The Road to Resiliency

Building a Robust Audit Plan for Operational Resilience
# Contents

**Executive Summary** 2

- Defining Operational Resilience 3
- Objective 3

**The Evolution of Operational Resilience** 4

- The Financial Industry Response 4

**A Comprehensive Resilience Assurance Strategy** 6

- Resiliency Governance 7
  - Assessing Critical Business Services and Related Metrics 7
  - Defining Impact Tolerance 8
- Foundational Audits 8
  - Cyber Resilience Audit 8
  - Vendor and Third-Party Resilience Audit 8
  - Standalone Resilience Audit 9
  - Integrating Resilience Assurance into Business/IT Audits 10
  - Firmwide and Sectorwide Testing 10

**Conclusion** 11
Executive Summary

The financial services industry has long relied on internal audit functions to assess and challenge the effectiveness of various programmes designed to protect and build organisational value. These programmes have included disaster recovery, business continuity, risk management, cybersecurity, and many others designed to help institutions recover from an event.

However, with rapid technology development and globalisation, internal audit functions are having to evolve and adapt to emerging business risks and regulatory expectations. Regulators expect and, in many cases, are demanding that firms and financial market infrastructures (FMIs) demonstrate greater resilience, while organisations, management and boards are under increased pressure to build out more robust resilience-focused programmes. The pressure comes amid fears that operational disruptions to the products and services organisations provide have the potential to harm consumers and market participants, threaten the viability of these entities, and create instability in the financial markets. A string of large-scale technology outages and cybersecurity attacks in recent years has exposed systemic vulnerabilities and intensified regulators’ concerns.

Consequently, financial institutions (FIs) are seeking assurance strategies that can evaluate all the various crisis and disaster management disciplines holistically and align them with their overall resilience objectives. Indeed, FIs recognise the need to develop formalised processes and capabilities that would enable them to continue to provide services when faced with extreme but plausible events.

Given the emerging nature and complexity of operational resilience, there is growing urgency for internal audit to play a bigger role in providing assurance that the governance, risk management and controls that are being created to enhance resilience capabilities are adequate. This changing dynamic also provides an opportunity for internal audit to develop a flexible and comprehensive approach that not only targets all aspects of a resilience programme but can also be incorporated into existing business and IT audits.
DEFINING OPERATIONAL RESILIENCE

Not a new concept, but one that is receiving scrutiny from regulators and leaders alike, operational resilience is defined as an organisation’s ability to detect, prevent, respond to, and recover and learn from operational and technological failures which may impact the delivery of critical business and economic functions or underlying business services. The concept of operational resilience is evolving as firms expand programmes and capabilities to address a broad range of threats that could cause business failures, systemic risks, and economic impacts.

Building the resiliency of the financial industry is a collective responsibility of FIs, regulators, key sector utilities, and industry associations. Within each organisation, operational resilience calls for stakeholders to promote a culture of resiliency through oversight, training and awareness, communications and board reporting. The key components of operational resilience, which include defining and understanding critical business services, impact tolerance and economic impact, are essential guideposts on the road to resiliency. And, vitally important is the role internal audit plays in assessing these various components, providing assurance that stakeholders are addressing the key risks identified.

Working in concert with leading financial industry groups and individual institutions, Protiviti’s internal audit experts are expanding existing programs to incorporate more comprehensive assurance over operational resilience. The revised resiliency audit approach addresses governance structures from an operational resilience perspective and provides coverage of all the foundational elements (e.g., cybersecurity, disaster recovery, business continuity planning, and vendor risk management) within business-as-usual audits, and front-to-back resiliency processes.

OBJECTIVE

This white paper outlines leading practices for providing comprehensive assurance over operational resilience programmes, explains key resiliency concepts, and identifies critical questions every chief audit executive should ask concerning resilience assurance.
As previously mentioned, operational resilience is not a new concept and there are multiple existing regulations and guidances aimed at promoting resilience. The concept, however, gained prominence last year after the Bank of England (BoE), the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) jointly released a discussion paper titled *Building the U.K. Financial Sector’s Operational Resilience (U.K. discussion paper)*, published in response to technology outages and major cyberattacks impacting the financial sector.

In the U.K. discussion paper, regulators sought feedback on how financial institutions and FMIs can maintain the continuity of services regardless of the cause of a major disruption. They raised questions about how the financial industry can develop an approach to operational risk management which includes preventative measures and capabilities (encompassing people, processes and organisational culture) and to help firms adapt and recover when things go wrong.

The European Banking Authority also issued revised guidance in February of 2019 on outsourcing arrangements, clarifying management’s role and a financial institution’s responsibility to ensure that outsourced services, particularly those deemed to be critical or important functions, comply with EU legislation and regulatory requirements. Subsequently, in March 2019, the Monetary Authority of Singapore (MAS) released two consultation papers proposing changes to its technology risk management and business continuity guidelines. The MAS consultation papers set forth enhanced measures that FIs can adopt to strengthen operational resilience, factoring in the rapidly changing physical and cyber threat landscape.

**THE FINANCIAL INDUSTRY RESPONSE**

FIs and FMIs increasingly recognise the need to improve response capabilities against major operational disruptions. Indeed, many leading firms are reexamining how they view and manage critical business services or functions, economic impact, impact tolerance and other critical aspects of an operational resiliency culture.

Collectively, the financial services industry has been consolidating its viewpoints on operational resilience as part of an effort to develop guidance that firms can incorporate to build an operational resilience culture. To date, the Global Financial Markets Association (GFMA), its member firms and associated organisations, have been particularly proactive on this front, working in cooperation with regulators around the world. In addition, as part of this exercise, the industry is developing a common lexicon that financial firms and regulators can use to facilitate discussions on the topic of operational resilience.

Through its partnership with leading financial trade organisations, Protiviti is playing a critical role in further developing and formalising the industry’s perspective on the topic of operational resilience. In addition, Protiviti is developing a framework that firms can leverage to understand, prevent, and recover from extreme but plausible events. Specifically, the framework identifies key components firms must consider when formalising and managing the resilience of their critical business services.
The components of Protiviti’s operational resilience framework include analysing existing business services to determine criticality; developing and reviewing resilience programme governance functions; establishing and monitoring impact tolerance; testing scenarios to better understand realistic recovery times versus established impact tolerance; defining economic impact; and improving the viability of the foundational elements to support resilience objectives.

Most importantly, the operational resilience framework is designed to be collaborative, with all the key stakeholders working together to strengthen firms’ ability to respond to an extreme but plausible event while continuing to deliver business services. The table below illustrates Protiviti’s operational resilience framework.

### Protiviti’s Operational Resilience Framework

<table>
<thead>
<tr>
<th>How is operational resilience governed effectively within the organisation?</th>
<th>RESILIENCE PROGRAMME GOVERNANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration</td>
<td>Enterprise Orchestration</td>
</tr>
<tr>
<td>Oversight</td>
<td>Sector Coordination</td>
</tr>
<tr>
<td>External Communications</td>
<td>Training &amp; Awareness</td>
</tr>
<tr>
<td>Board Reporting</td>
<td>Crisis Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What business services are critical? To what extent can they be interrupted?</th>
<th>BUSINESS SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define &amp; Prioritise Critical Business Services</td>
<td>Establish &amp; Monitor Impact Tolerances</td>
</tr>
<tr>
<td>Define Economic Impact</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Are the proper foundational elements in place and mature enough to support resilience objectives?</th>
<th>FOUNDATIONAL ELEMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Resilience</td>
<td>Cyber Resilience</td>
</tr>
<tr>
<td>Third-Party Resilience</td>
<td>Technology Resilience</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Can the organisation demonstrate resilience through substantive testing of extreme but plausible scenarios?</th>
<th>ASSURANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess</td>
<td>Mature</td>
</tr>
<tr>
<td>Orchestrate</td>
<td>Assure</td>
</tr>
<tr>
<td>Evolve</td>
<td>Recurring Testing Scenarios</td>
</tr>
</tbody>
</table>
The development of internal audit plans designed to test the various components of operational resilience is a critical aspect of Protiviti's comprehensive operational resilience framework. The resilience assurance process targets all aspects of a resilience programme and considers both business and technical audits. It includes a process for performing standalone resilience audits, which involve assessing the standards used in defining critical business services, impact tolerance and economic impact, structures or controls to govern resilience, and testing mechanisms for extreme but plausible scenarios. The strategy includes integrating resilience assurance into existing business and IT audits as well as performing firmwide and sectorwide testing activities for the purpose of gathering critical information.

The table below provides a summary of the key components of the resilience assurance strategy.

### Key Components of a Protiviti’s Comprehensive Operational Resilience Assurance Strategy

**SPONSORS**
- Executive Leadership
- Board/Audit Committee

**STAKEHOLDERS**
- Chief Operating Officer
- Resiliency Officer
- Chief Risk Officer
- Chief Information Officer/Chief Technology Officer
- Chief Information Security Officer
- Business Continuity
- LOB Leadership (for Critical Business Services)

**AUDIT SCOPING CONSIDERATIONS**
- Is a structure in place to properly govern resilience across the enterprise?
- How has the organisation defined and approached resiliency?
- Has the organisation formally defined criticality of business services?
- Are impact tolerances established and tested?
- Are “front-to-back” mappings of the components of business services understood and maintained?
- Are "extreme but plausible" scenarios tested regularly?

<table>
<thead>
<tr>
<th>Audit Channels</th>
<th>Resiliency Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foundational Audits (e.g., Cybersecurity, Business, Infrastructure, Third-Party)</td>
<td></td>
</tr>
<tr>
<td>Standalone Resilience Audit (e.g., front-to-back business service)</td>
<td></td>
</tr>
<tr>
<td>Integration into All Standard Business/IT Audits</td>
<td></td>
</tr>
<tr>
<td>Participation in Firm/Sectorwide Testing Activities</td>
<td></td>
</tr>
</tbody>
</table>
The comprehensive resilience auditing approach puts the onus on internal auditors to develop a front-to-back understanding of companies’ internal operations, third-party dependencies, the sector and industry to effectively analyse processes and risks, and identify key controls.

RESILIENCY GOVERNANCE

A robust internal audit plan includes auditing the design and operating effectiveness of internal governance structures created to support the resiliency programme.

Given there is no single right way to establish operational resilience governance, the audit should assess whether the aims and outcomes of the governance structures are consistent.

This exercise may involve:

• Assessing whether an effective resiliency framework is in place and communicated across the organisation, with clear roles, responsibilities and accountability for achieving and maintaining resilience.

• Confirming alignment of business strategies with the operational resilience strategy.

• Evaluating whether adequate oversight and monitoring against the resilience risk appetite exist to drive risk and investment decisions.

• Testing the enterprise orchestration response structure to a resilience event, particularly all management information that flows up through the committees.

As FIs create new roles and functions to handle resilience matters, internal audit would need to understand and test the effectiveness of those governance structures. For instance, some FIs have established enterprise resilience functions, comprising several roles that report directly to an executive-level business risk committee. In other cases, firms have appointed a resiliency officer who is tasked with monitoring individual business governance processes and driving consistency across the organisation.

Some organisations have resilience steering committees focused on regulatory matters related to their critical business services and responsible for providing regular reports to the board. Regardless of governance structure, internal audit would need to understand the different models and be able to evaluate the effectiveness and sustainability of a specific structure to address operational resilience.

Assessing Critical Business Services and Related Metrics

The resilience assurance strategy involves challenging the veracity of established definitions for critical business services and functions, as well as economic impact. As part of this exercise, internal audit would review internal, external and substitutability metrics as well as the process of determining criticality, which includes assessing whether it is repeatable and documented. The review should also challenge the definition, applicability and completeness of the following defined metrics:

• The percentage of overall revenue supported by a business service.

• The estimated daily impact of business service event on customers.

• The number of market participants providing a business service.

• The regulatory exposure due to an outage or resilience event.

• The length of time service can operate under a transfer scenario.
Finally, as part of the broader operational resilience audit, internal audit would scrutinise the organisation’s view on economic impact or, specifically, the total potential market impact of a disruptive event on these key stakeholders: the company, customers, financial sector, and the general public. The goal of this audit is to assess whether the organisation and its management has a clear understanding of the potential impact of an extreme but plausible event on service lines within the organisation, other external institutions and the sector as a whole.

**Defining Impact Tolerance**

The term “impact tolerance” is new to the industry, although the concept of tolerating service interruption is familiar. Under the comprehensive resilience assurance approach, internal audit would test established impact tolerances, analyse how they were determined and whether all appropriate measures are in place so the tolerance threshold will not be exceeded. This evaluation would cover the following viewpoints:

- Is the tolerance threshold at a level where the business can survive an event without triggering a scenario such as recovery and resolution planning?
- What is the tolerance of customers to accept the operational resilience event and continue services with the institution?
- What are the expectations of regulators and how would they respond to an incident?
- Will an institution close a critical business, and in what situations?

**FOUNDATIONAL AUDITS**

Internal audit functions are increasingly moving towards horizontal or programmatic reviews of the different processes or components related to operational resilience. A comprehensive assurance audit would focus on the foundational elements, namely business resilience, cyber resilience, third-party resilience and technology resilience, with an emphasis on extreme but plausible scenarios. The key question internal auditors seek to address is: Are the proper foundational elements in place and mature enough to support the resilience objectives of the organisation?

**Cyber Resilience Audit**

A traditional cyber resilience audit involves evaluating key aspects of a company’s ability to identify, monitor, contain and respond to a cyberattack. Under a comprehensive resilience audit approach, internal audit would assess whether an organisation’s cybersecurity practices and procedures align with its resiliency objectives.

Regulatory guidelines or industry frameworks can also be used to assess a cyber programme. For instance, assessing compliance with the G7 Fundamental Elements of Cybersecurity for the Financial Sector would include evaluating the organisation’s ability to identify activities, products and services — including interconnections, dependencies, and third parties — and whether it is able to fully assess and prioritise their respective cyber risks.

All implemented controls — including systems, policies, procedures and training — designed to protect against and manage cyber risks would be covered under a comprehensive cyber resilience audit.

**Vendor and Third-Party Resilience Audit**

The resiliency of third-party vendors that are involved in the delivery of business services to financial institutions can be enhanced by establishing third-party governance and risk management practices. Under the comprehensive resilience audit approach, internal audit would assess third-party risk programmes, processes and controls used for vendor risks, guidelines or controls for conducting due diligence, vendor selection, onboarding and monitoring. The third-party resilience audit would focus on whether the programmes support end-to-end critical business services.
The following are considerations to be included in a third-party resiliency risk audit:

- Contract management processes used by management to track third-party relationships.
- Monitoring of regulatory developments related to third parties.
- Consistency and enforcement of right-to-audit clauses.
- Enforcement of third-party compliance with the company’s information security standards.
- The development, implementation, and calibration of a continuous monitoring system of self-reported data from third-party business partners.
- The consistency of and ability to enforce exit clauses.
- The inclusion of third parties in resilience exercises.
- Clarity of roles and responsibilities and escalation processes.

**Standalone Resilience Audit**

Following a resilience governance audit, and after a firm has identified its lists of critical business services, a standalone resilience audit of individual business services may be conducted.

Take, for example, the retail banking unit of a global bank. The standalone resilience audit would involve assessing and providing an opinion on the process followed to determine the criticality of the retail business, with a focus on metrics such as the percentage of overall revenue driven by the unit and the estimated daily impact of a potential outage on customers. An impact tolerance audit would challenge the established impact resilience threshold for the retail business versus its established recovery time objective. Also, the metrics around the substitutability of retail business services during an outage (e.g., the time to transfer services) would be assessed.
Integrating Resilience Assurance into Business/IT Audits

Internal audit should build resilience components into existing business as usual (BAU) audits. Incremental additions to BAU audits will enable internal audit to develop detailed insights into an institution’s resiliency capabilities. For example, if conducting a payments audit, internal audit would obtain and assess important information such as which other business services are related to payments; whether payments should be considered a critical business service; which impact tolerances have been defined for this business service; and whether the business would be able to recover if an extreme but plausible event occurs.

Firmwide and Sectorwide Testing

Testing and auditing protocols provide essential assurance mechanisms for entities and public authorities alike. Although not an internal audit-driven activity, it is important for internal audit to understand an organisation’s level of participation in firmwide and sectorwide testing, the results of the test, and how they drive the overall operational resilience strategy. Testing exercises also provide an opportunity for internal audit to review the readiness of communication plans for internal and external stakeholders in the event of a disruption. Sectorwide events such as Quantum Dawn provide internal audit with a critical perspective on leading practices across the industry and potential opportunities to collaborate with industry associations.

Five Questions CAEs Should Ask About Resilience Assurance

01. How do we as an organisation approach operational resilience and how engaged are the board and executives in the operational resilience programme and the establishment of the resiliency strategy or objectives?

02. Has our organisation clearly defined and articulated its critical business services, as well as the impact tolerances for those services?

03. Do we have a process of testing our ability to withstand and respond to extreme but plausible events?

04. Is there a clear understanding of our organisation’s dependencies on third-party vendors and the level of risk that is introduced by these entities into critical business services?

05. Does our team have visibility into the foundational elements of the organisation, including business resilience, cyber resilience, third-party resilience and technology resilience?
Conclusion

As the financial industry adapts to an environment of heightened risks and technological changes, internal audit functions are expected to move towards more targeted, risk-focused reviews of all processes and components related to operational resilience. The resilience assurance strategies allow firms to meet their operational resilience objectives and satisfy growing regulatory concerns.

Incorporating a comprehensive resilience assurance approach into existing governance and foundational element audits will also enable firms to develop a resiliency culture and position themselves to respond effectively to common operational disruptions as well as extreme but plausible events which could threaten the viability of their organisations, customers and financial markets.
ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

PROTIVITI GLOBAL MARKET LEADERS

ARGENTINA
Pablo Giovannelli
+54.11.5278.6345
pablo.giovannelli@protivitiglobal.com.pe

AUSTRALIA
Garran Duncan
+61.3.9948.1200
garran.duncan@protiviti.com.au

BAHRAIN
Arvind Benani
+973.1.710.0050
arvind.benani@protivitiglobal.me

BRAZIL
Raul Silva
+55.11.2198.4200
raul.silva@protivitiglobal.com.br

CANADA
David Dawson
+1.647.288.4886
david.dawson@protiviti.com

CHILE
Soraya Boada
+56.22.573.8580
soraya.boada@protivitiglobal.cl

CHINA (HONG KONG)
Albert Lee
+852.2238.0499
albert.lee@protiviti.com

CHINA (MAINLAND)
David Cheung
+86.21.5153.6900
david.cheung@protiviti.com

EGYPT
Ashraf Fahmy
+202.2586.4560
ashraf.fahmy@protivitiglobal.me

FRANCE
Bernard Drui
+33.1.42.96.22.77
drui@protiviti.fr

GERMANY
Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

INDIA
Sanjeev Agarwal
+91.124.661.8600
sanjeev.agarwal1@protivitiglobal.in

ITALY
Alberto Carnevale
+39.02.6550.6301
alberto.carnevale@protiviti.it

JAPAN
Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

KUWAIT
Sanjeev Agarwal
+965.2242.6444
kuwait@protivitiglobal.me

MEXICO
Roberto Abad
+52.55.5342.9100
roberto.abad@protivitiglobal.com.mx

NETHERLANDS
Anneke Wieling
+31.20.346.0400
anneke.wieling@protiviti.nl

OMAN
Shatha Al Maskiry
+968 24699402
shatha.maskiry@protivitiglobal.me

PERU
Marco Villacorta
+51.1.208.1070
marco.villacorta@protivitiglobal.com.pe

QATAR
Andrew North
+974.4421.5300
andrew.north@protivitiglobal.me

SAUDI ARABIA
Saad Al Sabti
+966.11.2930021
saad.alsabti@protivitiglobal.me

SINGAPORE
Nigel Robinson
+65.9169.2688
nigel.robinson@protiviti.com

UNITED ARAB EMIRATES
Arindam De
+9714.438.0660
arindam.de@protivitiglobal.me

UNITED KINGDOM
Peter Richardson
+44.20.7930.8808
peter.richardson@protiviti.co.uk

UNITED STATES
Michael Thor
+1.317.510.4685
michael.thor@protiviti.com

VENEZUELA
Gamal Perez
+58.212.418.46.46
gamal.perez@protivitiglobal.com.ve