ICAEW KNOW-HOW
BUSINESS AND MANAGEMENT FACULTY

A GUIDE TO OPERATIONAL RESILIENCE

GUIDE

8 February 2021

Operational resilience is now a hot topic for all industries. The Covid-19 crisis has forced many organisations to assess their resilience ‘on the fly’. They are assessing how better to achieve resilience as a result of lessons learned during crisis, particularly those that lacked a structured approach to developing and embedding a resilience framework.

It’s also now clear that operational resilience is much more than having a business continuity plan in place. In this paper, we explore what organisations need to do to design and embed a framework to deliver operational resilience. This will be followed by guidance on how to audit operational resilience.

SETTING CONTEXT

Now more than ever, achieving operational resilience is accepted as a strategic goal for all organisations, irrespective of size, complexity, industry or sector. Operational disruption can impact stability within an industry, threaten the viability of individual organisations, or cause harm to consumers and other market participants.

Even before the Covid-19 crisis, high-profile disruptive events showed that the speed and effectiveness of communications with the people most affected, in particular customers, is crucial for a ‘successful’ response to operational disruption.

The Covid-19 crisis has now brought operational resilience into even sharper focus. It has triggered the need to better understand what it means to be operationally resilient. This includes analysing lessons learned and what further changes are needed as we move to the ‘new normal’.

For example, organisations may have learned they were overly-reliant on manual processes or had greater vulnerability to a non-resilient supply chain than originally thought. They may have struggled with plant availability or completing essential maintenance or inspection programmes which may have then impacted the delivery of critical services.

These are likely to drive the need for greater automation and accelerate or even initiate a digitalisation program. Cyber-threats and the pressure to maintain data and system security are also key drivers for stronger resilience.

Regulators are also taking a strong interest in operational resilience. This is particularly so within financial services, where the regulators have already issued consultation papers and guidance which set clear expectations on how regulated firms should respond to this challenge.

IS YOUR ORGANISATION DEMONSTRATING OPERATIONAL RESILIENCE?

Organisations need arrangements in place to prevent, respond and recover from disruption within their agreed risk appetite. Before we get into operational resilience, for many organisations, this means revisiting their risk appetite statements and metrics.

Experience tells us that many organisations have not sufficiently articulated their appetite for risk. Where statements are made, they are not always linked strategy, appropriately embedded across risk frameworks (however simple those frameworks may be) and not consistently understood and applied across the organisation.

Similarly, there will be a need for organisations to define and articulate what it what it means to be operationally resilient and how they aim to achieve this. This will need management to determine what activities currently contribute to resilience and what additional steps are needed to achieve the desired outcome. It's about understanding what needs to work and the implication of things not working such that resilience matches the potential business impact.

DEVELOPING AN APPROACH

Organisations need an approach to manage operational resilience that includes preventative measures and the capabilities – in terms of people, processes and organisational culture – to adapt and recover when things go wrong. This includes the need to define and manage operational resilience within the context of their existing risk management frameworks, in particular operational risk management, business continuity and disaster recovery arrangements. Management should assume that disruption will happen, and so need measures to remedy/keep a service running.

The financial services regulators view operational resilience much more from an external perspective; that is ensuring that business services can be maintained to avoid significant harm to consumers and markets. This is a move away from the more traditional approach that focusses on systems and processes. In some respects, how an organisation achieves resilience is less relevant – it is the ability to respond effectively to a disruptive event that matters.

To achieve this, organisations need a broad approach that addresses how the continuity of key services they provide can be maintained regardless of the cause of disruption.

BUILDING AND DELIVERING RESILIENT BUSINESS SERVICES

To build and deliver resilient business services, organisations need to:

- Prevent disruption occurring, as far as possible
- Adapt systems and processes to continue to provide services in the event of a disruptive incident
- A prompt return to business as usual (or a revised version of this) when the disruption is over
- Learn and evolve from both incidents and near misses
- Maintain effective communication with affected stakeholders, in particular the customer base.

These objectives should hold true for most, if not all businesses. Demonstrating that an organisation is operationally resilient is much more than assessing the robustness of its business continuity and disaster recovery plans. While this was an important element of an effective response to Covid-19, many organisations now see that their plans were not as robust as originally thought.

Many plans had not envisaged a fully remote working response to a pandemic and had not 'played out' this scenarios in sufficient detail. Greater consideration of higher impact, lower likelihood scenarios is also needed. While these elements are clearly key, there are more which need to be working well to deliver an integrated and effective approach.

Conversely, organisations should keep an eye out for 'complacency' around operational resilience. For some, the impact and response to the crisis looks to have been well managed. However, a pandemic is only one scenario and there is plenty more management needs to do to meet regulatory requirements in this area.

THE KEY ELEMENTS OF AN OPERATIONAL RESILIENCE FRAMEWORK

To deliver operational resilience, organisations need to ensure they have a number of supporting elements in place and these will include:

- 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
- Risk Management, Compliance and Audit oversight and assurance.

If any of these elements are missing or ineffective, it can significantly undermine an organisation’s ability to recover from a significant disruptive event. Furthermore, understanding and managing the interconnections between the framework elements is critical to embedding a framework that can deliver the desired outcomes.

RELEVANT STANDARDS, GUIDANCE AND GOOD PRACTICES

Management should be considering and adopting relevant standards, guidance and good practices. For example, drawing on the consultation papers and guidance from the financial services regulators, international management standards such as business continuity (ISO 22301) and information security (BS7799 and ISO27001).

MANAGEMENT INFORMATION

Organisations will need to enhance and develop their management information to provide senior management and the Board with oversight of the robustness of the organisation’s operational resilience capabilities. This should typically include:

- A focus on quality not quantity
- Highlighting key issues and trends
- Measuring activity against targets
- Drawing information and data from a range of sources
- Ongoing assessment of the probability of disruption and its potential impact.

THE CHALLENGE AND OPPORTUNITY FOR INTERNAL AUDIT

The above poses a challenge for internal audit as it seeks to provide assurance in this complex area. We will shortly issue a paper providing guidance on how to assess the threats to operational resilience and how to develop an effective audit approach that reflects the relative levels of maturity across an organisation’s framework for defining, measuring and managing risks related to this.

Given the far reaching aspects of resilience and the different ways it can be approached, the paper will be principles based rather than attempting to provide a ‘one-size fits all’ detailed audit approach and review programme.

Despite being technically demanding subject, this is an opportunity for internal audit to be ‘on the front foot’. Operational resilience practices are evolving and many organisations are at a relatively early stage of design and embedding a fit for purpose approach and framework.

In this respect, a technically aware and skilled internal audit function can 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.

Given the depth and breadth of internal audit's skills and its deep understanding of the organisation's business and risk management practices, internal audit can also advise on how to leverage existing business continuity and disaster recovery plans as a basis for creating an operational resilience framework.

IN SUMMARY

Achieving operational resilience is now non-negotiable. It 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.

A successful outcome is dependent on a number of interconnected activities and this is a real challenge as organisations seek to embed a framework, policies and procedures that will achieve the desired outcome in a proportionate, coordinated and cost-effective way.

ICAEW will not be liable for any reliance you place on the information in this material.
You should seek independent advice.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

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