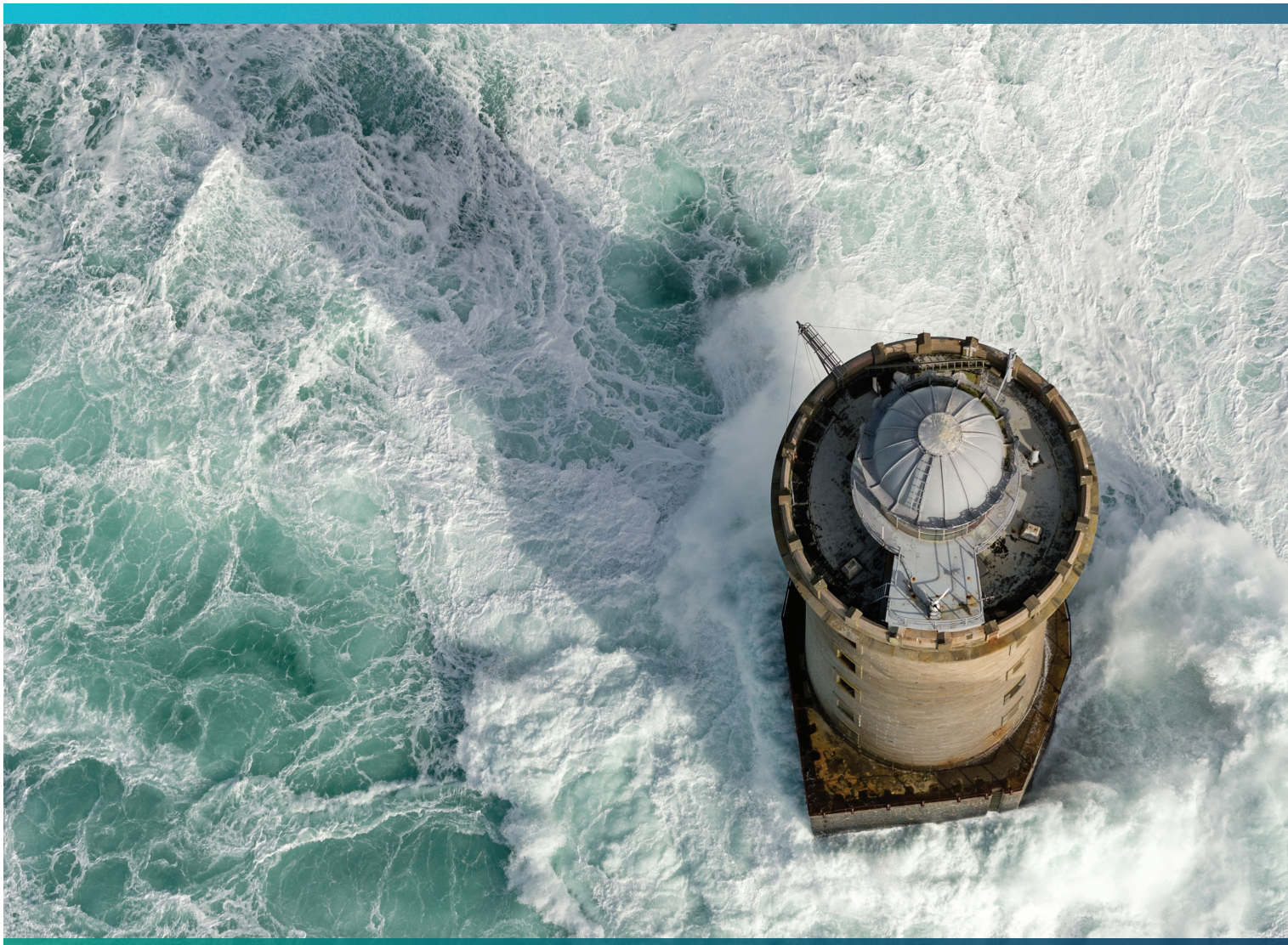
protiviti®

Face the Future with Confidence



The Road to Resiliency

Building a Robust Audit Plan for Operational Resilience

Internal Audit, Risk, Business & Technology Consulting

Contents

Executive Summary

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

The pressure comes amid fears that operational disruptions to the products and services organizations provide have the potential to harm consumers and market participants, threaten the viability of these entities, and create instability in the financial markets.

However, with rapid technology development and globalization, 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 organizations, management and boards are under increased pressure to build out more robust resilience-focused programs. The pressure comes amid fears that operational disruptions to the products and services organizations 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 recognize the need to develop formalized 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 program but can 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 organization's ability to detect, prevent, respond, recover and learn from operational and technological failures that may impact delivery of critical business and economic functions or underlying business services. The concept of operational resilience is evolving as firms expand programs and capabilities to address a broad range of threats that could cause business failures, systemic risk, 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 organization, 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 a 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 programs, explains key resiliency concepts, and identifies critical questions every chief audit executive should ask concerning resilience assurance.

The Evolution of Operational Resilience

As previously mentioned, operational resilience is not a new concept and there are multiple existing regulations and guidance 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[1] 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 that includes preventative measures and capabilities — people, processes and organizational culture — to adapt and recover when things go wrong.

The European Banking Authority also issued revised guidance in February of 2019[2] 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[3] and business continuity[4] 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 recognize 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 organizations, 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 organizations, Protiviti is playing a critical role in further developing and formalizing 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 formalizing and managing the resilience of their critical business services.

[1] BOE Discussion Paper: www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A.

[2] EBA Guidelines on Outsourcing: https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.

[3] www.mas.gov.sg/-/media/Consultation-Paper-on-Proposed-Revisions-to-Technology-Risk-Management-Guidelines.pdf.

[4] www.mas.gov.sg/news/media-releases/2019/mas-consults-on-proposed-enhancements-to-trm-and-bcm-guidelines.

The components of Protiviti's operational resilience framework include analyzing existing business services to determine criticality; developing and reviewing resilience program 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 important, 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

How is operational resilience governed effectively within the organization?	**RESILIENCE PROGRAM GOVERNANCE**	• Collaboration • Oversight • External Communications • Board Reporting • Enterprise Orchestration • Sector Coordination • Training & Awareness • Crisis Management
What business services are critical? To what extent can they be interrupted?	**BUSINESS SERVICES**	• Define & Prioritize Critical Business Services • Establish & Monitor Impact Tolerances • Define Economic Impact
Are the proper foundational elements in place and mature enough to support resilience objectives?	**FOUNDATIONAL ELEMENTS**	Business Resilience; Cyber Resilience; Third-Party Resilience; Technology Resilience
Can the organization demonstrate resilience through substantive testing of extreme but plausible scenarios?	**ASSURANCE**	Assess → Mature → Orchestrate → Assure → Evolve Recurring Testing Scenarios

A Comprehensive Resilience Assurance Strategy

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 program 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 purposes 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 structure in place to properly govern resilience across the enterprise?
- How has the organization defined and approached resiliency?
- Has the organization formally defined criticality of business services?
- Are impact tolerances established and tested?
- Are "front-to-back" mappings of components of business services understood and maintained?
- Are "extreme but plausible" scenarios tested regularly?

Audit Channels
Resiliency Governance
Foundational Audits (e.g., Cybersecurity, Business, Infrastructure, Third-Party)
Standalone Resilience Audit (e.g., front-to-back business service)
Integration into All Standard Business/IT Audits
Participation in Firm/Sectorwide Testing Activities

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 analyze 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 program.

Given there is no single right way to establish operational resilience governance, the audit would 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 organization, 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 organization.

Some organizations 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 business service.
- Estimated daily impact of business service event on customers.
- Number of market participants providing business service.
- Regulatory exposure under outage of resilience event.
- Length of time service can operate under transfer scenario.

Finally, as part of the broader operational resilience audit, internal audit would scrutinize the organization'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 organization and its management has a clear understanding of the potential impact of an extreme but plausible event on service lines within the organization, 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, analyze 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 the 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 organization?

Cyber Resilience Audit

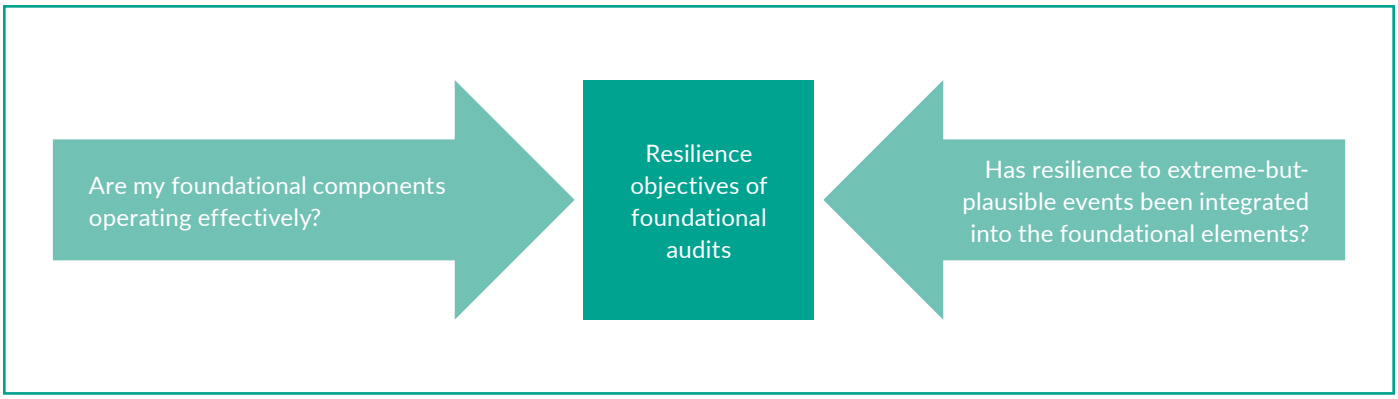
A traditional cyber resilience audit involves evaluating key aspects of a company's ability to identify, monitor, contain and respond to a cyberattack. Under a comprehensive resilience audit approach, internal audit would assess whether an organization's cybersecurity practices and procedures align with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

Regulatory guidelines or industry frameworks can also be used to assess a cyber program. For instance, assessing compliance with the G7 Fundamental Elements of Cybersecurity for the Financial Sector would include evaluating the organization's ability to identify activities, products and services — including interconnections, dependencies, and third parties — and whether it is able to fully assess and prioritize 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 programs, 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 programs 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 company's information security standards.
- Development, implementation, and calibration of a continuous monitoring system of self-reported data from third-party business partners.
- Consistency and ability to enforce exit clauses.
- 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 estimated daily impact of a potential outage on customers. An impact tolerance audit will 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., time to transfer service) will 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 what other business services are related to payments; is payments a critical business service, what are the impact tolerances that have been defined for this business services, and is the business 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 organization'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 would provide internal audit 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 organization approach operational resilience and how engaged are the board and executives in the operational resilience program and establishment of the resiliency strategy or objectives?
02	Has our organization 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 organization'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 foundational elements of the organization, 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 will 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 that could threaten the viability of their organizations, 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.

CONTACTS

Michael Thor (US)
Managing Director, IAFA-IT Audit
michael.thor@protiviti.com

Carl Hatfield (US)
Managing Director, IAFA-IT Audit
carl.hatfield@protiviti.com

Laura Moore (UK)
Associate Director, Risk & Compliance
laura.moore@protiviti.co.uk

Ron Lefferts (US)
Managing Director, Global Leader,
Protiviti Technology Consulting
ron.lefferts@protiviti.com

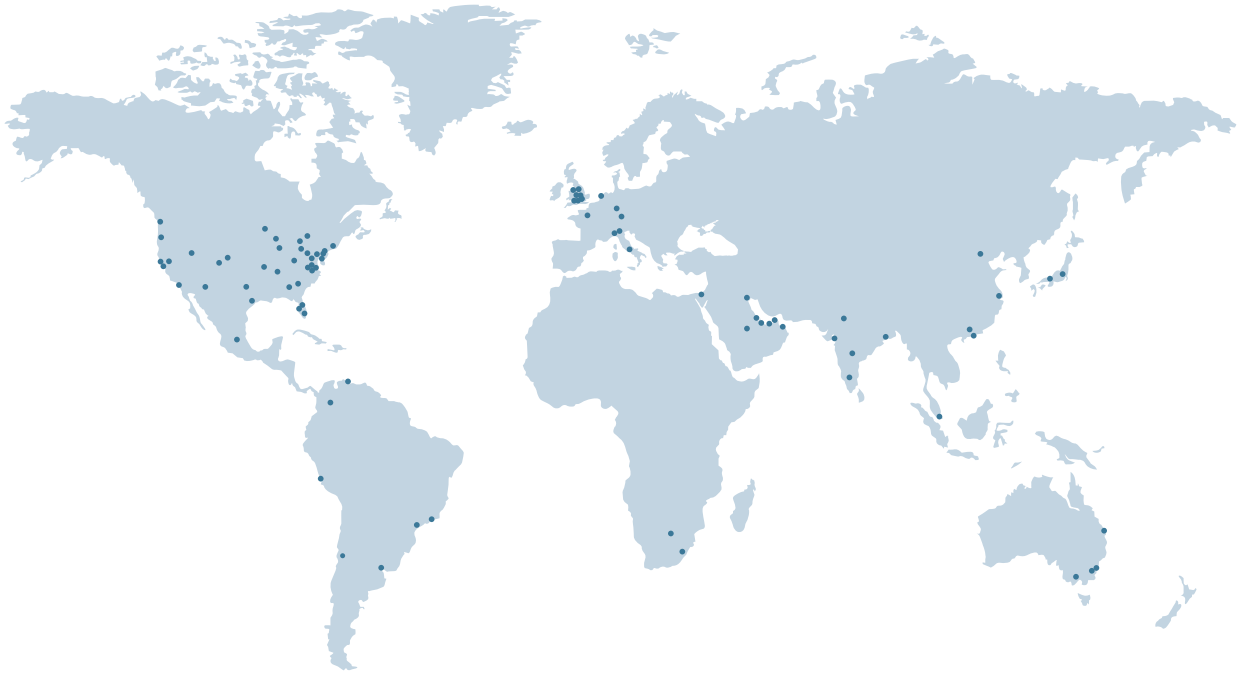
Andrew Retrum (US)
Managing Director, Global Operational Resilience Leader,
Technology Consulting
andrew.retrum@protiviti.com

Douglas Wilbert (US)
Managing Director, US Operational Resilience Leader,
Risk & Compliance
douglas.wilbert@protiviti.com

Bernadine Reese (UK)
Managing Director, UK Operational Resilience Leader,
Risk & Compliance
bernadine.reese@protiviti.co.uk

Thomas Lemon (UK)
Managing Director, UK Operational Resilience Leader,
Technology Consulting
thomas.lemon@protiviti.co.uk

Kim Bozzella (US)
Managing Director,
Technology Consulting Financial Services Industry Leader
kim.bozzella@protiviti.com



THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
Sao Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

COLOMBIA*

Bogota

MEXICO*

Mexico City

PERU*

Lima

VENEZUELA*

Caracas

EUROPE, MIDDLE EAST & AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

NETHERLANDS

Amsterdam

SWITZERLAND

Zurich

UNITED KINGDOM

Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

SAUDI ARABIA*

Riyadh

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

EGYPT*

Cairo

SOUTH AFRICA *

Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Sydney

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*

Bengaluru
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

*MEMBER FIRM

protiviti®