accentureconsulting

OPERATIONAL RESILIENCE IS FINANCIAL RESILIENCE

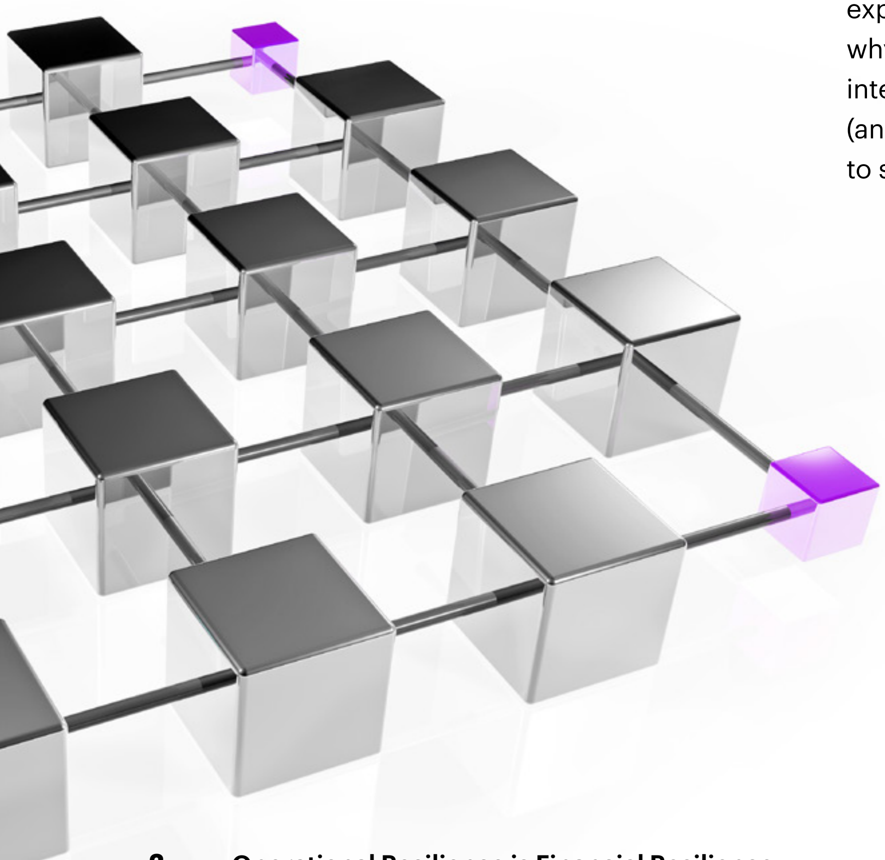
What the Financial Services Industry can do

Operational resilience is arguably now as important to the financial services industry as financial resilience.

With operational and security incidents on the rise (e.g. 219 incidents affecting payments services in the United Kingdom (UK) alone were reported in the last nine months of 2018 according to Out-Law.com),[1] reducing the risk and impact of system outages and building resistance to cyber security threats in financial services is becoming increasingly vital on a global basis.

It is not just financial services institutions (FSIs) and market infrastructure companies themselves who are focusing on operational resilience. Regulators across the globe,[2] too, are increasingly scrutinizing firms' ability to adapt to and recover from operational disruptions, reflecting the central role the financial services industry has in the broader context of society and the wide-ranging impacts that could result when firms fail to operate seamlessly.

With operational resilience high on the agenda for both industry players and regulators, this paper explains what it means for financial services, why regulators across the globe are increasingly interested in it, and some of the steps needed (and some common roadblocks) on the journey to strengthen an organization's resilience.



WHY SHOULD A FINANCIAL SERVICES BUSINESS BE RESILIENT?

#1 Meet evolving regulatory requirements

"The operational resilience of firms and FMIs (financial market infrastructures) is a priority for the supervisory authorities and is viewed as no less important than financial resilience."[3]

Central banks and supervisory bodies are moving to address systemic risks to the financial system through enterprise operational resilience. Following a series of recent high-profile service outages for FSIs, both the Bank of England[4] and the European Banking Authority[5] have issued discussion papers with a view to agreeing and implementing legislation to build up the financial sector's operational resilience. Across the globe other regulators are expected to follow suit.

Operational resilience is defined as "the ability of firms, FMIs and the system as a whole to prevent, adapt and respond to, recover and learn from, operational disruption."[6] Notably, this is a responsibility financial firms already have towards their customers, shareholders and the overall economy under existing legislation and in specific areas like cyber security, risk management and outsourcing.

The objective of the regulators' discussion papers is to now review enterprise operational resilience holistically in light of market and technology changes. These changes include:

- the greater interconnectedness between FSIs and third-party providers (such as cloud services providers) which increases the risk of service incidents;
- the increased sophistication of cyber attacks and the greater potential to disrupt individual FSIs as well as entire markets;
- the dependence on a select group of providers which has the potential to increase concentration risk.

For these reasons, the operational resilience of firms is now even more important than their financial resilience, because a lack of operational resilience could result in financial instability. Regulators are therefore expected to ask firms to define their critical business services and evidence their resilience through joint testing. In addition, a resolvability assessment framework (RAF) has been proposed by the Bank of England to make firms accountable for their own wind-up costs in the event of a catastrophic failure and that can absorb significant financial losses caused by large disruption events.[7]

#2 Reduce risk and impact of outages

"Complexity of Information and Communication Technology (ICT) risks is increasing and frequency of ICT related incidents (including cyber incidents) is rising…"[8]

Enterprise operational resilience is a multifaceted and diverse objective, one that has become more complex in recent years during a period of major technological change. FSIs are developing business services to meet growing customer expectations faster than ever. The need to adapt quickly and accelerate the pace of change increases the risk of outages. Enterprise operational resilience now goes beyond the four walls of an organization, encompassing the entire complex ecosystem of FSIs, partners and third-party providers required to deliver services that meet today's customer needs. Thanks to social media, the public is now aware of both major and minor outages faster than ever. Service disruptions can thus dent firms' reputations with customers, stakeholders and regulators—and impact their bottom lines.

Furthermore, the impact of operational failure is now much more than just a question of system outages. Many FSIs hold ever-increasing amounts of data. And that brings greater exposure to risk where the reliability and validity of that data is threatened by a security breach. FSIs would be expected to have processes in place so that sensitive data remains protected and uncompromised. Disaster recovery is therefore a critical piece of the operational resilience framework, helping to maintain continuity of service and reducing the impact on the FSI's wider ecosystem.

#3 Prepare for security threats

Greater digitalization, interconnectedness and reliance on third parties has increased the financial service industry's vulnerability to external security attacks.

A more hostile cyber environment has intensified the need for FSIs to plan for and mitigate security threats. Unlike many other sources of risk, malicious cyber attacks are often difficult to identify or fully eradicate. The breadth of damage can be difficult to assess: 'successful' data breaches can go undetected for an average of 191 days, and require 66 days on average to fully contain.[9] To make matters more complex, while the threat of an external cyber attack is growing, internal attacks are becoming a major concern. According to a recent study conducted among 472 cybersecurity professionals, 90 percent of organizations feel vulnerable to insider attacks.[10]

WHAT DOES OPERATIONAL RESILIENCE REALLY MEAN?

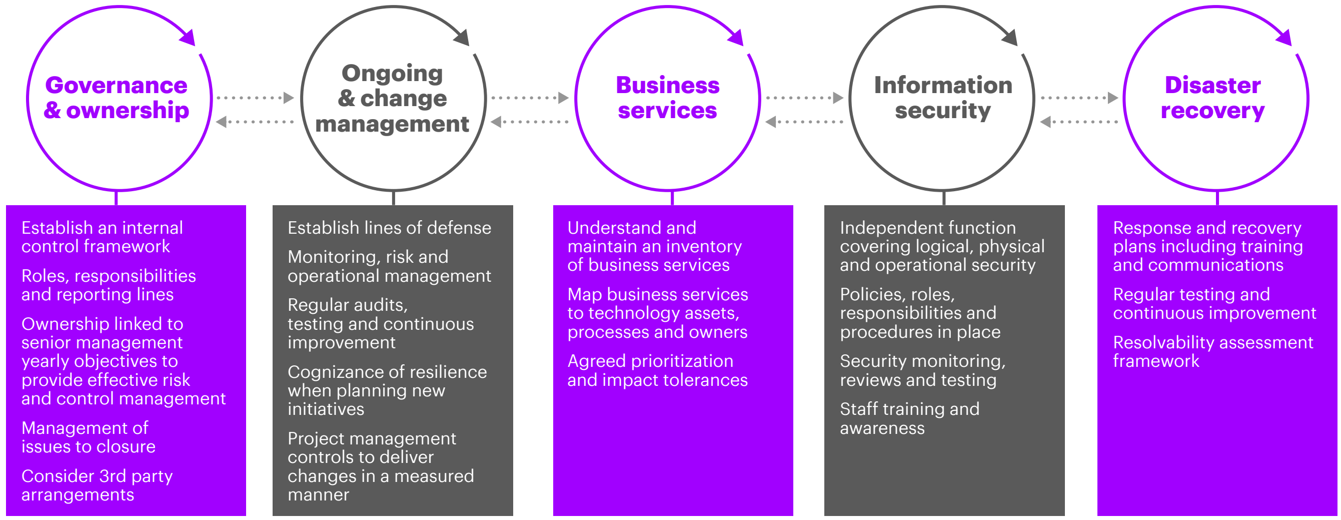
> **"Operational resilience refers to the ability of firms, FMIs and the sector as a whole to prevent, respond to, recover and learn from operational disruptions."[11]**

A resilient enterprise is able to recover its key business services from a significant unplanned disruption, protecting its customers, shareholders and ultimately the integrity of the financial system. Enterprise operational resilience is about more than just protecting the resilience of systems; it also covers governance, strategy, business services, information security, change management, run processes and disaster recovery. Avoiding disruption to a particular system that supports a business service contributes to operational resilience. But ultimately it is the business service itself that needs to be resilient.

A key element of a resilient enterprise is its people. A cultural change is therefore required to make operational resilience a priority across the organization, and that everyone is engaged and working towards that end. This includes training staff to understand what operational risk entails, alongside communication from senior management. Ownership of key risks, and the controls that mitigate them, should be assigned to maintain resilience practices. Remedial actions should be identified and, crucially, completed to create a stronger resilience framework.

In the event of disruption, FSIs should also be able to recapitalize and restructure using their own financial resources. Where there is a catastrophic failure, it is imperative that FSIs can continue to operate and recover while decisions are made on potential restructuring or the closing down of operations to stop further harm. A comprehensive operational resilience framework is key to limiting the impact of failures and providing continued market resilience (not simply resilience within the organization).

Figure 1. Operational Resilience Methodology for Sustainability



Governance & ownership

- Establish an internal control framework
- Roles, responsibilities and reporting lines
- Ownership linked to senior management yearly objectives to provide effective risk and control management
- Management of issues to closure
- Consider 3rd party arrangements

Ongoing & change management

- Establish lines of defense
- Monitoring, risk and operational management
- Regular audits, testing and continuous improvement
- Cognizance of resilience when planning new initiatives
- Project management controls to deliver changes in a measured manner

Business services

- Understand and maintain an inventory of business services
- Map business services to technology assets, processes and owners
- Agreed prioritization and impact tolerances

Information security

- Independent function covering logical, physical and operational security
- Policies, roles, responsibilities and procedures in place
- Security monitoring, reviews and testing
- Staff training and awareness

Disaster recovery

- Response and recovery plans including training and communications
- Regular testing and continuous improvement
- Resolvability assessment framework

Source: Accenture, June 2019

STARTING THE JOURNEY TO RESILIENCE

Making an enterprise resilient is an ongoing journey of continuous improvement.

This journey should start with a discovery phase, then move through assessment, remediation and testing:

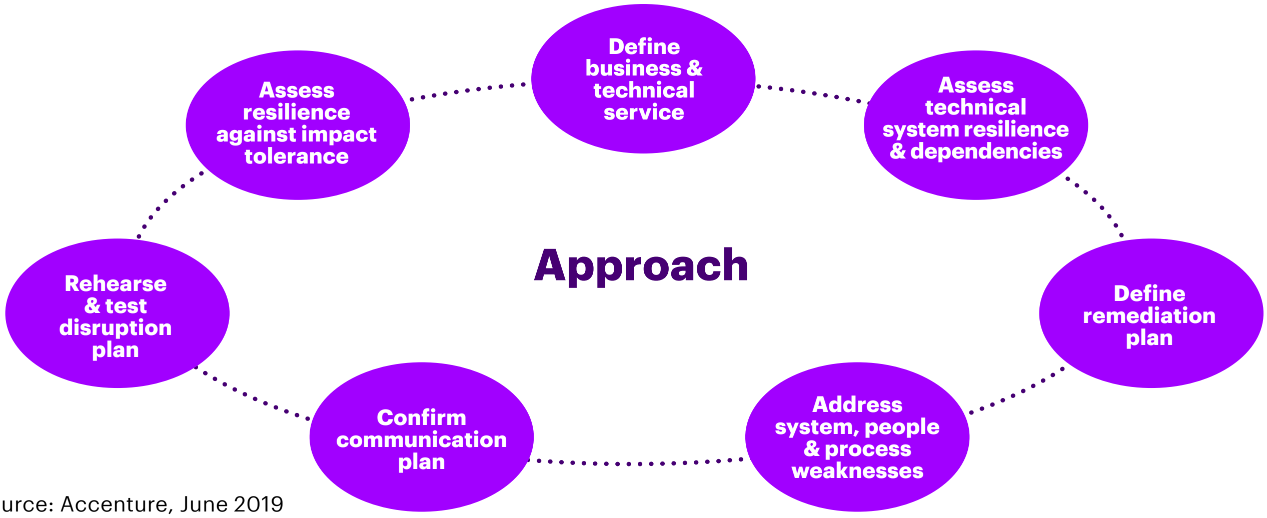
- **Discovery**. The enterprise should begin by documenting its business services and mapping them to the underlying technology (cloud infrastructure, data centers, applications, etc.) and business processes (disaster recovery, cyber-incident response plans, etc.).

- **Assessment**. These underlying technologies and processes are then assessed against Key Performance Indicators (KPIs) or Key Risk Indicators (KRIs). This assessment is used to create a risk score for each business service which is then reviewed against agreed impact tolerances.

- **Remediation**. Using the assessment, a remediation plan is developed which gives priority to the business services with the largest disparity between risk score and acceptable impact tolerance. Having been communicated to the regulators, and aligned with their expectations, the remediation plan is then funded and executed, and the business service is reassessed for resilience.

- **Testing**. An important step in the process is testing, which is also prioritized by the risk materiality of key business services. Penetration team testing and simulating disruption events can advance the enterprise from informed assessments to demonstrating capabilities to stakeholders and regulators. Learnings from testing should cycle back into the resilience assessment process and remediation planning. Equally, remedial actions should be followed back through the testing process to provide completeness.

Figure 2. Operational Resilience Remediation Approach


Define business & technical service
Assess technical system resilience & dependencies
Define remediation plan
Address system, people & process weaknesses
Confirm communication plan
Rehearse & test disruption plan
Assess resilience against impact tolerance
Approach

Source: Accenture, June 2019

COMMON ROADBLOCKS

Priority and culture

A single business service can often extend across numerous technologies and third parties. Take credit transfers, where an FSI might have a mobile application hosted in the cloud, on-premises payments engines, third-party fraud detection systems and a number of middleware and integration components. When premises, cyber crime and people risks are added to the equation, it can be difficult to gather the required data points, map them against key business services and report effectively.

Clearly defined ownership is required to measure, manage and drive resilience for critical cross-team business services. This approach may be new to some organizations but requires prioritization and cultural changes to be effective. Each impacted team should provide input into the assessments, improving and testing "their" component of the business service. Teams should be trained and integrated into the operational resilience framework of the FSI so they have the necessary tools and motivation. As part of this, senior management should prepare for and commit to the resilience agenda and framework and communicate it to impacted teams and third parties.

Investment

Depending on the resilience maturity of the enterprise, the cost of providing operational resilience could be high. However, with increased attention from regulatory bodies, and high-profile incidents and cyber security threats on the rise, this investment in resilience is critical to maintaining and improving business services. As such, FSIs are also expected to:

- regularly assess the operational risks they face in line with regulatory developments and emerging risks;
- analyze potential vulnerabilities; and
- implement appropriate defense mechanisms.

A well-aligned and resilient operational risk management program can not only control volatility and reduce the costs incurred from failures in processes, people and systems, but also unlock and increase the intrinsic value of the firm's operations.

Complexity of legacy systems

FSIs' legacy systems can be complex, as well as difficult and costly to maintain and upgrade. To improve operational resilience, the full stack of these legacy systems (both applications and infrastructure) should be upgraded, patched and assessed for resilience capabilities.

OWNING RISK, CHANGING CULTURE, STRENGTHENING RESILIENCE

Maintaining and improving enterprise resilience is a new way for an organization to build trust with its customers, its regulators and the economy it serves.

Without an effective and comprehensive resilience management framework in place, FSIs may fail to identify and understand, let alone plan for and remediate, emerging internal and external resilience challenges.

Such a framework should have the following essential elements:

1. **Reporting.** Effective reporting of KPIs and KRIs is key to making informed resilience risk decisions.
2. **Testing.** Regular testing and audits (including red teaming and disaster recovery/business continuity testing) should be used to assess resilience levels.
3. **Technology.** Technology assets should be kept up to date and patched appropriately to retain currency to mitigate against cyber threats and out-of-support technology. Major change programs may need to be established to tackle any technology debt.
4. **Tolerance.** Impact tolerances should also be reviewed regularly as business strategies change, customer expectations develop, technology advances and regulations evolve.
5. **Third parties.** Resilience should be an ongoing consideration for third-party contracts and change programs. Resilience goes further than just the immediate organization and extends to all parties that the organization interacts with.
6. **Change programs.** Resilience criteria should be met or committed to before change programs (whether IT or business process) are allowed to proceed.
7. **Communication.** Effective internal and external communication plans should be maintained. The ambition should be to reduce any resilience backlog of lower-priority business services over time.

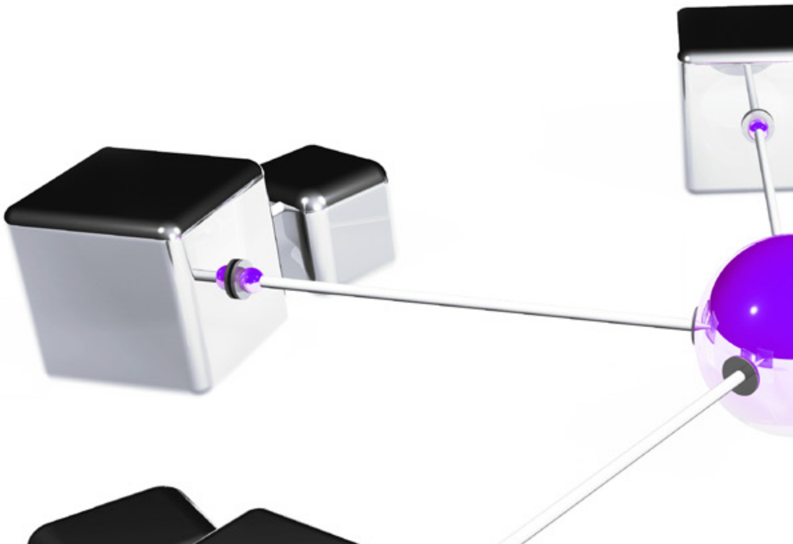
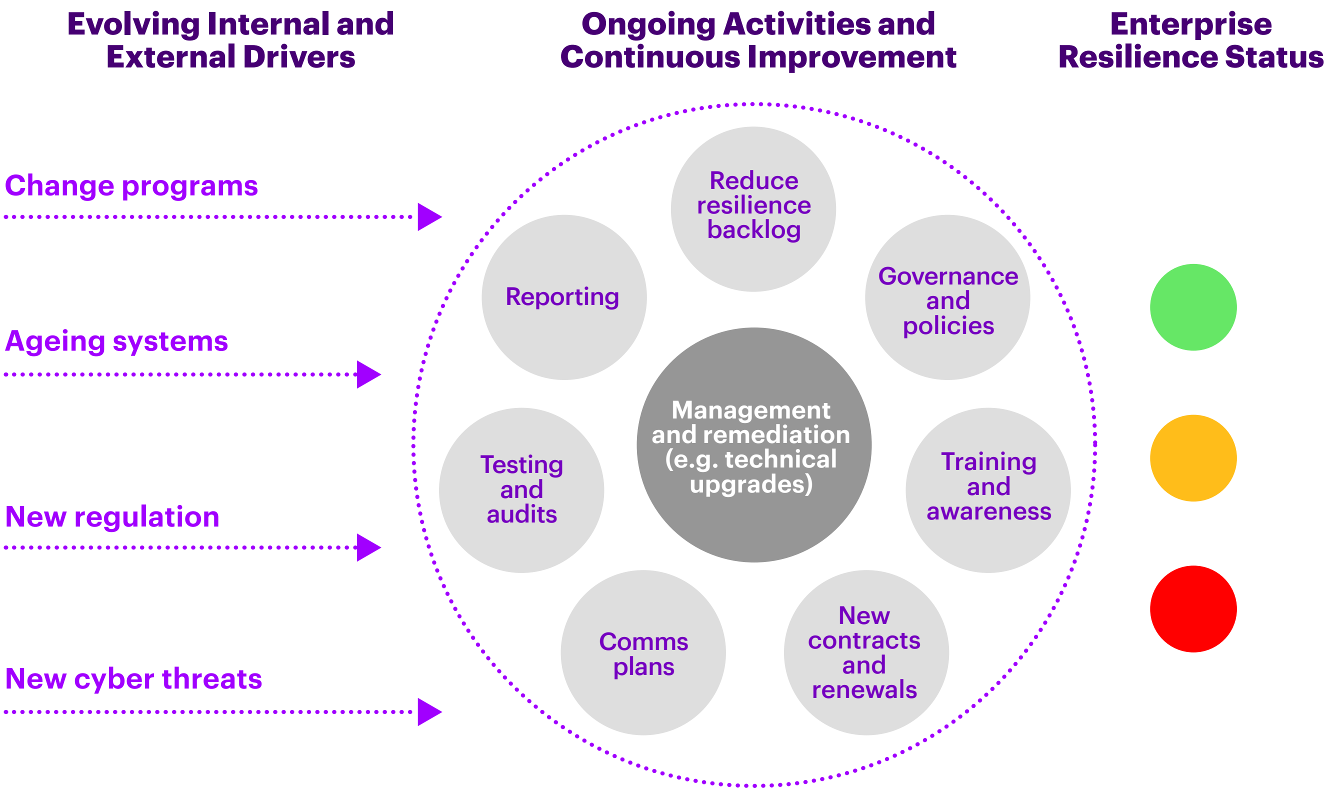


Figure 3. Operational Resilience Management Process


Evolving Internal and External Drivers
Ongoing Activities and Continuous Improvement
Enterprise Resilience Status
Change programs
Ageing systems
New regulation
New cyber threats
Reduce resilience backlog
Reporting
Governance and policies
Management and remediation (e.g. technical upgrades)
Testing and audits
Training and awareness
Comms plans
New contracts and renewals

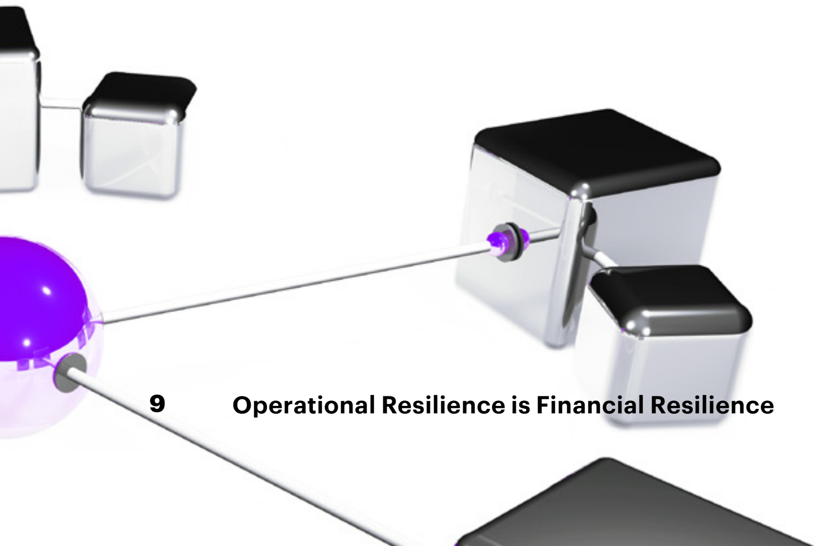
Source: Accenture, June 2019

8. **Disaster recovery.** Disaster recovery plans should not only cover the impact of operational disruption but also extend to the FSI's resolvability, with effective crisis management teams ready to be mobilized.

9. **Cultural change.** A cultural change is critical so that all employees understand the resilience framework, how they fit into it and its importance to the continuity of the enterprise.

10. **Ownership.** Clearly defined ownership of key elements within the operational resilience framework is necessary so that practices are running as they should and responsibility is assigned.

Achieving and maintaining enterprise resilience is crucial for FSIs if they are to meet current and pending regulations, keep up with customer demands and protect the organization against major internal and external service threats.



WHY ACCENTURE

Accenture can help FSIs address all these aims through the combined services and experience of both our Technology Advisory and Finance & Risk practices.

Accenture Financial Services Technology Advisory helps banks, capital markets and insurance firms create business value through technology. We bring deep technology experience, robust security capabilities and blueprints which are specific to the financial services industry. We work with clients to strengthen their cyber and operational resilience capabilities and skills as they drive forward with their digital transformations.

Accenture Finance & Risk works with clients to create and implement integrated risk management capabilities designed to gain higher economic returns, improve shareholder value and increase stakeholder confidence. With over 5,000 Finance and Risk professionals across the globe, we offer extensive experience in operational risk as well as deep risk and compliance capabilities including cyber-risk resilience and surveillance technology solutions.

Points of contact

Colm Kilfeather
Managing Director, Technology Advisory
Technology Advisory Security Lead, Europe, Africa, Middle East, Latin America
colm.kilfeather@accenture.com

Heather Adams
Managing Director, Finance & Risk
Resilience Risk Consulting Lead,
United Kingdom & Ireland
heather.d.adams@accenture.com

Hamish Wynn
Managing Director, Finance & Risk
Regulatory and Compliance, North America
hamish.wynn@accenture.com

Tales Sian Lopes
Managing Director, Financial Services,
Australia & New Zealand
Finance, Risk and Compliance Consulting
Services Lead
tales.s.lopes@accenture.com

Kieran Hanley
Senior Manager, Technology Advisory,
United Kingdom & Ireland
kieran.hanley@accenture.com

Vanessa Duffy
Senior Manager, Finance & Risk,
United Kingdom & Ireland
vanessa.duffy@accenture.com

Claire Aldworth
Senior Manager, Finance & Risk,
United Kingdom & Ireland
claire.aldworth@accenture.com

Elodie de Fontenay
Senior Principal, Technology Advisory
Technology Advisory Offering
Development Lead
elodie.b.de.fontenay@accenture.com

Manish Jaju
Senior Principal, Finance & Risk
Finance & Risk Offering Development Lead
manish.jaju@accenture.com

References

1. Out-Law.com; (01 March 2019); "Banks publish data on operational and security incidents"; retrieved from: https://www.out-law.com/en/articles/2019/March/banks-operational-and-security-incidents-data.

2. Australian Prudential Regulation Authority; (22 May 2019); "APRA releases report on industry self-assessments into governance, culture and accountability"; retrieved from: https://www.apra.gov.au/media-centre/media-releases/apra-releases-report-industry-self-assessments-governance-culture-and. Danmarks Nationalbank; (18 December 2018). The Financial Sector for Operational Resilience's vision is that the Danish financial sector should be best in class in Europe when it comes to countering the threat from cybercrime, so that it can: 1) continue to provide a secure and efficient infrastructure; and 2) support the Danes' continued trust in the digital solutions of the Danish financial sector. Retrieved from: http://www.nationalbanken.dk/en/financialstability/Operational/Pages/default.aspx. Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation; "Enhanced Cyber Risk Management Standards". The Fed out of FRBNY put forward this extension of the supervisory framework laid out by CPMI IOSCO. Additional requirements include governance and management of cyber risks for sector-critical systems. Retrieved from: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf.

3. Bank of England, Financial Conduct Authority, Prudential Regulation Authority; (July 2018); "Building the UK financial sector's operational resilience"; BoE DP01/18; FCA DP18/04; PRA DP01/18; retrieved from: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.

4. Ibid.

5. European Banking Authority; (13 December 2018); "EBA draft Guidelines on ICT and security risk management"; EBA/CP/2018/15; retrieved from: https://eba.europa.eu/documents/10180/2522896/EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf.

6. Bank of England, Financial Conduct Authority, Prudential Regulation Authority; (July 2018); "Building the UK financial sector's operational resilience"; BoE DP01/18; FCA DP18/04; PRA DP01/18; retrieved from: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.

7. Bank of England; (December 2018); "The Bank of England's approach to assessing resolvability"; retrieved from: https://www.bankofengland.co.uk/paper/2018/the-boes-approach-to-assessing-resolvability.

8. European Banking Authority; (13 December 2018); "EBA draft Guidelines on ICT and security risk management"; EBA/CP/2018/15; retrieved from: https://eba.europa.eu/documents/10180/2522896/EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf.

9. TechBeacon; (22 March 2018); "The 30 cybersecurity stats that matter most"; retrived from: https://techbeacon.com/security/30-cybersecurity-stats-matter-most.

10. Cybersecurity Insiders; "2019 Insider Threat Report"; retrieved from: https://www.cybersecurity-insiders.com/portfolio/insider-threat-report.

11. Bank of England, Financial Conduct Authority, Prudential Regulation Authority; (July 2018); "Building the UK financial sector's operational resilience"; BoE DP01/18; FCA DP18/04; PRA DP01/18; retrieved from: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 482,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is **www.accenture.com**

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.