes.
- The mapping of business services is needed.
- Tolerance to disruption needs to be defined.
- Closer interaction between risk management and business continuity.
- More challenging risk scenarios, appreciating connectivity of risk

FTSE Top Five Risks Ranked by Occurrence for Each Industry



Source: Marsh and Cranfield University study 2019

History or Hindsight?

> *Given the ease and speed with which people can travel around the world, it is therefore possible that a new infection could spread rapidly before it is detected.*

> *This rapid spread of a new infection is a reminder that new infections pose a global threat, challenging the whole global public health community.*

Source: Cabinet Office National Risk Register 2010

COVID as the Catalyst for a Wider Debate About Operational Resilience

Supply chains unknown and/or lack resilience.

Rapidly evolving policy responses which differ by country and industry.

Unclear data and inconsistent projections for epidemic and economy.

Prior business continuity planning often unequal to the challenge.

- **Prior resilience planning too narrowly focussed** relying too heavily on work area recovery.
- **Inflexible risk responses inadequate** for a rapidly evolving pandemic.
- **Critical decisions made without full data** availability or assessment.
- **Hard knowing when to bring resources back on stream** by country/sector/product.
- **Remote working making** it harder to maintain professional support networks.
- **Difficulty maximising the recovery** when future scenarios are so uncertain/volatile.

Summarised as:

Data and Analysis

Scope

Depth

The Need for Resilience is Not Going Away

Increased complexity and connectivity of crisis events.

Rising expectations and an increased requirement for assurance.

Growing cyber exposures and increased automation.

Increasing costs and margin pressure, trade-off with resilience.

Poll #1

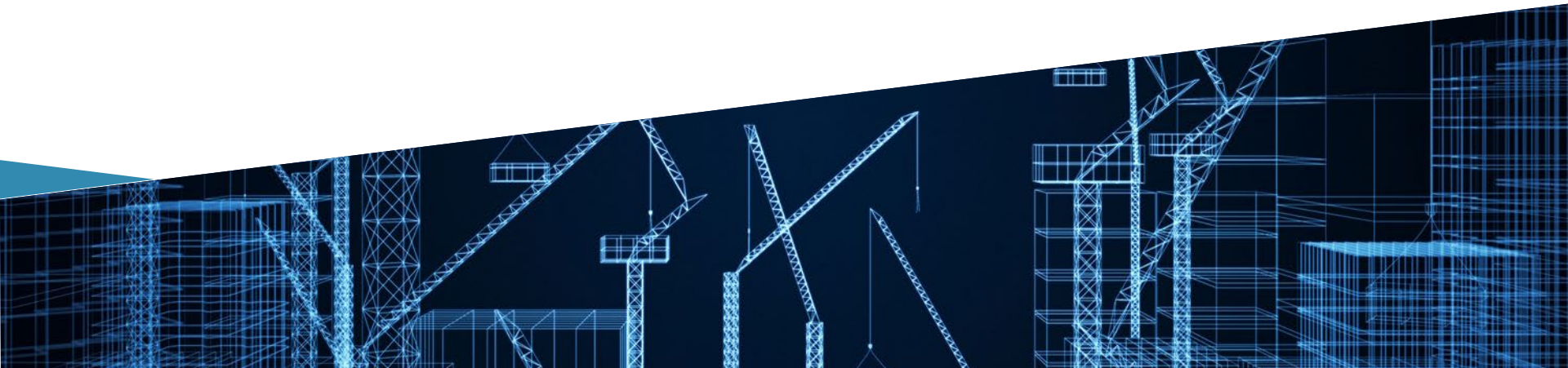
Where do you anticipate your focus to be over the next 18 months?

a) More of the same, we do not anticipate a need to change.

b) More time spent providing assurance to senior management.

c) Greater effort spent on stress testing our resilience controls.

d) Leading a change programme to transform our approach to resilience.



Linear Approaches to Resilience are Insufficient

	Risk Driven by Event	**Value of an Integrated Approach**	**Resilience** Driven by Business Process
1. Define	• Risk landscape and risk appetite definition.	**Aligned and customer-centric view of tolerance to disruption and risk appetite.**	• Strategic view of business services and the impact of disruption.
2. Assess	• Risk assessment and quantification (including stress testing).	**Common failure scenarios understood using risk modelling and business process mapping.**	• Mapping of critical supporting business processes and systems.
3. Manage and Implement	• Assessment and overlay of controls and risk transfer.	**Optimised investments in preventative and recovery controls.**	• Build recovery plans and resilience measures.
4. Test and Monitor	• Monitoring of control and risk indicators. • Integrated controls assurance.	**Resilience of provision of key customer services and confidence to stakeholders that risks are well managed.**	• Business continuity and crisis exercises. • Updating plans and enhancing resilience arrangements.

Worked Example
Major System Failure of Mortgage Lending Services

Set tolerance levels for business services in line with risk appetite. → **Map processes** → **Identify resource dependencies, risks, related controls, and assurance coverage to define risk exposure versus impact tolerance.**

Business Service

Mortgage lending
Disruption impact tolerance: 1 day

Impact driven by potential to:

- Harm consumers and market participants.
- Undermine financial stability.
- Threaten firm's viability.

Key Process Steps

1. Application
2. Approval
3. Payment
4. Collection

Tolerance

1. Application	5 days
2. Approval	5 days
3. Payment	1 day
4. Collection	3 days

Resources	Risk Areas	Risk Controls
IT	• System failure. • Change control failure.	• IT disaster recovery. • ITIL processes. • Paper based/phone applications.
People	• Employment practices. • Errors and omissions. • Training. • Internal fraud.	• Quality management. • Training and certification. • Fraud monitoring.
Premises	• […]	• […]
Data	• […]	• […]
Vendors	• […]	• […]

Use risk modelling to define impact tolerances and common failure scenarios.

Stress testing to validate control effectiveness, provide MI for monitoring of impact tolerance.

ITIL: Information Technology Infrastructure Library

Poll #2

How integrated is your resilience and risk framework?

a) We are completely integrated with one framework, an integrated system, and clear lines of reporting.

b) There is some connectivity, for instance risk knowledge informs the BCP threat assessment.

c) There is some interaction at a risk controls level (typically in the first line of defence).

d) We have separate frameworks and reporting lines with very limited connectivity.

BCP: Business Continuity Planning

Pre COVID

- Often property and IT focussed.
- Processes over people.
- Scope limitations.
- Assumptions often untested.
- Scenarios not sufficiently challenging.
- Difficulty maintaining executive committee input.
- Depth of planning shallow.

Post COVID

- Leading a crisis with empathy.
- Rebalancing of resilience solutions.
- Acceleration of operational resilience.
- Using data to drive disruption modelling.
- Closer scrutiny of third-party continuity.
- Balance of cost reduction versus resilience.
- Stronger role for the second line.

Insurance Brokers

Chartered