Supervisory perspectives and regulatory approaches to enterprise resilience:

Common themes and differing approaches

Building a better working world

Introduction

Enterprise resilience is a firm's ability to respond to, recover from, and resume operations at acceptable levels of service to customers, clients, and counterparties through significant disruptions

Higher expectations from customers and market participants for firms to deliver continuous services to the marketplace and more frequent and extended outages affecting financial services firms have drawn increased scrutiny from regulators worldwide. Enhancing capabilities to strengthen enterprise resilience is critical for firms to remain competitive, maintain market confidence and support financial stability. With business disruptions on the rise, including increased risks from cyber-attacks, natural disasters, pandemics and critical service provider failures, improving enterprise resilience is a board-level imperative across the financial services industry.

A number of market trends are driving this increased emphasis on resilience from external and internal stakeholders. These include, but are not limited to:

- Client demand for "always on" services and 24/7 access to products and services, along with the assurance that their information is safe and protected
- Concentration risk in third-party service providers (e.g., cloud service providers)
- Adoption and usage of newer technologies (e.g., digital), which enhances resilience but also introduces additional risks
- Highly complex and interconnected businesses and operations with heavy reliance on third-party service providers
- Increased frequency of extended IT outages

With the ever-changing, global business environment subject to heightened client and regulatory pressures, and the increased risk of a major cyber-attack and natural disasters, building enterprise resilience is no longer a choice.

Chapter 1: Renewed regulatory focus on operational resilience

Global regulators' focus on resilience is not new, but the scope and emphasis have evolved over time in response to disruption events, changes in market infrastructure, emerging technologies and shifting supervisory priorities. In the past, resilience has been more narrowly construed by the regulators as business continuity planning (BCP), disaster recovery (DR), physical recovery and so forth. But today, regulators define it more broadly to include all the aforementioned components and much more. For instance, BCP today is only a small component of — but not all — resilience. Additionally, regulators now are paying more attention to a firm's ability to maintain operational continuity through a broader range of disruption events.

Over time, regulators have updated, consolidated and elevated their supervisory expectations related to resilience to enhance their efficacy, drive internal consistency and alignment with related guidance, and increase relevance, given firms' operational complexity and risk profile. The recent regulatory focus on resilience should be viewed in the context of a continuing evolution of standards and expectations across global regulators to foster safety, soundness and financial stability of the financial sector.

1. Origin of resilience standards

In the aftermath of the disruptions following the 9/11 terrorist attacks, regulators' initial focus on resilience centered on the recovery and resumption of critical Financial Market Infrastructures (FMIs) for systemically important wholesale payment systems. For example, US regulators adopted interagency guidance on "Sound Practices to Strengthen the Resilience of the U.S. Financial System."[1] The guidance was narrowly focused on core clearing and settlement activities of systemically important firms and excluded other types of activities (e.g., retail) and firms (non-FMIs). European banking regulation followed a similar evolution with an initial focus on recovery and resumption of systemically important payment systems, with emphasis on central counterparties in 2012.[2] Like the US, the European Union (EU) and the UK have gradually expanded the scale and scope of these expectations to different types of financial services firms (beyond just FMIs) to encapsulate a broader range of banking activities (retail and wholesale) provided by the financial system.

Notably, the foundation for the first, international standard on business continuity management (BCM) was also laid during this era in 2006, and resulted in ISO 22301 Standard in 2012, which became a recognized benchmark of good practices in BCM.

2. Post crisis reforms

The 2008 financial crisis raised concerns about the resilience and viability of the financial sector to withstand severe market stress and contagion. As a result, global regulators turned their attention toward ensuring financial resilience — the ability of firms to continue to provide credit and market intermediation to clients and counterparties during a period of extreme market and liquidity stress. An important element was due consideration of the impact of stress on the firm's abilities to meet its' obligations (in this case financial) to other market participants. Thus, this period marked a notable expansion in the scope and rigor of requirements related to financial resilience, as seen through a series of global regulations on liquidity, capital, recovery and resolution, to address the scale and systemic impact of the crisis.

Importantly, expectations around operational resilience evolved and became more integrated with financial resilience during this time as regulators expected firms to demonstrate operational capabilities required to achieve resolution outcomes. For example, the UK adopted a policy

statement on "ensuring operational continuity in resolution" with the goal of ensuring that the firms' operational arrangements continue to facilitate delivery of critical functions to the market during a resolution event.[3] Thus, the work to inform the firm's resolvability naturally put the spotlight on advancing capabilities required to meet service obligations and maintain operational continuity through a broader range of disruption scenarios.

3. Focus on operational and technology resilience

As the 2008 financial crisis subsided, and global regulators became increasingly satisfied with both the quality and quantity of capital and liquidity in the financial system, they renewed their focus on operational resilience. Key drivers were the risks associated with operational complexity due to firms' increased reliance on emerging technologies, highly-publicized outages in the US and UK and concerns about firms' vulnerability to cyber-attacks. These factors reinforced the perceived need for greater scrutiny on operational and technology resilience.

In the US, the regulators have issued resilience guidance on a number of topical areas, such as BCP, information security, operations, and outsourcing technology services, through inter-agency guidance or the Federal Financial Institutions Examination Council (FFIEC) IT handbook and supporting booklets.[4] Earlier this year, the Federal Deposit Insurance Corporation (FDIC) articulated gaps in firms' contracts with technology service providers based on exam findings, and required intervention from firms to better manage their business continuity and incident response for such service providers.[5]

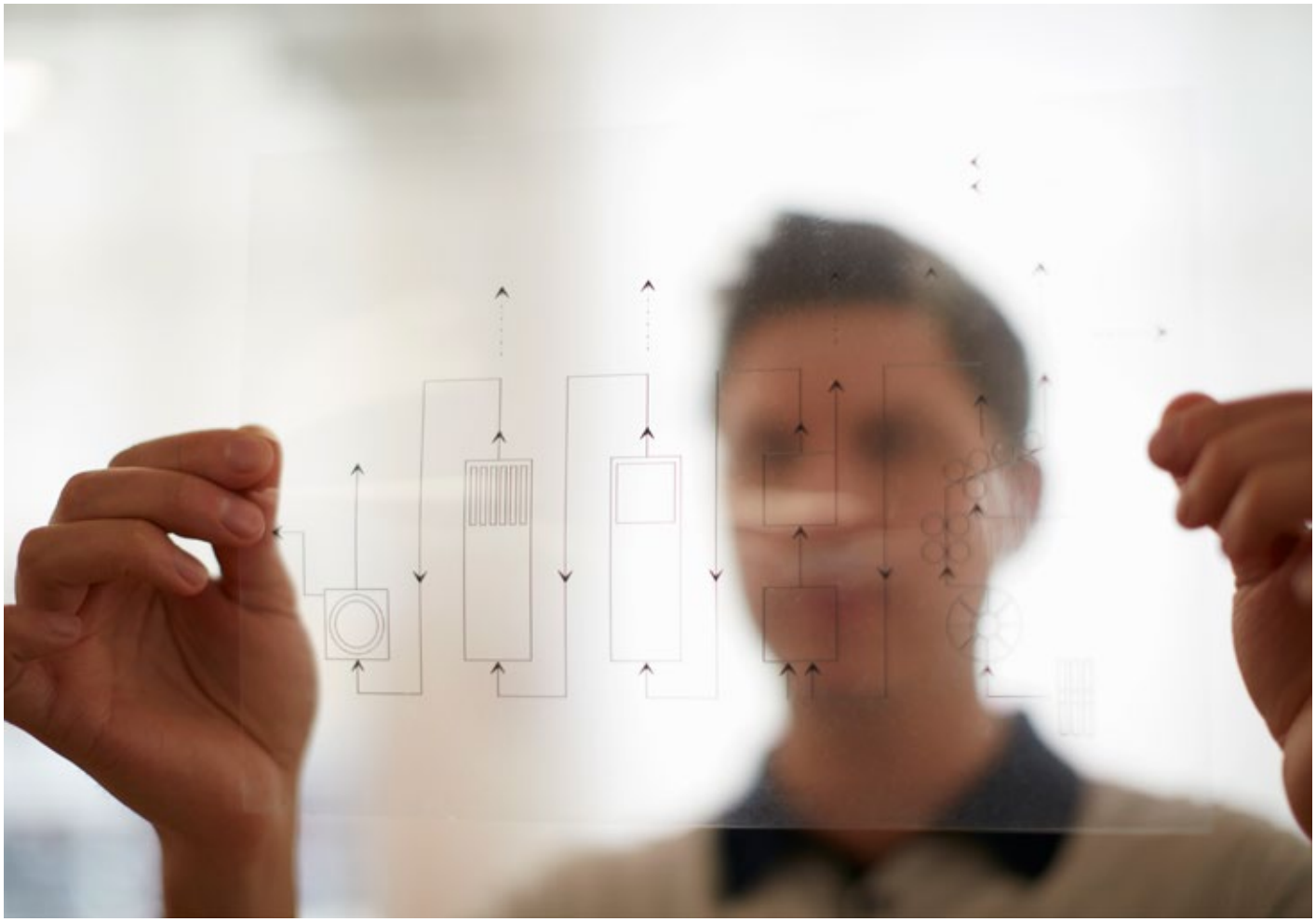
European regulators have taken a similar approach. Under the auspices of the European Banking Authority (EBA), European regulators have sought to consolidate and provide more explicit guidance across payment and credit institutions on information and communication technology risks, to address gaps in light of emerging cyber threats and seek public comment.[6] The disparity of practices and expectations across financial institutions was a key impetus for consolidation. This was further accelerated by the issuance of General Data Protection Regulation (GDPR), which creates additional requirements with implications for information security. The EBA is also proposing separate guidance relating to cyber resilience across systemically important FMIs, which can be viewed as a logical extension of EBA's initial focus on systemically important payment systems and central counterparties.[7]

The UK regulators have been at the forefront of resilience and have taken a top-down, integrated approach by synthesizing relevant components of resilience under an "operational resilience" umbrella. This is observed through the joint discussion paper, *Building the UK financial sector's operational resilience*, published by the Bank of England, Prudential Regulatory Authority (PRA) and FCA in July 2018.[8] Like their counterparts, UK regulators' have

UK regulators: at the forefront of resilience

On 5 July 2018, the Bank of England, PRA and FCA issued a joint discussion paper (DP) on maintaining operational resilience of financial institutions and FMIs.

The UK regulators, through the DP, have been the first among global regulators to publicly release their expectations for an integrated and customer-centric approach to resilience. The DP is currently the most developed regulatory guidance on enterprise resilience available, and is providing the basis for other regulators to formulate their approaches on resilience. Since the publication of the DP, the UK regulators have actively engaged with the industry participants to refine their approach on resilience and may be close to finalizing their guidance.

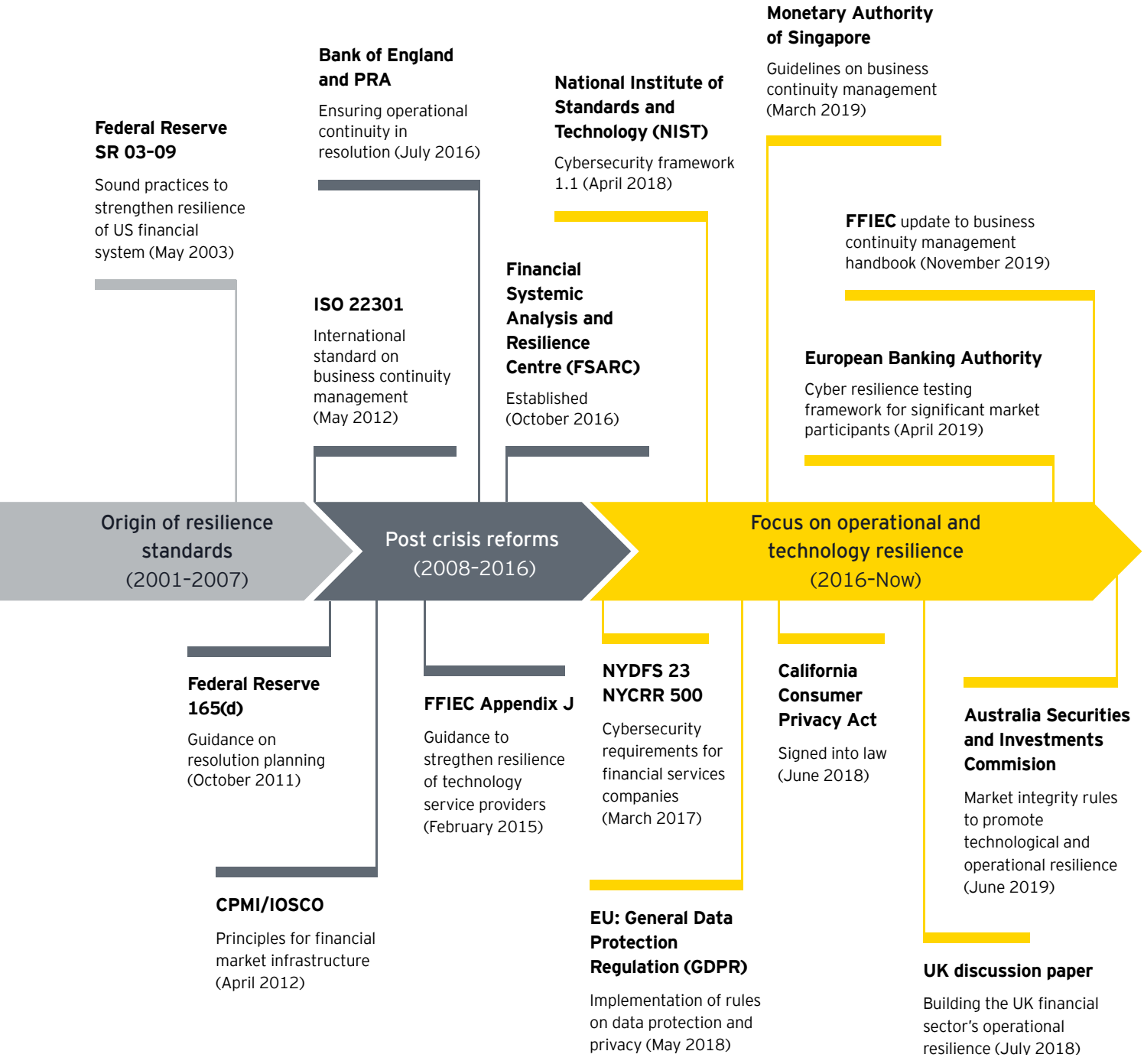


included operational resilience as a key consideration in both their safety and soundness and, more recently, in financial stability assessments. The UK has adopted many of the same guidelines and principles that form the basis of European and international requirements (as set forth by the Basel Committee of Banking Supervisors (BCBS)). Other regulations, such as the Senior Manager Regime (SMR) that entail governance and risk management requirements also reinforce operational resilience requirements.

In Australia, like other jurisdictions, there has been a historical focus on operational resilience and, as elsewhere, increased operational complexity has raised operational continuity concerns that have encouraged the Australian Prudential Regulatory Authority (APRA) to update its existing guidance. For example, in late 2018, APRA released a new prudential standard, CPS 234 Information Security, to strengthen firms' resilience against information security incidents (including cyber-attacks), and their ability to respond in the event of breaches.[9] APRA also developed additional industry guidance on the use of shared computing services, such as the cloud.[10] In June 2019, Australia Securities & Investments Commission (ASIC) released a consultation paper proposing new market integrity rules to promote technological and operational resilience for securities and future market operators and their participants.[11]

In Asia, the Monetary Authority of Singapore (MAS) guidance on resiliency has evolved in a similar manner to both US, Australian and EU guidance, where the focus began with operational continuity, then information security and ultimately cyber resilience. The MAS issued its BCM guidelines in 2003 and updated them recently to reflect increased expectations, including heightened expectations for board and senior management accountability (e.g., annual review, and attestation by management to the board on business continuity preparedness).[12] The MAS also enhanced its technology risk management (TRM) guidelines, which were first issued in 2013.[13]

Regulatory evolution



Chapter 2: Differing regulatory approaches reflect differences in areas of emphasis, not core principles

Global regulators will likely continue to support common principles related to enterprise resilience, to encapsulate all the elements of resilience described in chapter one. The Basel Committee on Payments and Settlement Systems is in the process of drafting a common set of principles to foster greater harmonization. Nevertheless, differences in approach are likely to persist, although these differences are largely expected to be in emphasis to incorporate actual and perceived risks within a jurisdiction rather than differences in objectives. The risks associated with resilience are varied, dynamic and inter-related, cutting across various operational risk dimensions (e.g., people, process, technology and third-parties), which creates challenges in ensuring the ongoing efficacy of supervisory standards and expectations.

One emerging approach to meet this challenge is through more holistic guidance around resilience, as embraced by the UK regulators, to cover these broad range of risks. They have synthesized relevant components or topical areas of resilience under an "operational resilience" umbrella and have tied it more explicitly to its financial stability objectives, as described through the joint discussion paper on operational resilience. The more recent and highly publicized disruptions of financial services to retail customers and the advent of Brexit have highlighted the risks associated with disruptions of services. As a result, the UK regulators have been more comprehensive and specific in outlining standards and expectations for operational resilience, particularly in the areas related to the definition of business services (e.g., by providing an initial list of business services linked to economic functions for firms to consider), and the importance of impact tolerances. They have also actively engaged with the industry through workshops and surveys to gather input to further fine tune their approach for resilience before finalization.

In contrast to the UK, the US regulators have taken a more bottoms-up and education-focused approach to resilience that leverages existing guidance and firm-specific information to understand current industry practices, with the goal to identify areas requiring additional guidance. US regulators have exercised their oversight mainly through supervisory exams to evaluate and compare existing resilience programs at various firms, and inform their approach on resilience. They view resilience as an additional risk management discipline, have been less prescriptive than the UK, and are using their prior experience in supervising financial resilience (e.g., capital, liquidity) to drive their approach on operational resilience.

Like the US, the EU, Australia and Singapore have also undertaken a bottoms-up approach on resilience and are generally less prescriptive than the UK, except for IT security requirements. Compared to the UK, these jurisdictions have provided less guidance on which business services are crucial or how to define a critical business service, allowing more discretion to the firms.

Chapter 3: Common components and expectations that regulators are prioritizing across jurisdictions

While the regulatory approaches and details in the regulations may differ across jurisdictions, global regulators seem aligned on the fundamentals and core principles of resilience. They remain focused in ensuring that the risks due to a firm's operational complexity and interconnectedness with the broader ecosystem are not transmitted into the financial markets, and that the interests of the customers, and market participants are safeguarded during business disruptions. The following represents the six areas that are most impacted by increased regulatory scrutiny of resilience:

1. Orientation to end-to-end business services

Regulatory expectations

The regulators expect firms to take a business service view on resilience that prioritizes the resilience of its most critical business services instead of focusing on individual systems and applications. The criteria for identifying the most critical business services should be inclusive of client and market impacts, and should consider the firm's interconnectedness with other market participants. To enable end-to-end recoverability and resumption of business services, firms must identify and map critical assets across people, process, technology, data, facilities and beyond the firm's internal ecosystem to encompass reliance on critical third-parties. Moreover, regulators expect firms to perform risk assessments (e.g., business impact analysis (BIA) and BCPs) at a more granular level to incorporate a service-focused view, map asset interdependencies extensively, and identify any concentration risks, including single points of failure.

Implications for firms

- **Service criteria and listing.** Define clear criteria to identify a common list of the most critical business services across various inter-related programs (e.g., BCP, DR, cyber risk management)
- **Asset identification and mapping.** Expand on existing asset mapping to identify and assess the impact of interdependencies outside of the firm's environment (e.g., third-parties)
- **Risk assessments (e.g., BIAs and BCPs).** Enhance current approaches to conduct BIAs and BCPs to enable service-focused prioritization of recovery requirements across various impact dimensions, peak periods and critical processing deadlines
- **Concentration risks.** Devise back-up strategies to diversify exposure and reliance on critical third-parties

As firms shift from a technology focused view to a business service view on resilience, several instances of variances between service level RTO (inclusive of recovery objectives across people, process, technology and data), and technology-based RTO (focused on recovery objectives across systems and applications only) are being observed, with lack of an adequate governance process to resolve such variances. Strategies to address certain types of concentration risks (e.g., reliance on cloud service providers), including single points of failure, remain an industry-wide challenge. In addition, firms are yet to fully integrate results of BIAs and BCPs into their existing risk assessment frameworks.

Interconnecting with the broader ecosystem (third-party service providers, FMIs, outsourcers, counterparties)

Firms are exposed to potential vulnerabilities and risks due to interconnectedness with critical third-parties, such as FMIs, data providers, cloud service providers, outsourcers and technology vendors. Many of these third-parties cater to several firms within the industry, including fourth-or fifth-party service providers, resulting in high concentration risks (including single points of failure), knock-on impacts due to interdependencies, and potential systemic impacts during third-party outages. These risks are further exacerbated when a third-, fourth-, fifth- party provider is in the same geography as the firm's operations, thereby posing additional challenges to continuous delivery of business services during regional disruptions.

An additional layer of complexity comes from the fact that many of the critical third-party providers are not currently regulated or overseen directly by the banking regulators. While the banking regulators have tried to use different approaches to supervise these entities through indirect laws and regulations, the effectiveness of such supervision is yet to be seen.

2. Impact tolerances based on client and market impacts

Regulatory expectations

Regulators expect firms to establish impact tolerances, with clear metrics and specific outcomes for their most critical business services, to quantify the amount of disruption that could be tolerated. They want firms to derive the impact tolerances inclusive of client and market impacts, and irrespective of where the systems and processes supporting the business service are located. Additionally, regulators expect firms to demonstrate that they can meet the established impact tolerances under plausible and severe scenarios, and specifically identify instances in which the tolerances may be at the risk of being breached.

Once established, firms should leverage the impact tolerances to inform delivery of business services to clients and the market, and to prioritize investment management and resource allocation decisions related to resilience.

Implications for firms

- **Impact tolerance framework.** Develop an enterprise-wide framework and criteria to establish impact tolerances
- **Impact tolerances and related metrics.** Define qualitative and quantitative metrics (e.g., KPIs or KRIs) for each critical business service inclusive of client, market and firm impacts
- **Monitoring and testing.** Demonstrate capabilities to track and meet impact tolerances under severe and plausible scenarios
- **Alignment to risk appetite.** Integrate impact tolerances into existing methods of monitoring and measuring risks, including firm's risk-appetite

Firms have metrics (KPIs and KRIs) and thresholds that they monitor on a day-to-day basis to manage the business. However, firms have defined these tolerances more subjectively based on direct, financial impact to the firm, and excluding client and market impacts. They are struggling to quantify the impact tolerances to a number: for example, into maximum tolerable outage time for a business service or service level RTOs. This is partly due to additional work needed to move away from a narrower construct of a technology-based RTO, and because firms are hesitant to assign a numerical value of impact against a service that their peers may be able to surpass. Additionally, firms are yet to fully translate how these tolerances should inform prioritization of investments and resource allocation decisions on resilience.

Chapter 3

Common components and expectations that regulators are prioritizing across jurisdictions

3. Alignment of coherent set of capabilities

Regulatory expectations

The regulators expect firms to develop a comprehensive suite of capabilities required to recover and resume business services during disruption. They want firms to move away from the traditional, siloed approach of managing distinct capabilities to an overarching enterprise-wide framework for resilience across various inter-related programs (e.g., BCP, DR, cyber or third-party risk management (TPRM)). As the emphasis shifts to a business-service-focused view, firms should develop a common set of capabilities that are flexible and adaptable to meet objectives across various inter-related programs.

Additionally, regulators want firms to designate a centralized role or function, with ownership of resilience planning, coordination and management across the enterprise. They also expect firms to establish and align policies and standards for resilience across various inter-related programs and implement an operating model that drives accountability for resilience across all three lines of defense.

Implications for firms

- **Enterprise resilience framework.** Define an enterprise-wide resilience framework that includes the full suite of capabilities required for resilience management across BCP, DR, cyber-risk management, TPRM, information security and data management
- **Centralized ownership.** Designate a role or function within the firm accountable for resilience planning and management, with connectivity to localized resilience teams at regional levels
- **Resilience policy.** Develop a standalone, enterprise-wide resilience policy as a wrapper to collate and align disparate resilience expectations across various inter-related policies and standards (e.g., BCP policy, DR policy or cyber-risk management policy)
- **Operating model.** Enhance the existing operating model to outline roles and responsibilities for resilience management across all three lines of defense

As firms look to integrate their existing operating models to encompass enterprise-wide capabilities for resilience, the key challenge remains how to reconcile varying resilience taxonomies and approaches across inter-related programs. Firms, at times, have competing definitions and criteria for business resilience management, for instance differing views of business services across BCP and the cyber-risk program, that they need to bring together to provide a unified and holistic view of resilience risks and capabilities across the enterprise.

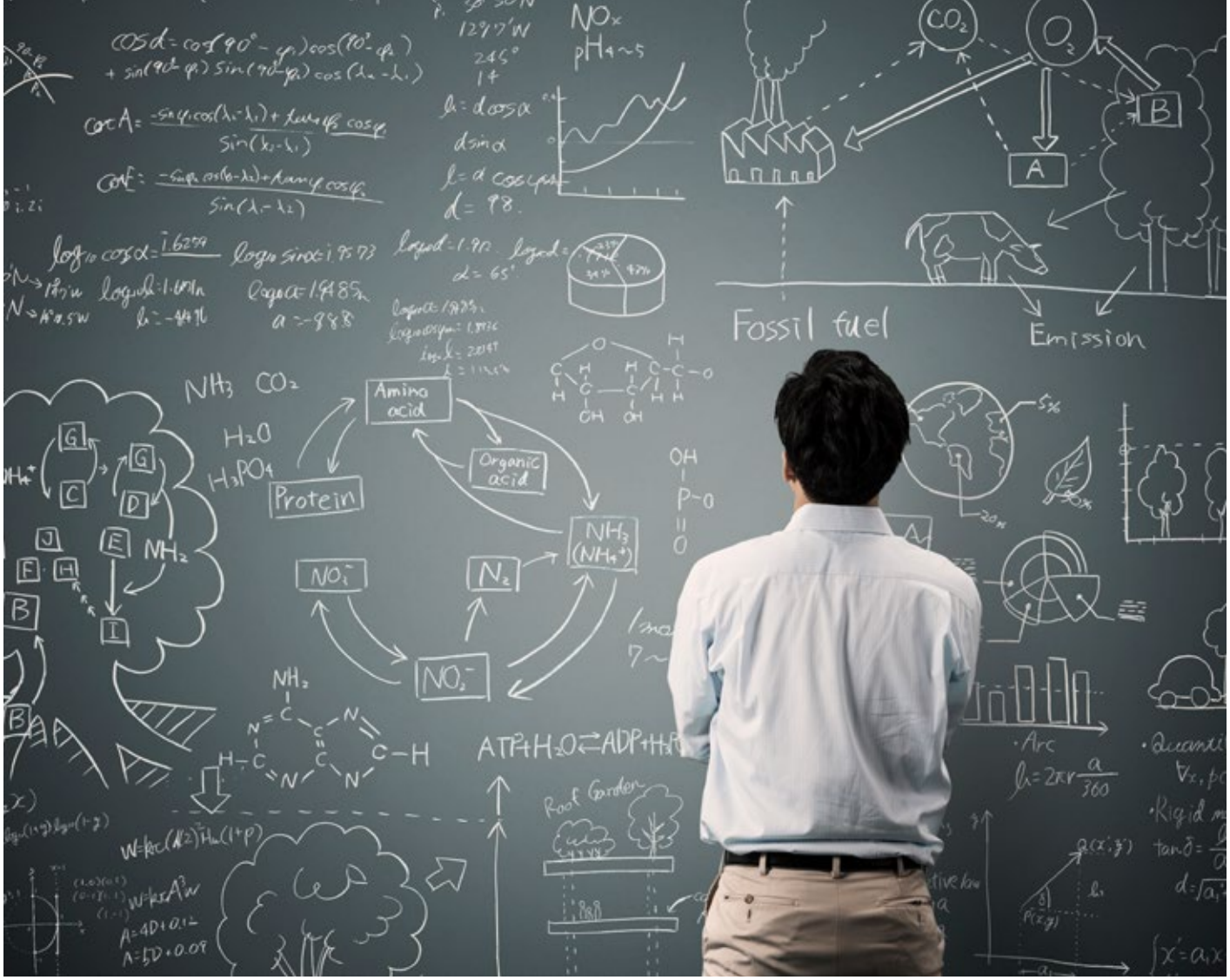
4. Approach to respond cohesively to range of disruptions

Regulatory expectations

Business service disruptions can occur from a wide range of situations, including isolated technology issues, weather-related operational outages, third-party failures and cyber-attacks. Firms often have disparate approaches and protocols to respond to these various types of disruptions. As regulators focus on business service resumption and less on recovering individual components, they require firms to demonstrate greater integration between incident management and crisis management protocols, and demonstrate capabilities that are responsive to different types of disruptions. Additionally, regulators expect firms to improve the speed, transparency and timeliness of communications, particularly to clients, regulators and market participants, to minimize client impacts and rebuild customer trust and market confidence. Furthermore, they expect firms to have clearly defined escalation paths to enable information flows to decision-makers all the way up to the board for timely decision-making.

Implications for firms

- **Crisis management framework.** Define a risk-agnostic crisis management structure with alignment and linkages to other contingency plans and protocols



- **Communications strategy.** Augment the firm's traditional communications strategy with a robust social media strategy to ensure consistent, accurate and timely dissemination of information to internal and external stakeholders
- **Interdependency management.** Enhance the firm's governance process to prioritize and manage interdependencies across its business and functional areas
- **Regulatory engagement strategy.** Outline a process to manage and respond to an influx of queries from regulators across various jurisdictions

Most firms have developed various contingency protocols to respond to different types of crises. The challenge, however, is in determining when to enact which contingency protocol and how to better integrate these together to provide a cohesive enterprise response during a crises. Additionally, while firms routinely test their crisis management framework and protocols, these tests often do not sufficiently involve participation from critical decision-makers, such as the board and senior management, to build muscle memory (e.g., management reflexes) and exercise relevant plans and playbooks.

5. Integrated testing framework

Regulatory expectations

Regulators require firms to demonstrate end-to-end resilience of their most critical business services, inclusive of people, process, technology, data and third-party components. They expect firms to test recovery and resumption of business services under a range of severe and plausible scenarios, and may prescribe pre-defined scenarios for firms to use in certain situations. In addition, they want firms to define a comprehensive and integrated testing strategy for resilience across BCP, DR, cyber risk management.

In addition, regulators expect firms to implement an integrated testing framework that gradually increases in rigor, complexity and scope of tests over time, pressure tests key assumptions and strategies, and drives continuous improvement by embedding key learnings from tests into resilience plans and capabilities. Regulators also want firms to continue participating in sector-wide exercises to rehearse collective response mechanisms and decision-making during industry-wide events.

Implications for firms

- **Integrated testing strategy and framework.** Develop an enterprise-wide testing strategy and framework to articulate objectives, success measures and approach for resilience testing across various inter-related programs (e.g., BCP, DR, cyber risk management, TPRM)
- **Scenario planning.** Increase the rigor and complexity of testing by using more severe but plausible scenarios based on market events, firm-specific vulnerabilities, and emerging risks and threats
- **Third-party assessments.** Incorporate mechanisms to gain assurance on the resilience of select third-parties supporting critical business services, including those with high concentration risks
- **Continuous improvement.** Demonstrate how learnings from the testing exercises and actual disruption events are embedded into existing frameworks, plans and capabilities to improve firm's resilience

Firms are struggling to find the right balance to streamline and optimize testing across different programs as they are performing too much testing in certain areas while under-testing in others. Firms also recognize the need to augment existing tests with new tests and approaches to confirm design and effectiveness of the end-to-end capabilities required to deliver a business service. Rigor and discipline to ensure timely remediation of gaps identified through testing is an area where firms can show improvement.

6. Board and senior management oversight

Regulatory expectations

The regulators expect the board and senior management to take an active role in overseeing the firm's resilience strategy and framework in alignment with the enterprise strategy and risk appetite. They want board and senior management to effectively challenge the capabilities underpinning the most critical business services and related impact tolerances. In addition, the board and senior management should receive periodic reporting on the firm's resilience risk profile, including emerging risks and trends (market and firm-specific) that may pose a threat to the continuity of critical business services. Their oversight of resilience management activities should include review of reliance on critical third-party providers, including any concentration risks or single points of failure stemming from such relationships.

Implication for firms

- **Board sponsorship.** Provide strong sponsorship, including "tone at the top," to reinforce their expectations for resilience management and to promote an organizational culture of resilience
- **Resilience strategy and risk appetite.** Define a clear enterprise vision and objectives for resilience, and align those to enterprise mission and risk appetite
- **Committee and management oversight.** Embed resilience-related discussions into existing committees and management forums at enterprise, business and functional levels
- **Resilience reporting.** Review and expand on current board and senior management reporting to enable performance measurement against a set of pre-defined objectives and provide transparency into significant risks and trends

There is a common consensus among firms that enterprise resilience is an area that boards need to focus on. However, firms are debating on how to engage their boards in a strategic and informative way, and at what frequency. While many firms currently report on resilience-related matters to their boards, the scope of current reporting is limited to results of testing exercises and major incidents, and does not provide critical insights to proactively identify and manage significant resilience risks and exposures.

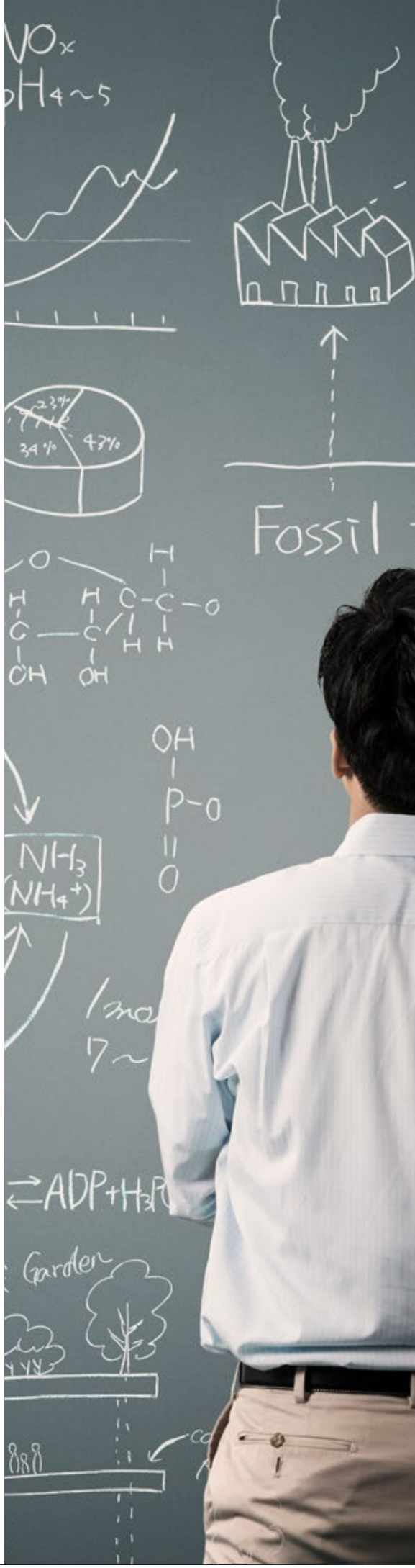
Chapter 4: Next steps expected from regulators

Firms can expect to see continued regulatory scrutiny and focus on resilience, including increased supervisory engagement on this topic. Based on industry working groups and review of the internal audit functions, the industry is waiting to see how the UK regulators update their views on resilience in the next discussion paper expected to be released in Q4 2019. The existing PRA rulebook and the FCA handbook are likely to contain a majority of the baseline regulatory requirements, and additional clarifications of how supervisors will assess operational resilience are expected. Firms can also expect the regulators to finalize their stress-testing approaches on resilience and launch a pilot on stress-testing by end of 2019. In certain instances, we may see regulators making top-line adjustments to firm-defined impact tolerances to encompass impacts from severe market-wide scenarios.

On the US side, firms can expect the regulators to articulate their expectations on resilience as direct feedback to regulatory exams. As firms respond to the regulatory line of questioning and showcase their current and target state capabilities, they have an opportunity to shape-up the regulatory agenda and define the bar on "what good looks like" for key capabilities and focus areas.

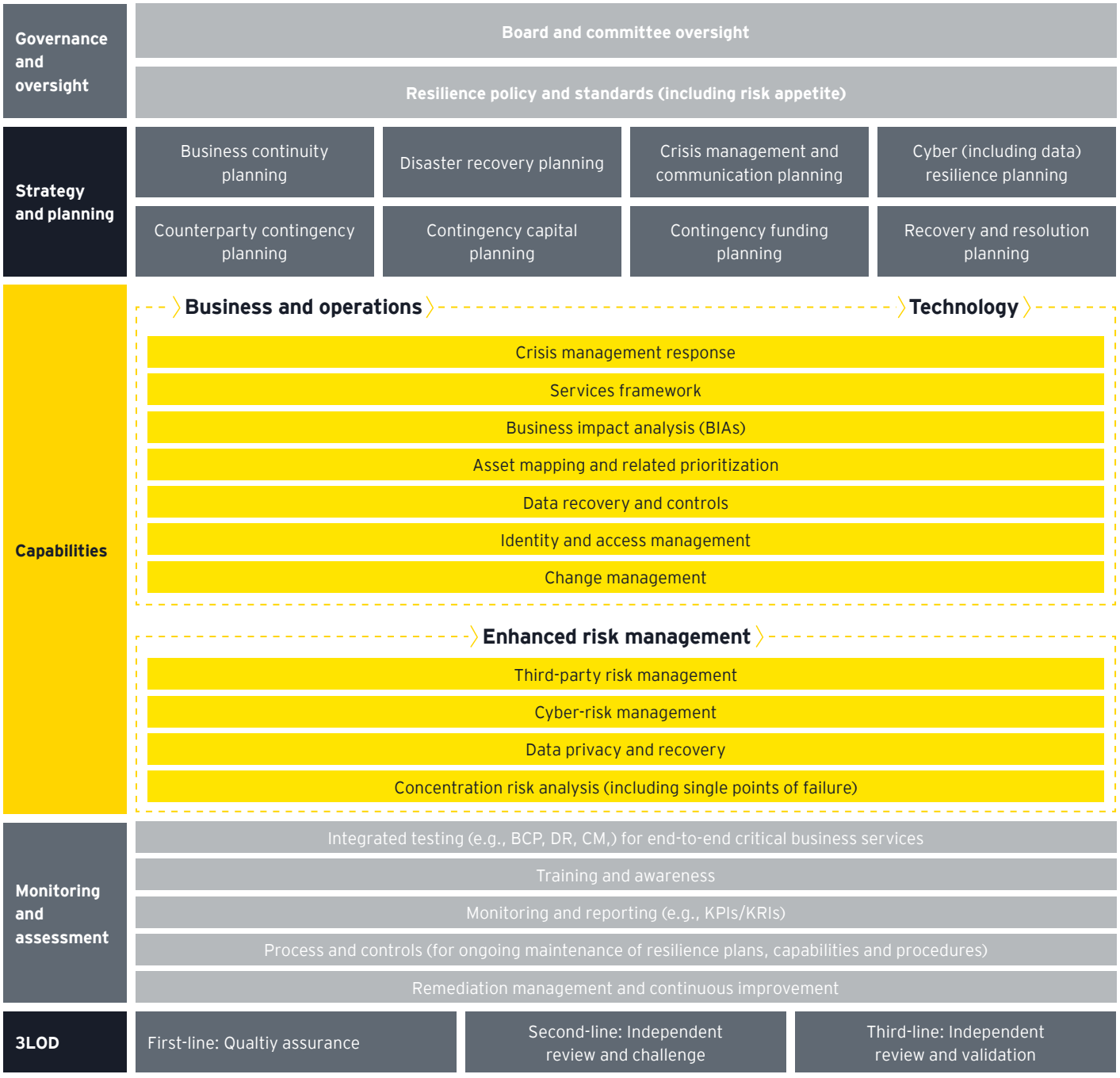
The working group study by the BCBS will also likely articulate the core principles of resilience, which may provide a basis for global regulators to come together on a common core regulatory approach to resilience.

How much the global regulators will converge on their resilience approaches in the future is yet to be seen. However, any divergence in regulatory expectations due to jurisdictional differences will have to be reconciled, especially for global firms, given the cross-jurisdictional nature of business services and the supporting infrastructure.



Chapter 5: Next steps for firms on how to get started

EY resilience framework: Full suite of capabilities to demonstrate enterprise resilience



Firms can undertake the following measures to enhance and transform their existing framework and capabilities to become more resilient:

1. Perform a **maturity assessment** on current state resilience capabilities against regulatory expectations and industry leading practices

2. Define an **enterprise strategy and framework** for resilience

3. Identify and map the **most critical business services**

4. **Establish and test impact tolerances** for the most critical business services

5. Enhance **board and senior management engagement** over resilience management activities

EY Contacts

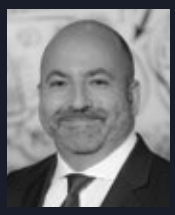
Lisa Choi
lisa.choi@ey.com
+1212 773 8947

Chris Richardson
crichardson4@uk.ey.com
+44 20 7951 1012

Eugène Goyne
eugene.goyne@hk.ey.com
+852 28499470

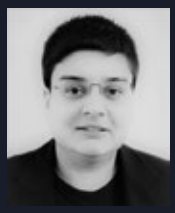
Marc Saidenberg
marc.saidenberg@ey.com
+1212 773 9361

Alex Latorre
alejandro.lattore@ey.com
+1212 773 7694



David Scott
david.scott@hk.ey.com
+852 26293070

John R Liver
jliver1@uk.ey.com
+44 20 7951 0843



Nandini Sud
nandini.sud@ey.com
+1703 747 0143

Rushabh Mehta
rushabh.mehta@hk.ey.com
+852 26293263

EY Global Regulatory Network executive team previous appointments

Kara Cauter
kara.cauter@uk.ey.com

She has over 20 years' experience working in global professional services firms, advising banking clients on the implications of the regulatory agenda and designing approaches to effectively meet those obligations.

Mario Delgado
mario.delgadoalfaro@es.ey.com

FROB (Spanish Banking Resolution Authority) Head of International Coordination and EBA and FSB representative; Spanish Ministry of Economy: Director of Office of the Secretary of State for the Economy in the Economic Affairs; Head of the Spanish Delegation in the Paris Club; Deputy Head of relations with the IMF.

Marie-Hélène Fortésa
marie.helene.fortesa@fr.ey.com

Autorité de Contrôle Prudentiel (French Prudential Supervisory Authority); Association Française des Banques (French Banking Association); and French National Institute for Statistics and Economic Studies. She has also held senior roles at a global investment bank.

Eugène Goyne
eugene.goyne@hk.ey.com

He has over 20 years in government and senior regulatory roles. He was previously deputy head of enforcement at the Hong Kong Securities and Futures Commission (SFC). Prior to the SFC, Eugène worked at the Australian Securities and Investments Commission and the Australian Attorney General's Department.

Kentaro Kobayashi
kentaro.kobayashi@jp.ey.com

He spent 37 years as a financial regulator. He held positions in the National Tax Agency and later, Ministry of Finance (MOF), Japan's former financial regulator. After the establishment of the Financial Supervisory Agency (FSA) of Japan in 1998, he served as Chief Inspector and Inspection Administrator and continued to serve in this role after the FSA was reorganized into the Japan Financial Services Agency in 2000.

John Liver
jliver1@uk.ey.com

Divisional Compliance Lead at Barclays; Head of Department, Investment Firm Supervision and prior roles in enforcement and supervision of investment management, life insurance and pensions at the UK Financial Services Authority and its' predecessors. He is currently EY/UK Financial Conduct Authority relationship lead.

Shane O'Neill
soneill2@uk.ey.com

He has 20 years experience in banking, capital markets, asset finance and prudential regulation in a variety of CFO, COO, strategy and planning, and regulatory roles. Following the financial crisis, Shane was Head of Banking Supervision at a Eurozone Central Bank for four years, during which he influenced significant restructuring, recapitalization and change in the banking sector and in credit institutions, and executed numerous stress tests and asset quality reviews.

Keith Pogson
keith.pogson@hk.ey.com

Immediate past President of the Hong Kong Institute of Certified Public Accountants; more than 20 years of experience advising governments and regulators across Asia-Pacific on acquisitions, market-entry strategy and due diligence across banking, asset management and securities.

Marc Saidenberg
marc.saidenberg@ey.com

Senior Vice President and Director of Supervisory Policy at Federal Reserve Bank of New York; Basel Committee Member and Liquidity Working Group Co-chair; involved in the development of supervisory expectations for capital planning, liquidity risk management and resolution planning.

Scott Waterhouse
scott.waterhouse@ey.com

He was capital markets lead expert for large banks at the Office of the Comptroller of the Currency (OCC) and Examiner-in-Charge of the OCC's London Office. He coordinated the supervision of trading, treasury and capital markets activities including Dodd-Frank implementation and Basel Committee requirements.

End notes

[1] US regulators placed emphasis on identifying and articulating recovery time objectives for critical activities, maintaining geographical dispersed resources and routinely testing recovery and resumption arrangements, with the objective of reducing the impact on external parties. See SR Letter 03-09, "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" https://www.federalreserve.gov/boarddocs/srletters/2003/sr0309.htm.

[2] See Committee on Payment and Settlement Systems: Principles for Financial Market Infrastructures: https://www.bis.org/cpmi/publ/d101a.pdf; and the EBA Single Rulebook: Regulatory Technical Standards on Prudential Requirements for Central Securities Depositories: https:// www.eba.europa.eu/regulation-and-policy/market-infrastructures/-/activity-list/MEKsZIcZDf7H/more.

[3] https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2016/ps2116.pdf?la=en&hash=31C2D0A887C1BA2AD005778AEE4C1CD05E8976DE.

[4] FFIEC IT Handbook and individual booklets https://ithandbook.ffiec.gov/.

[5] FDIC Financial Institution Letter (FIL-19-2019): Technology Service Provider Contracts https://www.fdic.gov/news/news/financial/2019/fil19019.pdf

[6] See EBA Single Rulebook: Proposed Guidelines on ICT and Security Risk Management: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[7] https://eba.europa.eu/documents/10180/2551996/JC+2019+25+%28Joint+ESAs+Advice+on+a+coherent+cyber+resilience+testing+framework%29.pdf

[8] "Building the UK financial sector's operational resilience" https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.

[9] Like other jurisdictions, the standard requires firms, at a minimum, to clearly define information-security related roles and responsibilities, maintain an information security capability commensurate with the size and the extent of threats to their information assets, implement controls, and undertake regular testing and assurance of the effectiveness of those controls. See discussion paper: https://www.apra.gov.au/sites/default/files/20180307-Discussion-Paper-Information-Security-Management.pdf; see the draft standards: https://www.apra.gov.au/sites/default/files/draft_prudential_practice_guide_cpg_234_information_security_march_2019.pdf

[10] See "Building Resilience in Three Dimensions", Wayne Byres, Chairman APRA at the Australian Financial Review Banking Wealth Summit; https://apra.gov.au/media-centre/speeches/building-resilience-three-dimensions

[11] ASIC consultation paper 314: Market integrity rules for technological and operational resilience https://download.asic.gov.au/media/5169120/cp314-published-27-june-2019.pdf

[12] The updated BCM guidelines take greater account for interdependencies across a firm's operational units and linkages with external service providers. Firms are also expected to have an independent audit program to regularly review the effectiveness of their business continuity practices. See: https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Consultation-Paper-on-Proposed-Revisions-to-Business-Continuity-Management-Guidelines.pdf

[13] The MAS is proposing to expand the TRM guidelines to include effective cyber surveillance, secure software development, adversarial attack simulation, and management of cyber risks posed by the Internet of Things. Both guidelines reinforce the importance of effective risk management and board oversight. The MAS is also proposing that certain elements of the guidance be made compulsory, such as specific information security measures related to patch management, unauthorized traffic, malware detection and prevention, and access controls. See: https://www.mas.gov.sg/-/media/Consultation-Paper-on-Proposed-Revisions-to-Technology-Risk-Management-Guidelines.pdf


NOx
pH4~5
CO2
O2
A
Fossil fuel
Organic acid
NH3
(NH4+)
N2
ATP+H2O⇌ADP+H3P
Roof Garden
5%
20%
Arc

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

About the EY Global Regulatory Network

Our Global Regulatory Network helps clients find solutions to their regulatory challenges, providing extensive experience, leadership and strategic insights on financial regulation. The network helps EY clients to understand and adapt to the impact of the changing regulatory landscape.

Led by John Liver and Marc Saidenberg, the network comprises more than 100 former regulators throughout the Americas, Asia and Europe, many with senior regulatory experience, including membership in the Basel Committee, the Financial Stability Board, the European Banking Authority, the Federal Reserve Bank of New York and the Japanese Financial Services Agency. The network helps our clients to understand and adapt to the impact of the changing regulatory landscape, advising on such topics as:

- Capital and liquidity
- Recovery and resolution
- Governance
- Risk culture and controls
- Structure
- Conduct

Learn more at ey.com/grn.

EYG no: 005226-19Gbl

BMC Agency
GA 1013405

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/grn