ICAEW KNOW-HOW
BUSINESS AND MANAGEMENT FACULTY

HOW TO AUDIT OPERATIONAL RESILIENCE

GUIDE

8 February 2021

In this second paper on operational resilience, we will look at how to develop the audit approach. Our first paper highlighted this as a complex subject, which presents both challenges and opportunities for internal audit, given many organisations are in the early stages of their resilience journeys. The topic can seem deeply technical and so when developing a framework for achieving operational resilience, organisations need to turn the principles underpinning this goal into simple and proportionate activities as far as they can.

INTERNAL AUDIT OBJECTIVES

Internal audit should aim to assess the effectiveness of their organisation's operational resilience arrangements. In doing so, it should firstly determine whether there is a good articulation and understanding of what operational resilience means to the organisation within the context of their specific industry.

This includes defining and identifying the business services which, were they to fail, could impact customers, markets, and other stakeholders together with the measures needed to ensure the business remains operational.

DEVELOPING AN OUTLINE APPROACH

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

- How management has articulated what operational resilience means for the organisation;
- The relative maturity of an organisation's operational resilience arrangements; and
- Whether the resulting (or planned) framework aligns to aspirations.

For example, in a less mature environment, internal audit is more likely to provide value by adopting a review and recommend scope to its work and focusing its effort on assessing the framework's design. Where the framework is more developed and embedded, internal audit should aim to provide greater assurance over the operating effectiveness.

Internal audit should also consider whether it will assess operational resilience as a standalone review or assess how resilience is covered within each element of a broader, more robust framework. This means adding a resilience component to the review scope in areas such as IT and cyber security, supply chain management, business continuity, disaster recovery and operational risk management. For example, internal audit may need to 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?

While the approach to be taken will be driven by an organisation's size and complexity, understanding how management ensures an integrated approach to achieving its overall resilience goals will be critical to delivering an effective and valued audit.

RISK ASSESSMENT

Internal audit should form its own view of the risks that could impair an organisation's operational resilience and/or cause operational disruption to guide its review scope and testing programme. If management has completed a resilience maturity assessment, internal audit should compare these results to its own view of the current position.

Many organisations are (or soon will be) looking at the lessons learned from responding to, and dealing with, the Covid-19 crisis and this will have covered (either directly or indirectly) elements of a resilience framework.

MANAGEMENT RESPONSIBILITIES

Understanding who within the management team is leading the organisation's efforts in this area is another important part of an audit. Typically, this will be the Chief Operating Officer working closely with the Chief Information/Chief Technology Officer and the Chief Risk Officer.

Unclear responsibilities, particularly where a business service is supported by a range of people, systems, processes and third parties is a real threat to effective resilience. In addition, assessing the extent of ownership, understanding at and escalation to Board level should be covered.

PLANNING CONSIDERATIONS

Internal audit should consider the extent to which management has completed the following:

- Has the organisation identified its key business services?
- Has the organisation identified and documented the people, processes, technology, facilities and information that supports the delivery of each important business service?
- Has the organisation defined the scenarios and supporting methodology to be used for the scenario testing and are the results current and justified?
- What does management think most threatens the resilience of the organisation?
- What areas of the organisation does management think are most mature?
- Which executive is leading and taking ownership of the operational resilience plan?
- Does the Board collectively have sufficient knowledge, skills and expertise in relation to operational resilience?
- What evaluations of past experience have been performed?
- Does management have a view as to what are acceptable levels of disruption? Does it know it can meet this level?
- Does the organisation have any strategy for responding to lessons learned and modifying its processes in order to be more resilient in the future?

LOOKING OUT FOR RED FLAGS

When assessing risk, internal audit should consider potential red flags that could indicate weaknesses. These include:

- Lack of skills and understanding at senior levels
- Lack of substantiated analysis of key services and the required resilience levels
- Limited data and unrealistic assumptions supporting scenario analysis and testing
- Limited/incomprehensive register of business services
- Limited/incomprehensive inventory of people, processes, technology, facilities and data (especially those relevant to critical services
- Over reliance on end-user computing
- Qualification, experience and the role of personnel involved in performing resilience arrangements (including analysis and design activities)
- Significant/unexplained fluctuations in probability assessments, disruptions and the potential impact
- Poor articulation and understanding of risk appetite and risk tolerances across the organisation
- Inflexible legacy infrastructure that is hard to fix and further complicated by adding ever more layers and systems to manage
- New regulations that increase operational resilience challenges (particularly when it relates to the risk of illegally sharing sensitive customer information).

The interconnectedness of technology infrastructure that exists today is also a concern and the potential risks attached to this should be acknowledged. For example, the outage RBS had in 2012 following a routine software upgrade that went wrong led to a £56million fine. This outage impacted many customer facing activities and lasted a number of weeks.

Organisations should therefore always consider the impact of small scale changes that are made incrementally or through minor alterations. These can often attract less oversight and control than major projects, but can lead to significant issues.

FOCUS AREAS FOR INTERNAL AUDIT

Internal audit should focus on assessing how well management has carried out and implemented the following activities which are needed in some shape or form to ensure a fit-for-purpose framework and approach.

Framework Design

This will assess whether the organisation has an effective resilience framework given the size and complexity of its business. This could be an operational resilience framework itself or enhancements made to existing policies and processes addressing the elements of operational resilience.

What standards, guidance and good practices has management adopted when developing the framework? Are these appropriate given the organisation’s business model and activities? Has the framework captured the key elements of operational resilience, including risk appetite, policies and underlying building blocks/supporting elements?

Identification and mapping of Key Business Services

A key business service is one that, if disrupted, would be most likely to cause significant levels of harm to stakeholders, particularly customers or the wider marketplace. It should be identifiable as a separate service and it should be clear as to who uses the service and how the service is delivered. In this regard, understanding how management has completed the following actions needs to be considered:

- Assessed which business services present a risk of customer or market harm in the event of a disruptive event
- Identified and documented the services that are key to the business and its customers

- Mapped the key business services to the underlying systems, premises, people, and third parties etc. that support its delivery. This is a fundamental input to risk mitigation strategies and continuity plans
- Highlighted any reliance/dependency on an outsourced provider, including an assessment of how the failure of an individual system or process could impact the provision of the business service ie, the identification of “critical systems/processes”
- Identified the possible points of failure and assessed the organisation’s ability to withstand the failure and continue to provide the key business service in the event of disruption. For each scenario, management should establish the potential level and impact of disruption. As part of this process, management should also identify which systems and processes are capable of being substituted if such an interruption occurs
- Established escalation protocols to enable them to take timely action
- Developed remedial plans assuming there is a process or system failure and no readily available substitute (as well as highlighting those processes and systems which can be substituted during disruption)
- Identified where possible investment is needed, whether that be updates to systems, new systems, training to staff etc.

If management has already carried out a business impact analysis as part of its business continuity activities, then this will help inform the mapping exercise and help save time. When assessing how well management has carried out its mapping, it is important to look out for elements that are overly subjective or are not supported by enough meaningful analysis, as both of these reduce confidence in the robustness of the documented outputs.

Defining impact tolerances

This is a relatively new term and is being used by the regulators in financial services. Impact tolerance levels should describe the organisation’s tolerance for disruptions to a particular business service, under the assumption that disruptions to the systems and underlying processes supporting the service will occur.

Setting impact tolerance levels is intended to change the mind-set of an organisation away from traditional risk management towards accepting that disruption to business services is inevitable and needs to be managed effectively.

In principle, the use of impact tolerance is a sound element of operational resilience, and its application should be proportionate to the nature and scale of the business. While larger and more complex organisations will have lots of data to support their efforts, smaller and simpler businesses will need to take a more qualitative approach to defining and measuring impact tolerance.

Impact tolerances should be expressed by reference to specific outcomes and metrics. Such metrics may include:

- The number and types (eg, vulnerability) of consumers or other key stakeholders
- Financial loss to consumers
- Financial loss to the organisation where this could hurt consumers
- Financial loss that could affect market stability
- Loss of functionality that could affect market stability
- Loss of functionality or access for consumers
- Reputation damage that could harm consumers
- Impact to market or consumer confidence
- Spread of risks to other business services or markets
- Any loss of data confidentiality, integrity or availability
- Maximum acceptable outage time for a business service or system
- Maximum number of customers affected by an event
- Maximum allowed time for restoration of a business service or system

- Number of outages in the year.

When assessing how well management has defined impact tolerances, it will be important to assess the thoroughness and analysis of information/intelligence relied upon. For instance, when evaluating harm to customers, management may need to seek the opinion of most customers as to what constitutes/defines harm as opposed to inconvenience.

Impact tolerances should be monitored and evaluated through scenario testing (ie, severe but plausible events) and the impact this would have on the key business service. Outcomes of testing should be included in operational resilience management information and reporting.

If an event has materialised and caused an impact to the delivery of a key business service, this should be reported in the context to the impact tolerance threshold to establish whether this has been breached and whether it is still appropriate to the business given its real-life response.

Setting tolerances should also recognise that a zero tolerance for disruption in a complex and connected environment would be unrealistic. Organisations need to be clear on what they consider to be the threshold for non-acceptable levels of disruption so that they can measure themselves against it.

FURTHER QUESTIONS TO CONSIDER

Business Continuity Plans

How has management developed and implemented business continuity plans that are designed to maintain the provision of a service either within impact tolerances or within current organisational capabilities? Has management identified and defined important business services and articulated the outcomes required for each?

Scenario Testing

Has management developed a range of plausible scenarios and does it test the efficacy of its continuity plans in maintaining services within its impact tolerances? Is there a consideration of intelligence (such as emerging risks, near misses, previous incidents within the business, local and global industry) in developing the scenarios? Are the scenario testing plans for each scenario commensurate? Are the root causes of failed tests being addressed?

While scenarios should be severe, it would be unreasonable to expect the organisation to withstand the most extreme forms of disruption.

Incident response

How has management designed its methodology and playbook for responding to disruptive events such as cyber-attack or data protection breach?

Lessons Learned

How does management capture and assess lessons learned from scenario testing and develop strategies for closing identified gaps? This is likely to have been brought to the forefront through responses to the Covid-19 crisis. The crisis is likely to have highlighted shortcomings in the way many organisations have historically set and tested scenarios as part of their business continuity arrangements.

Digitisation

How has management assessed the extent of manual processes across the organisation and identified opportunities for automation? Again, this is likely to have been accelerated because of Covid-19, given the levels of remote working practices that have been introduced.

Governance

Does the organisation have appropriate arrangements in place, including the following?

- An effective and sustainable governance strategy to address operational resilience (and is this aligned to the business strategy)
- Adequate oversight and monitoring of the resilience risk appetite and investment decisions
- Sufficient and appropriate testing of its response to a disruptive event
- Relevant and adequate management information (both quantitative and qualitative) that flows up through committees to the Board. Good quality management information should enable a Board to measure and monitor the key drivers of operational resilience and have appropriate oversight over the business' performance against risk appetite.
- A set of Key Risk Indicators linked to the drivers of operational resilience and operational availability
- Whether the organisation's risk appetite statement gives recognition to operational disruption as a key risk and quantifies the amount of disruption that could be tolerated in the event of an incident
- Is the risk appetite statement sufficiently clear, and does it include metrics/limits that are subject to an annual review by the Board
- An aligned and integrated framework for the management of operational resilience within the enterprise wide risk management framework
- Allocated roles and responsibilities for managing and reporting on operational resilience, particularly those between the 1st and 2nd lines of defence.

IN CONCLUSION

As we noted in our first paper, achieving operational resilience is non-negotiable. It is also far-reaching and complex, and for many organisations, assessing what they need to do and how to do this is very much a work-in-progress.

This presents a challenge and opportunity for internal audit to provide appropriately balanced and valued advisory and assurance support as their organisations seek to embed a fit-for-purpose framework, policies and processes that will achieve the desired outcomes.

© ICAEW 2021

All rights reserved.
If you want to reproduce or redistribute any of the material in this publication, you should first get ICAEW's permission in writing.
ICAEW will not be liable for any reliance you place on the information in this material.
You should seek independent advice.

Chartered accountants are talented, ethical and committed professionals. There are more than 1.8m chartered accountants and students around the world, and more than 186,500 of them are members and students of ICAEW.

ICAEW promotes inclusivity, diversity and fairness. We attract talented individuals and give them the skills and values they need to build resilient businesses, economies and societies, while ensuring our planet's resources are managed sustainably.

Founded in 1880, we have a long history of serving the public interest and we continue to work with governments, regulators and business leaders around the world. We are proud to be part of Chartered Accountants Worldwide, a global network of 750,000 members across 190 countries, which promotes the expertise and skills of chartered accountants on a global basis.

We believe that chartered accountancy can be a force for positive change. By sharing our insight, expertise and understanding we can help to create strong economies and a sustainable future for all.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)20 7920 8100
E generalenquiries@icaew.com