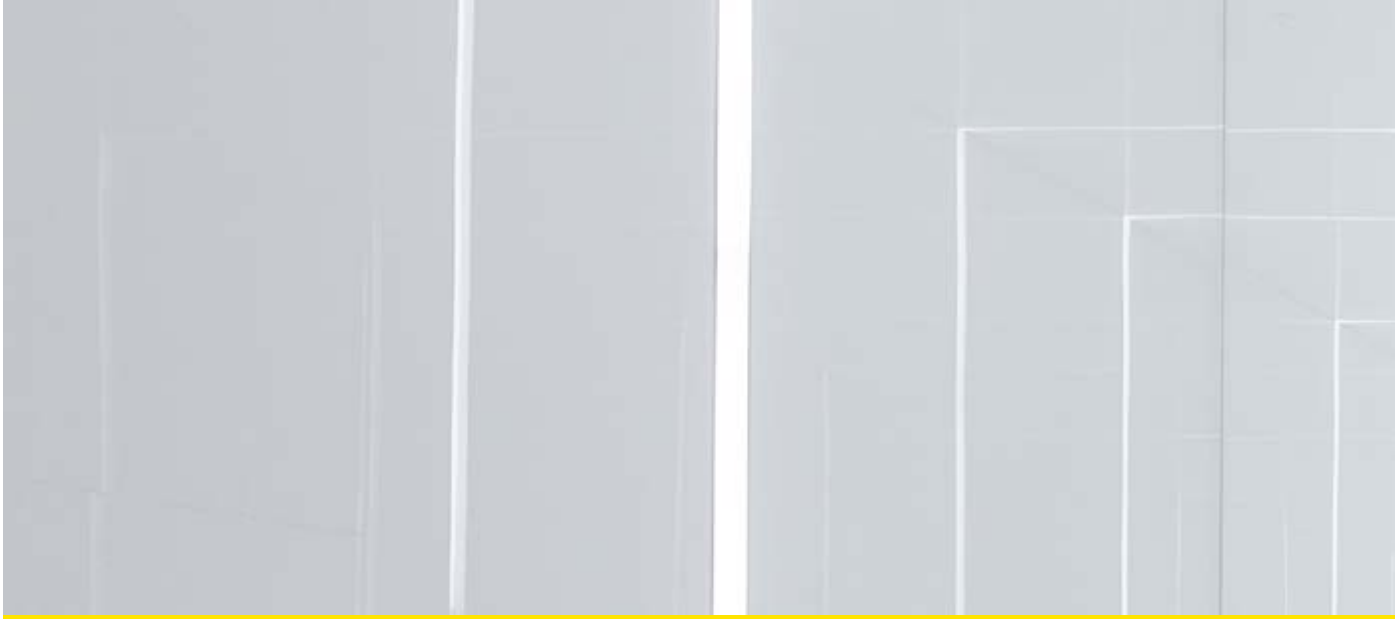
Getting serious about resilience: a multiyear journey ahead

EY
Building a better working world



Resiliency and its impact on the enterprise have shot up the financial services board agendas over the past two years. Boards of directors and senior management are now heavily focused on reducing the probability and impact of disruptions to business, as well as on how to deliver services continuously when such interruptions occur. They also want to know that their firms foster a learning culture, such that resiliency plans are improved upon after near misses or actual incidents. Regulators have also stepped up their focus on resilience and firms' ability to deliver uninterrupted business services because customers demand this level of service convenience.

In recent months, EY professionals have engaged a broad range of financial services organizations globally in discussions about this heightened focus on operational resilience, including bringing together more than 70 firms in group dialogues across London and New York.

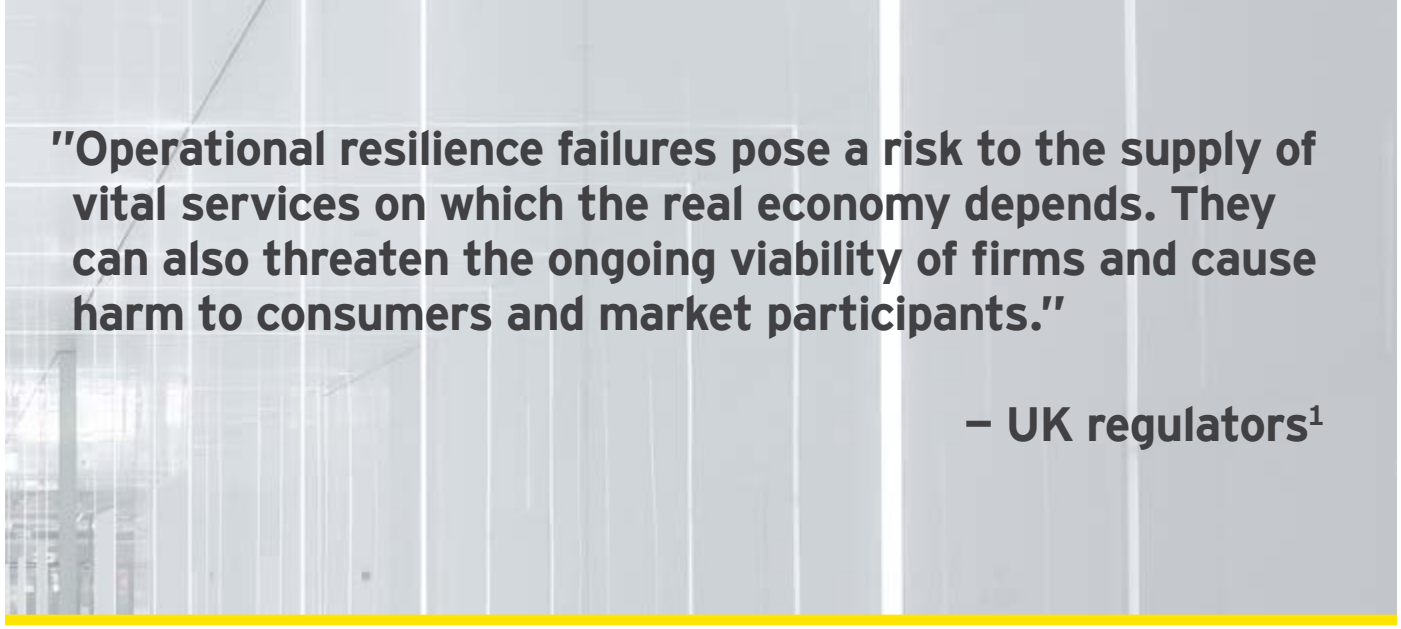
This report outlines why we believe resilience has escalated within firms and the regulatory community, and identifies 10 discrete actions firms can take immediately to better achieve operational resilience.

What's different today?

Firms have long focused on recovery. Indeed, in many cases, core regulatory standards on business continuity and disaster recovery date back 15 years or more. However, a new view of "operational resilience" is now emerging. So what's changed to bring about a different type of discussion about resilience, and how does it differ from prior discussions on continuity and recovery?

Several items stand out:

- **Cyber, cyber, cyber:** Without question, the ever-increasing threat from cyber attacks has pushed resilience atop the agendas of boards, senior management and regulatory agencies. The threat landscape seems to be increasingly more challenging and attacks much more frequent and intense.
- **Data manipulation and destruction are now part of the threat landscape:** Firms are now very aware that new threat actors are not only using ransomware to lock up data for financial gain, but some also have motives that focus on causing potential harm to the financial system. These new actors are seeking to plant malicious code that can manipulate data — sometimes through imperceptible changes — or ultimately destroy data.
- **Interconnectivity of the financial services ecosystem:** An evermore digital and online/mobile environment — and changing operating models — creates more reliance on business partners and third-, fourth- and even fifth-party vendors. In turn, this extends the financial system ecosystem and amplifies the complexity of managing within it in a resilient manner (e.g., the creation of single points of failure, the need for alternative providers or third-party outages).



"Operational resilience failures pose a risk to the supply of vital services on which the real economy depends. They can also threaten the ongoing viability of firms and cause harm to consumers and market participants."

– UK regulators[1]

- **Focus on continuous service delivery:** Customer and market demand for always-on and 24/7 access requires much higher levels of availability and reliability than ever before. Customers and clients are asking how firms will continue to serve them, even if systems are down.
- **Heightened regulatory focus on operational resilience:** Globally, regulators focused much of their attention on financial resilience in the years following the last financial crisis, and understandably so. However, high-profile operational, technological and third-party breakdowns at major financial services firms over the past few years have increased regulatory concerns about everyday operational resilience and on the capabilities of firms to protect customers and the overall functioning of markets. Regulators are now putting operational resilience on par with financial resilience.
- **IT outages are becoming more commonplace:** Globally, there has been an uptick in the number of firms experiencing outages that are causing customers or markets to be disrupted – sometimes for several days in a row. Such outages are often caused by IT or third-party outages.
- **Concerns about legacy IT have escalated:** Everyone knows that many incumbent financial services firms operate their processes on legacy IT systems – those 25- to 30-year-old mainframes come to mind. In recent years, firms have undertaken major initiatives to upgrade their IT systems to increase speed and enhance how they serve customers, to cut maintenance costs and to compete more effectively with new entrants to the market (many of which have far superior technology). However, such digital transformations are complex, expensive and risky and take years to fully implement, so the transition has been slow. Recent outages at major firms globally have shone a new light on the role legacy systems have played in creating system vulnerabilities and operational instability leading to frequent and at times severe disruptions.

Taken together, firms have concluded that the environment for operational resilience has changed materially. Even as recently as two years ago, operational resilience didn't garner so much attention. Today, it's a major issue for the industry at large – one that firms feel may take the same kind of management attention, resources and time that were applied to stress testing or recovery and resolution planning (RRP) over the past decade.

[1] "Building the UK financial sector's operational resilience," Bank of England, 2018.

10 ways to enhance firmwide resilience

Achieving greater resilience is complicated. It requires many groups across each firm — most with differing priorities and disparate reporting lines — to operate differently and more cohesively than in the past, and to do so in a more prioritized, integrated and coordinated manner. Firms' complex legal entity structures, operating model and technology environment can exacerbate this challenge.

Leveraged from dialogue with industry participants, we point to 10 important ways financial services firms can enhance firmwide resilience in an efficient, effective and urgent manner:

1

Focus on mapping and demonstrating end-to-end critical business services, beyond the firm's borders: Too often, firms map their processes by function, which constrains resilience and promotes siloed thinking and solutions. Today, there is a need to understand and manage the entire process, starting with the business service being delivered to the customer or client, then mapping applications, middleware, infrastructure, people and processes — and data flows — that support each service. Such mapping extends outside the firm to include third or fourth parties that are needed to deliver each business service.

Given the scale of many financial services firms — and the fact that not everything can exist at the same level of resilience — the key is having an evolving focus on the most critical business services. This extends beyond those core services in RRPs to services required to meet stakeholder needs day to day. Globally, regulators now want firms to consider potential financial-stability factors in identifying such processes, including factors relating to safety and soundness. Some regulators — such as those in the United Kingdom — also want potential customer harm to be considered, which could greatly expand the potential list of services deemed "critical."

2

Adopt a common resiliency language: Firms have invested much time over the past decade working toward building a common firmwide language or taxonomy. As of yet, few have achieved that fully. Most have sets of taxonomies, each one developed for a specific use case in mind: one for periodic risk-and-control-self-assessment (RCSA) processes, one for operational risk, one for RRP, one for third parties and so on.

A common challenge in developing a firmwide taxonomy is embedding business ownership. Too often, taxonomy efforts are viewed as being performed to the first line, rather than by the first line; the first line views these as efforts control groups have to complete to conduct their work and complain they are written in control-speak. Few first-line leaders view such taxonomies as necessary to deliver operational resilience or as being written in a way the first line would describe what it does and how it operates.

Some firms are seeking new ways for the first line to own the taxonomy to promote first-line accountability for resilience, and to encourage the first line to keep the taxonomy up to date as operations change. Being successful in such an approach would sharpen the first line's business-impact assessments and subsequently improve its business continuity plans. However, any new approaches have to deliver consistency firmwide — having myriad first-line-generated taxonomies would undermine firmwide resilience, and make it difficult — if not impossible — to align that taxonomy with the other taxonomies that exist. In the end, it's a balancing act.

A common taxonomy has to be supported by an up-to-date and well-integrated set of technology enablers, such as the governance, risk and control (GRC) platform; the configuration management database (CMDB); key enterprise-wide IT operations tools; and the continuity/incident management toolset.

3

Identify and manage dependencies, and single points of failure and concentration inside and outside the firm: Mapping only gets you so far. It's not simply about understanding how the process or data flows, but as important about identifying key choke points or areas of concentration (e.g., a firm's key operations or locations). These could include IT or processes that support one or more critical steps to deliver a service, a key upstream or downstream dependency (i.e., something before or after the specific process without which the service is interrupted) and even key subject-matter experts.

Such choke points can lie outside the firm, and include key third parties (e.g., major technology providers or large-scale outsourced capabilities). In reality, the list of third- to fifth-party firms that create concentration risk across the industry is fairly long — there are many firms that have dominant positions in the financial services value chain whose disruption could create system-wide disruption: think data processors; equity-, debt- and credit-data providers; technology and cloud providers; and so on. Firms need to identify where they are dependent on such firms, either directly or indirectly (that is, when they are key fourth or fifth parties), and integrate that knowledge into their contingency plans and set of scenarios those plans address.

4

Establish a firmwide resilience strategy and operating model: Increasingly, firms have recognized that their continuity and resilience activities are disparate and unconnected. They often have countless activities across business continuity, disaster recovery, cyber-incident response and crisis management. Often, myriad crisis and contingency plans exist across lines of business, technology, human resources and other areas. Few plans are connected or consistently applied; few plans have common or consistent triggers for escalation and decision-making; and few companies have properly prepared their senior executives and/or boards for actual crises. The result is often ineffective, erroneous or slow decision-making in times of stress.

Firms are developing a more cohesive strategy that straddles the many distinct and disparate groups and plans. In some cases, firms are shifting their focus to managing the impact, irrespective of how and where an event originates. To execute the strategy, some firms are centralizing some of their resilience functions with a first-line, enterprise-level resilience group, including:

- Strategy development
- Resilience program management (e.g., business continuity and disaster recovery)
- Overall change management
- Requirements setting (e.g., recovery time objectives (RTOs), recovery point objectives (RPOs), business availability objectives)
- Critical process and dependency mapping
- Response capabilities (e.g., the crisis management group and its linkages to various incident response programs)
- Testing strategy

Some are even incorporating their RRP work and resilience-related industry-level initiatives, such as so-called mutual assistance concepts. RRP capabilities can be particularly important in this regard — some of those capabilities are risk agnostic, meaning they can be leveraged effectively in the broader resilience program.

Centralized groups are supporting better coordination with other relevant activities in the business lines and key functions — notably technology, legal, corporate and client communications, privacy and information security, treasury and compliance. In a few cases, a chief resiliency officer has been appointed to lead these centralized groups and establish stronger accountability for strategy development and execution in a firmwide, coordinated manner.

Second-line risk management is taking a more prominent role, too, with some firms putting resilience framework development into their hands, alongside the development and monitoring of aggregate resilience metrics that are incorporated into the firm's board-approved risk appetite framework. A key task for risk management is linking the resilience framework to existing IT and operational risk frameworks and processes. See "Impact tolerances based on the assumption of disruption."

5

Promote prevention: While the focus has quickly turned to response and recovery, there still needs to be a strong focus on prevention to reduce the probability that disruptions occur and their potential impact. Strategies here include:

- Segmenting critical systems, including networks and systems, and limiting points of attack and entry
- Hardening access rights by reassessing access privileges, e.g., when individuals change roles, including those of third parties (especially client-hosted platforms)
- Addressing IT obsolescence to reduce dependency on redundant systems and validating that IT obsolescence does not create critical-process vulnerabilities
- Managing change effectively to reduce the likelihood that a poorly executed, a badly controlled, or an ill-timed IT or process change triggers a disruption
- Implementing resilience by design — versus resilience by remediation — to enable resilience principles to be adhered to from the outset of designing new systems or processes

Of course, in addition to technical prevention, it's important to remember employees are the first line of defense — and often the entrance point for or unknown subject of criminal actions. They need education on the role they play and reminders of how to act when they see something that seems abnormal or suspicious.

6

Establish a well-documented and well-tested resiliency strategy:[2] Traditionally, the discussion about business continuity starts with a discussion regarding the robustness of the firm's processes — or rather, a debate about whether a key process or piece of hardware or software will or will not fail. Today, firms are being asked by clients and regulators how they will continue to deliver a service assuming a system or process has failed — the exam question is no longer will a disruption occur, but rather when it does, what next?

Such an approach necessitates a different line of thinking: Which operational or technology backup processes or alternate third parties are available to continue service delivery? How well have those alternatives been tested and documented? Are those processes being used in production, rather than in a simulated environment? Have firms "failed over" to their disaster recovery capabilities and "fallen back" to primary systems in due course?

7

Validate that backup approaches are sustainable: Clients and regulators no longer want to know theoretical answers about resiliency capabilities — today, they want to know firms have tested those processes for a period of time to determine whether continuous service delivery is possible, and at what point material degradation in service quality will occur. This means moving from discussions about RTOs to recovery time realities.

Key questions follow: How long could the firm continue to deliver services when a key system or process has failed? 10 days? A month? Beyond a month, does the firm extend to month-end reporting? What about the loss of a key third party for a prolonged period?

An important new dimension in these backup strategies is the potential for bad actors to manipulate or destroy data. Backup plans have to accommodate scenarios that include firms having no access to key information or only having access to information that could be corrupted. This quickly moves the dialogue to:

- How and where do firms hold and protect a "golden source" of data?
- How do air-gapping strategies help? Which new technologies are available?
- How can data be modularized or segmented?
- Which external options (including industry initiatives) could offer temporary solutions?

Such thinking and preparation highlight that, while using cloud-based solutions may deliver higher resilience overall, such an approach does nothing for data corruption — once the integrity of data is in question, it doesn't matter where that data is stored (indeed, a cloud-based environment that operates "hot-hot" between primary and secondary sites may actually speed data corruption faster than otherwise may be the case with in-house systems that operate with more latency).

[2] For insights on how to be more prepared for disruptions, see Managing through crises: preparation is key.

Impact tolerances based on the assumption of disruption[3]

UK regulators have proposed that firms develop so-called impact tolerances that define their upper tolerance for disruption to certain business services, under the assumption that disruption to that particular service will occur.[4] Such statements differ from a firm's risk appetite statements and RTOs, as those incorporate an element of probability. The intent of setting impact tolerances is to focus boards and management teams on what would be done when a disruption occurs, rather than on activities that minimize the probability of disruption.

UK regulators propose that firms:

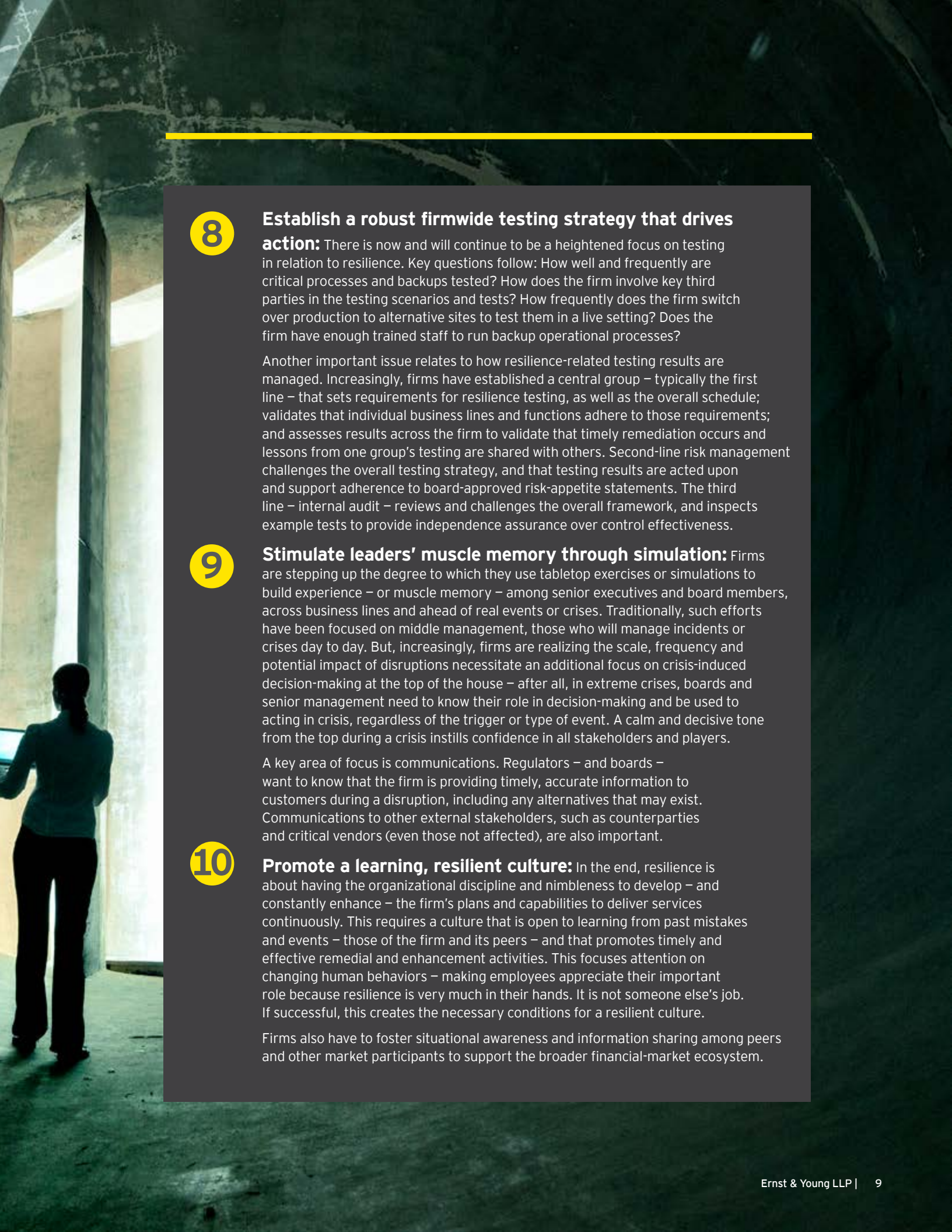
- Set impact tolerances for their most important business services
- Cover services that, if disrupted, could (a) cause customer or market-participant harm, (b) threaten the ongoing viability of the firm and (c) undermine financial stability
- Cover severe, but plausible, scenarios
- Prioritize those services for which impact tolerances are set
- Align impact tolerances with published supervisory objectives or service-based disruption tolerances (e.g., intraday processing of payments)
- Have their board of directors understand, approve and monitor adherence to all impact tolerances
- Incorporate metrics (e.g., the maximum tolerable duration or volume of disruption, the criticality of data integrity or the number of customers affected)
- Monitor and test their operations against impact tolerances on an ongoing basis
- Implement robust remediation plans to address identified gaps between approved tolerances and actual capabilities
- Document and explain the relationship between impact tolerances and risk-appetite statements and RTOs

The UK's financial stability regulator, the Financial Policy Committee, has said it will publish its tolerance for disruption to the delivery of critical services in the context of cyber and expects firms to operate within those tolerances.[5] Going forward, assuming UK firms will be required to set their own business service-level impact tolerances, UK regulators have stated they also may establish tolerances at the individual firm level that they would expect firms to manage within. However, initially, the onus will be on firms to define their own impact tolerances for critical services.

[3] "EY's response to 'Building the UK financial sector's operational resilience' – a BoE/FCA/PRA Discussion Paper," Ernst & Young LLP, 2018.

[4] "Building the UK financial sector's operational resilience," Bank of England, 2018.

[5] "Discussion paper: Building the UK financial sector's operational resilience," Bank of England, 2018.



8 **Establish a robust firmwide testing strategy that drives action:** There is now and will continue to be a heightened focus on testing in relation to resilience. Key questions follow: How well and frequently are critical processes and backups tested? How does the firm involve key third parties in the testing scenarios and tests? How frequently does the firm switch over production to alternative sites to test them in a live setting? Does the firm have enough trained staff to run backup operational processes?

Another important issue relates to how resilience-related testing results are managed. Increasingly, firms have established a central group – typically the first line – that sets requirements for resilience testing, as well as the overall schedule; validates that individual business lines and functions adhere to those requirements; and assesses results across the firm to validate that timely remediation occurs and lessons from one group's testing are shared with others. Second-line risk management challenges the overall testing strategy, and that testing results are acted upon and support adherence to board-approved risk-appetite statements. The third line – internal audit – reviews and challenges the overall framework, and inspects example tests to provide independence assurance over control effectiveness.

9 **Stimulate leaders' muscle memory through simulation:** Firms are stepping up the degree to which they use tabletop exercises or simulations to build experience – or muscle memory – among senior executives and board members, across business lines and ahead of real events or crises. Traditionally, such efforts have been focused on middle management, those who will manage incidents or crises day to day. But, increasingly, firms are realizing the scale, frequency and potential impact of disruptions necessitate an additional focus on crisis-induced decision-making at the top of the house – after all, in extreme crises, boards and senior management need to know their role in decision-making and be used to acting in crisis, regardless of the trigger or type of event. A calm and decisive tone from the top during a crisis instills confidence in all stakeholders and players.

A key area of focus is communications. Regulators – and boards – want to know that the firm is providing timely, accurate information to customers during a disruption, including any alternatives that may exist. Communications to other external stakeholders, such as counterparties and critical vendors (even those not affected), are also important.

10 **Promote a learning, resilient culture:** In the end, resilience is about having the organizational discipline and nimbleness to develop – and constantly enhance – the firm's plans and capabilities to deliver services continuously. This requires a culture that is open to learning from past mistakes and events – those of the firm and its peers – and that promotes timely and effective remedial and enhancement activities. This focuses attention on changing human behaviors – making employees appreciate their important role because resilience is very much in their hands. It is not someone else's job. If successful, this creates the necessary conditions for a resilient culture.

Firms also have to foster situational awareness and information sharing among peers and other market participants to support the broader financial-market ecosystem.

A long journey is ahead, but it's critical to succeed

No one expects delivering firmwide resilience to be easy. Even those firms that have dedicated the most resources to resilience in recent years have major work ahead to validate that they can deliver services to their customers at levels now expected by external stakeholders.

Some compare the resilience journey ahead with the one some firms have experienced over the past decade to establish and maintain stress testing and RRP. Those capabilities have required significant investments of management time and resources, and taken years to properly institutionalize.

Indeed, for many firms, the work ahead to properly embed those processes into day-to-day management decision-making, versus treating them as periodic regulatory exercises, is still significant.

Delivering resilience is sound business sense. As firms transform themselves digitally from front to back office, and as they seek to deliver against the 24/7 promise to customers, achieving operational resilience is core to each firm's – and industry's – long-term success and competitiveness.

There may be a long journey ahead. But it's a journey that could not be more important.

10 ways to enhance firmwide resilience

1. Focus on mapping and demonstrating end-to-end critical business services, beyond the firm's borders
2. Adopt a common resiliency language
3. Identify and manage dependencies, and single points of failure and concentration inside and outside the firm
4. Establish a firmwide resilience strategy and operating model
5. Promote prevention
6. Establish a well-documented and well-tested resiliency strategy
7. Validate that backup approaches are sustainable
8. Establish a robust firmwide testing strategy that drives action
9. Stimulate leaders' muscle memory through simulation
10. Promote a learning, resilient culture

Contacts

Americas – United States

Lisa Choi
lisa.choi@ey.com
+1 212 773 8947

John Doherty
john.doherty@ey.com
+1 212 773 2734

Cindy Doe
cynthia.doe@ey.com
+1 617 375 4558

Sundeep Nehra
sundeep.nehra@ey.com
+1 212 773 3888

Dan Stavola
dan.stavola@ey.com
+1 201 551 5073

Mark Watson
mark.watson@ey.com
+1 617 633 5570

Latin America

Bismark Rodriguez
bismark.rodriguez@pa.ey.com
+1 239 738 3643

Ariel Koch
ariel.koch@cl.ey.com
+56 2 676 1329

EMEIA

Ali Kazmi
akazmi@uk.ey.com
+44 20 7951 9052

Steve Holt
sholt2@uk.ey.com
+44 20 7951 7874

Asia-Pacific

Chris Lim
chris.lim@sg.ey.com
+65 6309 6320

Jeremy Pizzala
jeremy.pizzala@hk.ey.com
+852 2846 9085

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace

Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

US SCORE no. 04976-181US

1810-2903492 (BD FSO)

ED None

ey.com