Future proof your organisation - an internal audit approach to operational resilience

Today's presenters

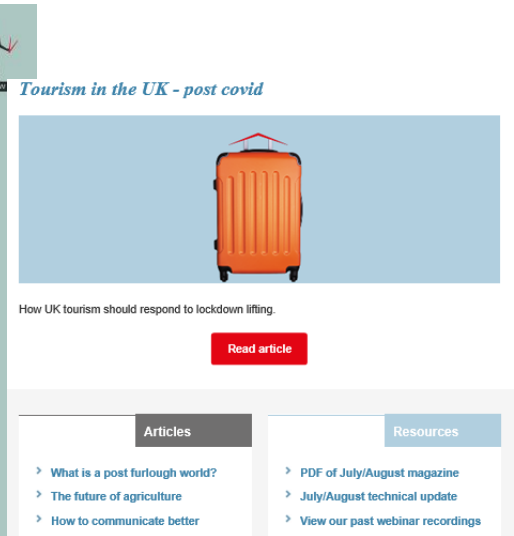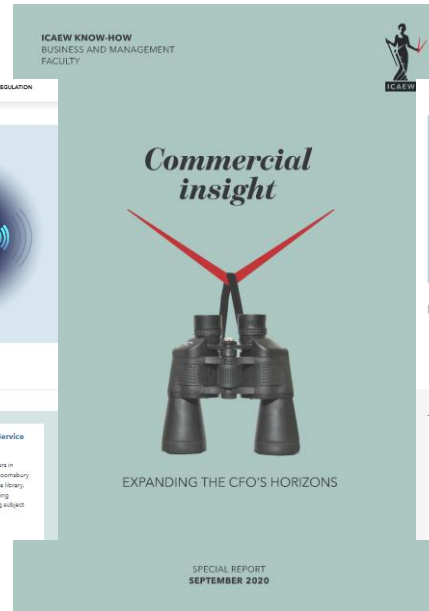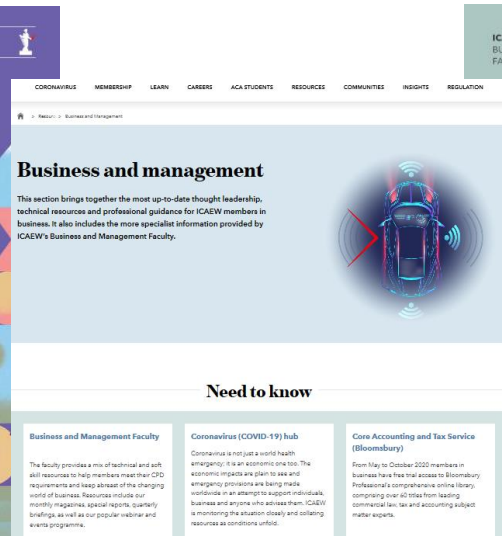*Michael Haddon*   *Abigail Harper*   *David Jardine*

Business and Management Faculty

icaew.com/joinbam

Agenda

Operational Resilience – 1 hour session

1. Setting context

2. What do we mean by operational resilience and what does it look like?

3. What we are learning from the Covid Crisis

4. Developing an audit approach

5. Q&A

Setting Context

- Operational disruption can:

  - Impact stability within an industry

  - Threaten the viability of individual organisations

  - Cause harm to consumers and other market participants

- Organisations should:

  - View achieving operational resilience as a strategic goal

  - Recognise operational disruption as a key business risk

  - Embed a framework, policies and procedures to reduce the likelihood and impact of disruption and achieve the desired outcome in a proportionate, coordinated and cost-effective way

Setting Context

- Achieving operational resilience is far-reaching and complex and for many organisations

- Assessing what they need to do and how to do it is very much work-in-progress

- Organisations should not lose sight of the fact that operational resilience is an outcome, not a function or process

- Regulators are also taking a strong interest in operational resilience

- The Covid-19 crisis has brought operational resilience into even sharper focus

What do we mean by operational resilience and what does it look like?

- Defining and articulating what it what it means to be operationally resilient and how aim to achieve this

- Having arrangements in place to prevent, respond and recover from disruption within an agreed risk appetite

- Determining what activities currently contribute to resilience and what additional steps are needed to achieve desired outcomes

- Embedding preventative measures and capabilities – in terms of people, processes and culture – to adapt and recover when things go wrong

What do we mean by operational resilience and what does it look like?

- A broad approach to maintain the continuity of key services regardless of the cause of disruption

- Define and manage operational resilience within the context of existing risk management activities, in particular:

  - Operational Risk

  - Business continuity

  - Disaster recovery

- Prevent disruption occurring, as far as possible

- Assume that disruption will happen and so establish measures to remedy/keep a service running

Building Resilience - What organisations need to do

- Enable a prompt return to business as usual (or a revised version of this) when a disruption is over

- Maintain effective communication with affected stakeholders, in particular the customer base

- Set tolerances at the first point at which disruption to a key business service would cause unacceptable levels of harm to consumers or markets

- Learn and evolve from both incidents and near misses

Building Resilience – Framework Elements

- Supply chain/outsourced function risk and mitigating measures

- Information Security, Cyber Security and Data Protection controls

- Change Management protocols

- Crisis Management and Communication plans

- Incident Response plans

- Business Continuity and Disaster Recovery plans, including mitigation strategies for risks to people, premises, technology and data

- Meaningful Management Information

- Risk Management, Compliance and Audit oversight and assurance

What we are learning from the Covid Crisis

- Demonstrating that an organisation is operationally resilient is much more than assessing the robustness of its business continuity and disaster recovery plans

- Many organisations now see that their plans were not as robust as originally thought – many had not envisaged a fully remote working response to a pandemic and had not 'played out' this scenario in sufficient detail

- Greater consideration of higher impact, lower likelihood scenarios is needed

- Organisations should keep an eye out for 'complacency' around operational resilience - a pandemic is only one scenario

- A successful outcome is dependent on a number of interconnected activities and this is a real challenge to do that efficiently

What we are learning from the Covid Crisis

- Managing outsourced providers, third parties and supply chains is much tougher in a crisis

- BCPs have been 'tested' in real life scenarios

- Assessing personal resilience and wellbeing – key elements of productivity and development

- Linking operational resilience with financial resilience

- Acceleration of automation and digitisation initiatives

- Translating 'agility' and 'adaptability' to the benefit of all stakeholders

What are organisations finding challenging?

- Many organisations have not yet:
  - Defined and articulated what it means to be operationally resilient and how they aim to achieve this
  - Gained clarity on what activities currently contribute to resilience and what additional steps are needed to achieve the desired outcome
- Many organisations have not sufficiently articulated their appetite for risk and how this relates to operational resilience
- Where risk appetite statements are made, they are not always
  - Aligned/linked to strategy
  - Appropriately embedded across risk frameworks (however simple those frameworks may be)
  - Consistently understood and applied

Developing an effective audit approach

- Operational resilience poses a challenge for internal audit - it's a complex area but it is an opportunity for internal audit to be 'on the front foot'

- Practices are evolving and many organisations are at a relatively early stage of design and embedding a fit for purpose approach and framework

- Develop an audit approach that reflects maturity across your organisation's framework

- Given the far reaching aspects of resilience and the different ways it can be approached, there is no 'one-size fits all'

- Internal audit is well placed to leverage existing business continuity, disaster recovery and operational risk audits/experience as a basis for creating an operational resilience audit approach

Developing an effective audit approach

- The approach will depend on a number of factors, including:

  - How management has articulated what operational resilience means for the organisation

  - The relative maturity of the organisation's operational resilience arrangements

  - Whether the resulting (or planned) framework aligns to aspirations

- In a less mature environment - provide value by adopting a review and recommend scope and focus on assessing framework design

- Where the framework is more developed and embedded - provide greater assurance over operating effectiveness

- Decide on a standalone review or to be covered within each element of a broader, more robust framework

Developing an effective audit approach

- Consider adding a resilience component to the scope in reviews on IT and cyber security, supply chain management, business continuity, disaster recovery and operational risk management

- For example, extend the scope of a traditional third party/outsourced management review to capture the following:

  - Does the organisation understand third party business continuity risk (including concentrations risks such as cloud provider and outsourcing geography concentration)?

  - Has management performed due diligence over its supplier's continuity arrangements (including their own supplier dependency to the necessary degree of dependency)?

  - Are there workarounds in place for supplier loss?

Developing an effective audit approach – review focus areas

- Design and Embedding a robust Framework

- Identifying and Mapping of Key Business Services

- Defining Tolerances and Limits

- Business Continuity Plans

- Setting and Testing Scenarios

- Incident response

- Considered Lessons Learned

- Digitisation

- Governance

Developing an effective audit approach - questions to be asking

- Has your organisation identified its key business services?

- Has your organisation identified and documented the people, processes, technology, facilities and information that supports the delivery of each important business service?

- Has your organisation set impact tolerances for important business services?

- Has your organisation defined the scenarios and supporting methodology to be used for the scenario testing of each impact tolerance?

- What do you think most threatens the resilience of your organisation?

- What area do you think your organisation is most mature?

- Which executive is leading and taking ownership of the operational resilience plan?

- Does your Board collectively have knowledge, skills and expertise in relation to operational resilience

Q&A

Upcoming BAM webinars

60 minute webinars – 10.00am

Digital downtime
16 March

Modern slavery: how to prepare a s54 statement
17 March

Using scenario planning to navigate uncertainty
14 April

Business resilience
27 April

Skills to future proof your career
5 May

Economic update
9 June

Building an innovative team
7 July

20 minute webinars – 12.30pm

Motivating your team: A three-pronged approach
24 March

Data valuation: the key to more value creation
26 April

Managing bribery and corruption in a downturn
12 May

Why You? 101 job interview questions you'll never fear again
21 September

Online learning – 10.00am

Get the job you want
14 September

icaew.com/bamevents

Thank you for attending

Contact the Business & Management Faculty

icaew.com/bam

✉ *bam@icaew.com*   ☎ *+44 (0)20 7920 8508*

@ICAEW_BAM

Upcoming Business & Management Faculty webinars
icaew.com/bamevents

Join the Business & Management Faculty
icaew.com/joinbam