



DESIGNING FOR OPERATIONAL RESILIENCE

Abstract

Operational resilience has always been a crucial topic within financial services and is gaining even more momentum as the landscape becomes increasingly complex. This paper talks about operational resilience based on business services and associated challenges and best practices. It also covers potential uses of next generation technologies, and lessons from other industries to support an organisation-wide resilience programme. There are diverse perspectives from our banking clients and an overall sense emerging that an organisation strongly designed to be operationally resilient could truly differentiate itself in an industry reliant on trust.

Mohit Joshi
President, Infosys Limited

CONTENTS

Introduction	3
Basing operational resilience on business services	5
Mapping of systems and processes to critical services	7
Mapping services to threats and impact	7
Establishing tolerable thresholds for service outages	8
Testing for established thresholds for service downtime	8
Use of next generation technology	9
How banks should manage communications in the event of an incident	10
Ongoing governance framework for operational resilience	11
Leveraging what firms in industries other than financial services are doing	13
In conversation with clients	14
Conclusion	15
References	16

Introduction

Operational resilience has been a critical topic within the financial services sector ever since banking began. However, with the increased variety and volume of industry players, emergence of digital-only platforms, proliferation of FinTech firms, expansion of regulations, increase in complexity of financial instruments and changes in the composition of assets and liabilities, the industry has become subject to increased risks.

Additionally, with new concerns related to privacy, cybercrime, counterparty risk, and interconnectedness of financial systems, the rule-making and supervisory roles that regulators and central banks have in ensuring that all the participants in the financial services ecosystem are operationally resilient, is becoming increasingly complex.

Recent banking examples of service disruptions – ranging from the unavailability of critical banking services such as money withdrawal from ATMs to major fraud such as international money laundering and cyber-crime – repeatedly highlight the problem, which is the lack of a robust, all-encompassing operational resilience programme.

The solution lies in answering the question: is it enough to address the operational resilience challenge by ensuring banking systems and processes are highly available, fool-proof and prepared to absorb shocks, or does more need to be done by ensuring the operational resilience of banking services themselves?



As a preamble to this discussion paper, the services that are central to the noiseless functioning of a mature economy include the following:

 Deposit-Taking and Savings	 Lending and Loan Servicing	 Capital Markets & Investment
<ul style="list-style-type: none"> • Retail current accounts • SME current accounts • Retail savings accounts/time accounts • SME savings accounts • Corporate deposits 	<ul style="list-style-type: none"> • Retail mortgages/other secured (auto) • Retail unsecured personal lending • Retail credit cards • SME lending (secured) • Corporate lending • Trade finance • Infrastructure lending • Credit card merchant services 	<ul style="list-style-type: none"> • Derivatives • Trading portfolio • Asset management • General insurance • Life insurance, pensions, investments and annuities
 Wholesale Funding Markets		 Payments, Clearing, Custody, and Settlement
<ul style="list-style-type: none"> • Securities financing • Securities lending 		<ul style="list-style-type: none"> • Payment services • Settlement services • Cash services • Custody services • Third-party operational services

Source: Bank of England



Financial services, in general, along with the support of market participants, are fundamental and critical for the smooth running of our daily lives, businesses, economies, and countries.

Hence, it is imperative to re-look at operational resilience beyond just ensuring the resilience of applications, systems, business processes, and infrastructure components. It should include identifying

and ensuring the resilience of those critical banking services that the population values and relies on for daily functioning.

Basing operational resilience on business services

Recently, a joint discussion paper has been published by the Bank of England, Prudential Regulation Authority and Financial Conduct Authority titled 'Building the UK Financial Sector's Operational Resilience'.

This paper focuses on the operational resilience of the financial system and the individual firms within it. According to the document, a resilient financial system is one that can absorb shocks rather than contribute to them. The financial sector needs an approach to operational risk

management that includes preventative measures and the capabilities to adapt and recover when things go wrong.

This document has invited commentary and responses from multiple industry participants towards the end of last year, and a few of these are highlighted below:

SWIFT

- SWIFT supports the supervisory authorities' proposed focus on continuity of business services (service resilience)
- SWIFT found the service resilience approach to be the best way of identifying which IT systems have the highest priority, something a 'bottom-up' approach does not properly reveal. This in turn means that firms can drive investment to the right areas
- In today's environment, it is vital to safeguard against operational disruptions and manage related risks. The Business Continuity standard ISO 22317 states: "As the first step in the business impact analysis process, the organisation's top management should agree on the priority of products and services following a disruptive incident which may threaten the achievement of their objectives"

Global Financial Markets Association (GFMA)

- GFMA believes the proposed focus on continuity of business service for operational resilience is appropriate
- However, there should be an acknowledgment that shifting from a system-based approach to a service-based approach is a significant change for financial service firms, based on the stakeholder's effort required to agree on common definitions and complete mapping within an industry-wide and globally applicable context
- The scale and effort required to adapt to the proposed approach will depend on how broadly the final scope is, how 'vital business services' are defined and the number of services that need to be captured

Standard Chartered

- The Bank published a formal response in October 2018 to the Discussion Paper, and while there is broad consensus and agreement, there is clarity the Bank has sought on specific topics including prioritised business services, impact tolerances, the assumption that disruption will occur, Board and Senior Management engagement and Third parties. They also raise two general points: firstly, that clarity and consistency in terminology would simplify coordination across the sector and secondly, stress testing regimes will be vital to prove a firm and the sector's resilience, so principles that guide firms to develop compatible approaches would be beneficial



This new approach has its own challenges, some of which include:



For firms that adopt this service-based approach to operational resilience, specific best practices are as follows

- Establish executive sponsorship and identify senior managers who will own and help proliferate this new approach
- Identify service tolerances, metrics to track variances and approaches to deal with potential issues that may arise
- Create a robust Organisation Change Management framework, identify champions and advocators within the existing delivery teams to drive the new

operational resilience-driven culture – both from within and from outside the resilience function

- Review gaps in the capability available and ensure the right training and knowledge uplift is provided to the people to deal with this new approach

Operational resilience management includes identifying, mapping, assessing, planning, integrating, testing, communicating and governing specific activities to ensure that banks can:

- Identify and mitigate business and system disruption risks before they occur
- Prepare for and respond to disruptive events in a manner that demonstrates command and control of response, coordination and service continuity
- Include scenarios such as cyber security incidents, technology/systems outages and people and process failures
- Recover and restore mission-critical services and operations following an incident within agreed risk appetite levels

System recovery on its own is not an appropriate measure to ensure continuous service availability. Instead, service resilience is a more holistic approach to ensuring operational resilience. A service resiliency approach also helps in identifying which technology assets have the highest priority, something which a traditional approach does not highlight adequately.

The steps required for this approach to work successfully include:

- Defining Critical Services most relevant for clients
- Mapping Processes & Systems to Critical Services

- Mapping Critical Services to Threats and Impacts to the firm and to its clients

These need to be collectively implemented (either as a big bang or in a phase-wise approach) before firms can safely begin a robust operational resilience journey.

Mapping of systems and processes to critical services

Currently, there are very few firms that have fully mapped their existing systems and processes to critical services and leverage established methods to continually update these interlinkages.

The maturity of critical business services mapping, i.e., the linking of business services, processes, systems, owners, etc., tends to vary across organisations. This could, in part, be driven by the automated vs. manual nature of their service management capability. For example, if an organisation uses an IT service management tool for business services mapping, then mapping services is easier than when these are maintained in manual process maps.

Some of the challenges that were discussed earlier apply here as well and are listed below:



Challenges of mapping systems and processes to critical services

- Lack of a common definition of 'critical business services' across the firm
- Global banks have different business service/product mixes in each country
- Inter-dependencies of systems supporting several vital services together across geographies and legal jurisdictions
- Constant changes in the technology landscape, operating models and organisational structures

Mapping services to threats and impact

To protect critical services from disruption, firms should look at the collection of services within their firms and map threats based on the distinct nature of the event

and its impact on the firm and its customers.

An example of this is highlighted below:

 Critical Services	 Type of Threats	 Impact on Firms	 Impact on Customers
<ul style="list-style-type: none"> • Deposits and savings • Wholesale funding • Lending and loans • Payments, clearing, custody, settlements • Capital markets and investments 	<ul style="list-style-type: none"> • Cyber-attacks such as denial-of-service (DoS) • Money laundering • Fraud • Card theft customer data theft through malware • Fake banking apps • ATM fraud 	<ul style="list-style-type: none"> • Loss of revenue • Steep fines imposed by regulators and lawsuits • Lost opportunity • Loss of clients • Loss of credibility and trust 	<ul style="list-style-type: none"> • Interruption in supply / availability of the firm's products / services • Denial of access to cash, credit or other financial services • Loss of personal and sensitive data • Unavailability of a vital link in the customer's personal financial value chain • Personal distress



Establishing tolerable thresholds for service outages

The path to developing acceptable thresholds can be arduous. It depends on the relative maturity of the bank and its state of preparedness. Given the interconnectedness of systems and processes in typical banks, an outage in one service can have a cascading impact on other services. For example, the unavailability of ATM withdrawals because of an outage can result in customers queuing up for money withdrawals at the bank's branch, causing further challenges as the bank may not have planned for additional tellers.

Moreover, given the web of IT systems in a typical bank and the dependencies on financial markets infrastructure (and international operations in the case of truly global banks), the objective of establishing thresholds is more challenging. For instance, banks may want to initially create thresholds for a limited set of local services and incrementally expand the scope over time.

The Bank of England (BoE) has laid out an approach to ensure that banks can quickly recover from outages by setting up preliminary thresholds and minimum recovery standards coupled with extensive stress testing. The key highlights of this approach are:

- The BoE plans to launch a pilot of its approach to stress testing in 2019. The

Financial Policy Committee (FPC) will collaborate with other regulators to establish which firms will be within the scope of the pilot program

- The initial focus will be for payments process. However, the FPC will also identify other areas of concern such as intermediating between savers and borrowers, channelling savings into investment through debt and equity investments, and insuring against and dispersing risk
- The FPC is setting standards for how fast critical financial companies should be able to restore vital services following a cyber-attack. It plans to test these standards against the appropriate response rates through cyber stress tests
- It may be useful to set impact tolerance thresholds that quantify the amount of disruption that can be tolerated during an incident. This way, board and senior management can set their own standards for operational resilience and prioritize and make investment decisions. One example here is the 'maximum acceptable outage time' for a business service. Firms can test their ability to stay within their impact tolerances in severe but plausible scenarios in order to identify vulnerabilities and take mitigating action
- The impact tolerance thresholds being established by the FPC will be based

on the time after disruption to services, which could cause material economic impact. For example, disruption to a bank's payments could have a direct impact on the economy by impacting the ability of customers of that bank to pay for goods and services. But, a severe disruption to a bank's ability to make payments may also have a subsequent impact on other firms that are initially unaffected by the incident. This could impair interbank lending and, in turn, hamper activities such as clearing, settlement or mortgage payments

- The BoE will collaborate with others, especially the National Cyber Security Centre, to test whether firms will be able to meet the FPC's standards for restoring services

Testing for established thresholds for service downtime

Irrespective of the types of threats, banks should be prepared to test critical business services so that they can conform to the availability levels committed to regulators, financial markets infrastructure and customers. These tests will need to be comprehensive and cover physical, software and stress tests (equally for capital adequacy as well as cyber stress-testing). These should also be automated to continuously test for vulnerabilities, availability and fall-back mechanisms.

Use of next generation technology



Model for stress tests based on AI/ML

AI/ML is becoming an important tool for preparing stress-test submissions. Some firms report spending as much as 40% of their total AI budget on risk “in its broadest sense.”

There are some popular examples of AI/ML applications in the financial services industry. For instance, investment banks are using ‘unsupervised learning’ - an algorithm that detects patterns in data that have not been previously labelled — to predict how much capital might be lost and how much capital lies with the bank. Some institutions are using AI to model the performance of their capital markets business in stress tests. Concepts of Driver-based Modelling are beginning to leverage AI / ML to predict high-probability outcomes when banks are faced with complex and interlinked economic changes.



Predict ATM outages using analytics and Machine Learning

Predictive analytics can help banks monitor ATM service performance to determine when a failure might occur. It can even predict 50% of potential ATM failures before they occur. For some banks, this process has resulted in a 2% increase in ATM availability whereby a single ATM location can remain online and serve customers for an additional 10,000 minutes per year.



Reduce bank fraud using data and analytics on the cloud

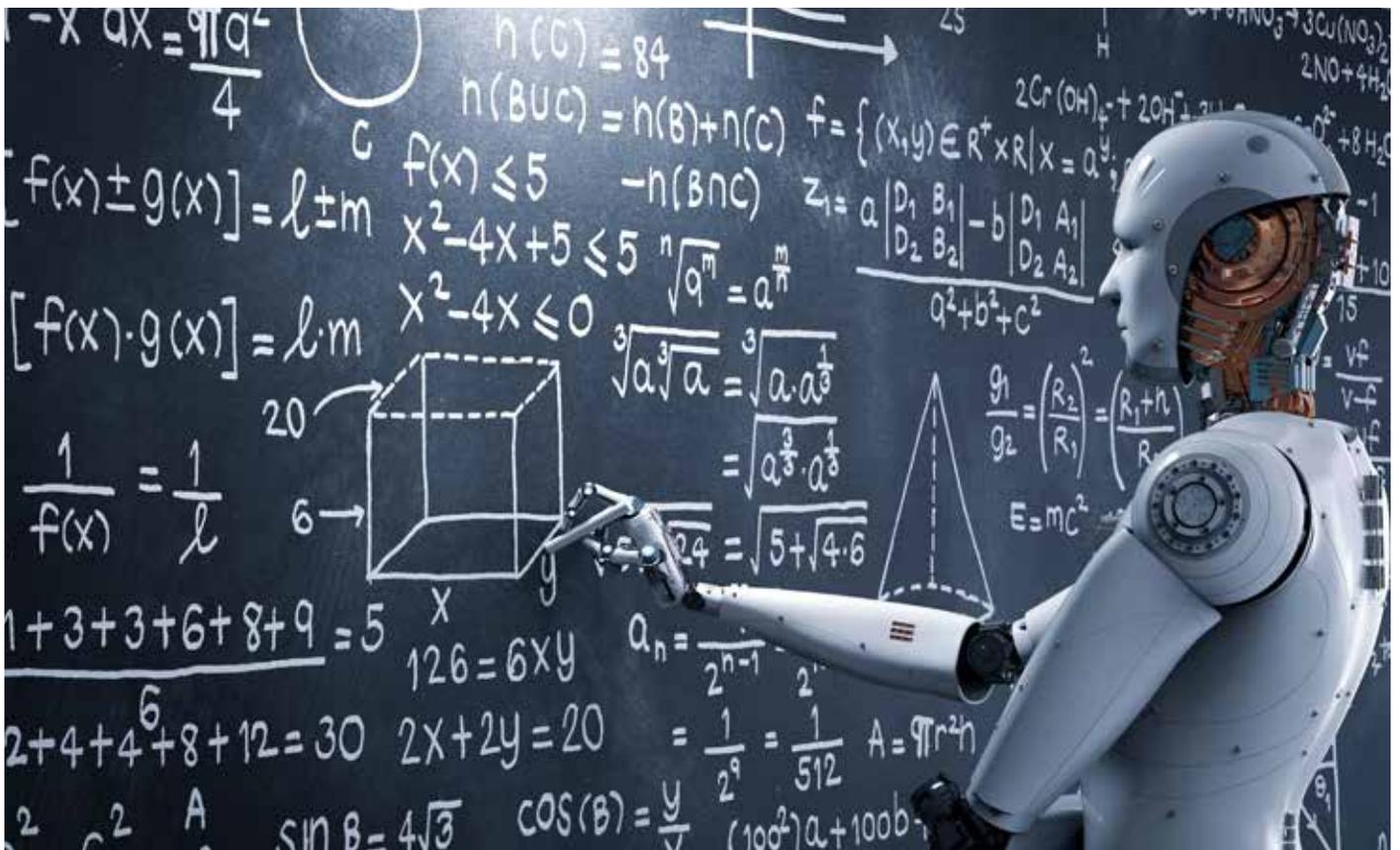
One of UK’s leading banks is looking to leverage a leading public cloud provider and its AI/ML capabilities for deep data analytics e.g. to identify fraudulent transactions in real-time. They plan to combine this data with geographic data

to determine the location of where the fraudulent payments originated and the associated destinations.



Eliminate and automate work-drivers for reducing operational risk, and predict outages

Some leading investment banks and asset management firms are creating an “Insights Fabric” leveraging the power of next generation AI/ML and Visualization tools to predict/prevent the next outage. They do this using platforms that thoroughly analyse the data from monitors, tickets, incidents, problems, user requests, logs, and drive direct / indirect correlations to understand underlying root causes. These root causes are then used to drive elimination / automation across the technology estate. This in turn reduces complexity, risk, and overall number of outages, thereby improving operational resilience.





How banks should manage communications in the event of an incident

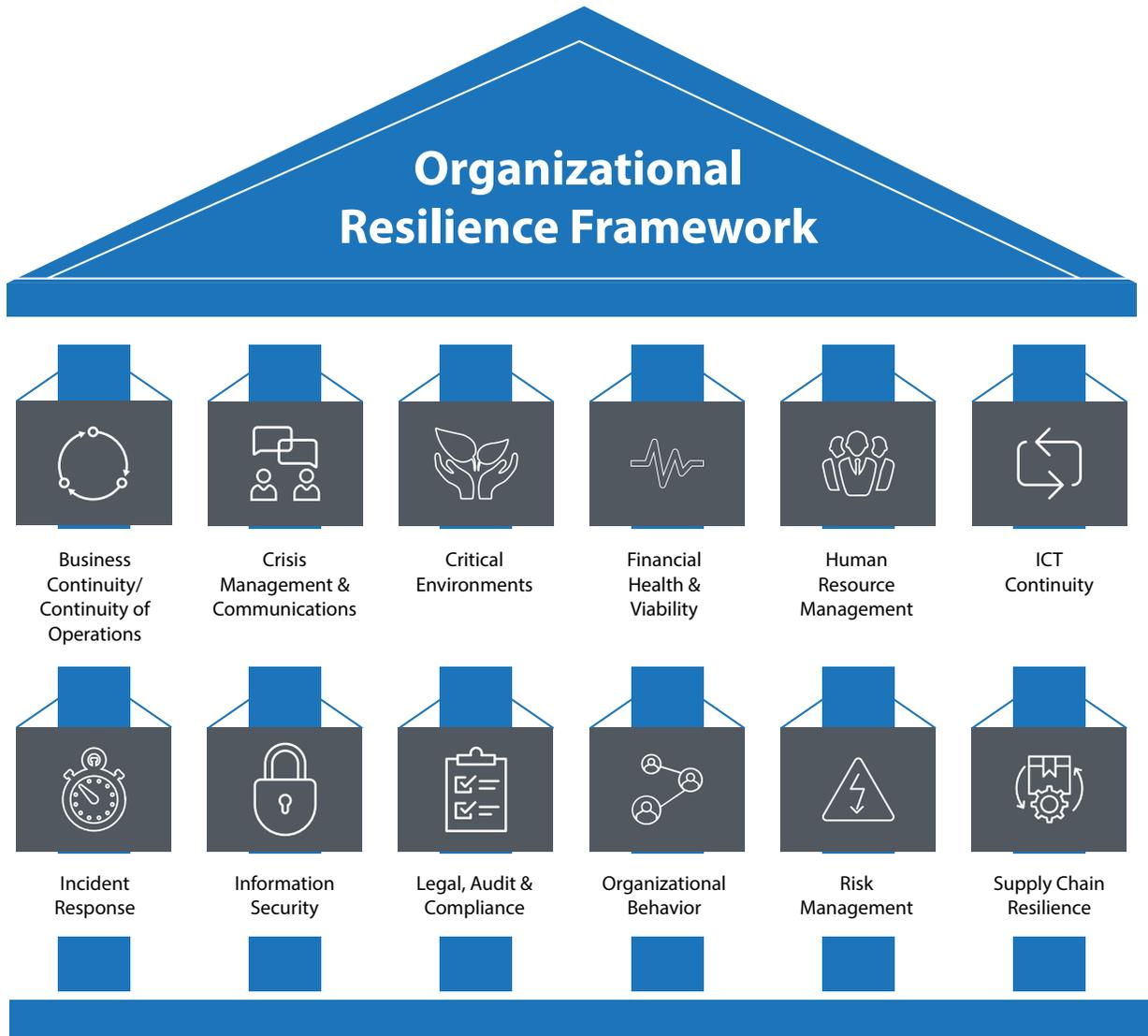
In the event of a threat, outage or total blackout, firms must be prepared to communicate internally and externally with precision and planning. An operationally resilient firm should have an effective internal communication plan, well-defined escalation paths and identified decision-makers in place. There needs to be an established hierarchy of communication based on the type and level of threat or outage with clearly-defined players and responsibilities leading up to senior managers and executives within the firm.

Firms should also have documented and effective communication plans for external stakeholders, customers, market participants, and regulators with clearly identified timelines on the timing and frequency of such communications. Such a plan can help avoid panic and anxiety internally and externally when a breach or a total outage has occurred.

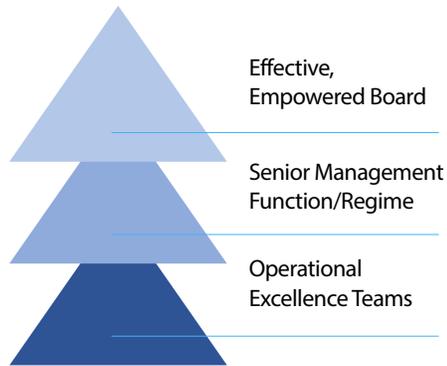
The communication plan should address how to get hold of key people, how to contact operational staff and how to contact consumers, suppliers, and supervisory authorities as in the case of a disaster recovery or business continuity plan. It is important that business continuity policies include prompt and meaningful communication arrangements for internal and external parties including supervisory authorities, consumers, other clients, and the media where necessary.

Ongoing governance framework for operational resilience

Several organisations have adopted elements of the comprehensive 12-discipline framework created by the International Consortium for Organisational Resilience (ICOR), to establish their operational resilience framework.



A recommended governance structure for operational resilience is illustrated below:



- There must be an effective and empowered board that can exercise appropriate oversight and be confident that their directions are carried out. This requires effective internal controls for prioritization, undertaking specific activities, reporting, and escalation
- The senior management must ensure that the resilience framework established/signed off by the board has been adequately communicated across the firm and that proper governance has been established to track and report implementation
- Operational excellence teams must ensure that resilience frameworks are being actively implemented across disciplines

The European Banking Authority (EBA) as of September 2018 has been working extensively on a regulatory framework for mitigating key resilience risks. The salient points of this framework are:

- In line with its mandate to ensure effective and consistent prudential regulation and supervision across the European financial sector, the EBA has undertaken several initiatives to adjust the regulatory framework and promote consistent supervisory practices for payment as well as financial institutions including in the field of cybersecurity

- While some pieces of the work are still in the pipeline, the regulatory and supervisory framework related to operational resilience is built around the following three areas:



Regulation: Strengthening governance and risk management arrangements

- In the area of regulation, the EBA has published guidelines on internal governance (at the start of 2018) specifying internal governance arrangements including risk management, business continuity management and outsourcing. Around the same time, they also completed the 'EBA recommendations on outsourcing to cloud service providers' as a very specific response to uncertainty in cloud adoption
- In the area of payment services, the EBA has published guidelines on security measures for operational and security risks, guidelines for the notification of major operational and security incidents, and guidelines on fraud reporting requirements



Supervision: Common framework for supervisory assessment and knowledge sharing

- Supervision plays an important role in evaluating the resilience of individual institutions and financial systems. As a practical contribution to this process, the EBA had published guidelines in 2017 for supervisors on the assessment of ICT risk as part of the supervisory review and evaluation process. They also organized several workshops and training events to support knowledge sharing



Resilience testing: Sound and proportionate resilience testing

- As an extension of the supervisory activities, the third component of operational resilience is the resilience testing. At a country level, the UK and the Netherlands have established their own respective exercises. This year, the European Central Bank (ECB) published its 'European framework for threat intelligence-based ethics (TIBER-EU)' aimed at testing and improving the entities' resilience against sophisticated cyber-attacks in the EU. The European Commission's FinTech action plan has mandated that the three European supervisory authorities – EBA, ESMA and EIOPA – evaluate the need for a coherent threat testing framework at EU level for significant entities



Leveraging what firms in industries other than financial services are doing

There are several examples of how firms in industries apart from financial services are managing operational resilience. Some of these are highlighted below.

Overcoming probable bottlenecks

When General Motor's supply chain was disrupted by the 2011 earthquake in Japan, GM was able to quickly redeploy the reduced supply of parts to its key division.

General Motors had leveraged its experience from prior incidents that had disrupted its supply chain and initiated a program to increase its resiliency. GM's resiliency protocol includes a conference call every Wednesday at 5:30 a.m. in Detroit to discuss potential supply bottlenecks and how to mitigate them. Within 24 hours of the earthquake, GM had set up a war room that analysed which plants, vehicles and parts supply chains were affected. They also knew how each vehicle line would be affected and the effect on the bottom line.

Based on the data available, they took decisions on how to shuffle parts among vehicles, plants, countries, and continents to keep their most important assembly lines working.

Implementing secure systems

Organisations should focus on creating safe management systems and applications so that reliability and performance of systems remain unaffected during distress and disruptions. Addressing cybersecurity incidents is a key task in the airline industry with Changi becoming the first airport in the Asia Pacific region to work with SITA to achieve ISO certification for information security.

Creating a Business Continuity Plan (BCP)

A robust BCP can help alleviate business interruption and ensure protection of assets. The main objective is to recover all business-critical processes and minimize the impact on employees, customers and organisation. For example, a retail company developed a BCP focusing on retail risk, service risk, employee health, etc., and created metrics and

organisation structures to assign ownership, identify threats and resources, and develop contingency plans and policies.

Creating Digital Twins for clients

Companies like Sanofi and GE have been involved in creating Digital Twins to not only operate their machinery much more efficiently and effectively but to also significantly reduce operational risk associated with working these machines.

For example, each of Sanofi's super-modern plants has a 3D computer model of the actual plant, called a "digital twin," that monitors all of the data and provides plant managers with a real-time view that allows them to make adjustments on the fly.

In Geel, the French drug-maker says it has installed sensors that measure more than 5,000 parameters along the production process. Those can be analysed to quickly spot and correct issues to keep yields high and to allow for predictive maintenance on equipment.





In Conversation with Clients

In discussions with Juan Colombas, Executive Director and COO of Lloyds Banking Group, and other industry leaders, additional perspectives emerged at the time of writing this paper.

Firstly, Banks should look at resilience of services that truly matter to clients and where their regular, day to day functioning is impacted. As an example, a mortgage application process affected for a few days may not be as critical as payments getting rejected at the point of sale in a supermarket. It is crucial to take the client-centric nature and relevance of the business process into account while building plans for resilience. Geographic spread of customer-base also plays a critical role in determining the extent to which banks need to prepare for operational resilience.

Secondly, this is an industry-wide problem and needs to be tackled collectively – a few banks being exceptional at operational excellence is not enough for resilience of the overall industry.

Thirdly, there are factors which will be beyond the financial service industry's control but need to be considered while strategising for firm-wide operational resilience. Examples include disruptions to national infrastructure, tsunami-like events causing widespread havoc, Black Monday-like events causing exchange closures, and several others of a similar nature.

Fourthly, while technologies such as AI / ML enable banks to leverage data in order to improve resilience, it is not a shortcut that will address the entire issue on its own. One needs to establish the foundations of operational resilience management first, such as understanding business critical processes, defining risk appetite and governing it at the top of the organisation.

And finally, the biggest enabler (or inhibitor depending on the perspective) for successfully creating an organisation-wide operational resilience framework is culture.

Conclusion

Operational resilience needs to be a critical feature in every financial firm's overall strategy. All firms should review critical services they perform for their customers, the threats they expect currently and in the future that can disrupt their business, and linkages of these threats to critical services, systems and business processes.

Recent high-profile disruptions to banks' technologies have demonstrated the need to over-engineer solutions for resilience and to monitor risks and threats on an ongoing basis. In fact, we believe clients will compensate firms that are well-prepared with increased trust, brand recognition and loyalty.

The opposite is also true however: without a systemic adoption of this services-led operational resilience approach, the pace at which business models are

evolving, FinTechs and non-banks are proliferating the industry and the pace of technology changes, it will expose multiple vulnerabilities within banking. It is down to the management of the resilience agenda that will allow banks to sustain themselves in the future.

The Prudential Regulation Authority (PRA)/Financial Conduct Authority (FCA) recognizes that embedding operational resilience within firms is a significant undertaking. Therefore, to start with, firms should build the foundational blocks for overall resilience. Moreover, firms should leverage tremendous opportunities provided by PSD2/open banking and disruptive technologies like AI/ML.

Preparing for operational resilience presents firms with opportunities to create multiple dialogues with markets, regulators, customers, shareholders, and investors alike that they are preparing their

firms for long-term sustainability and are protecting interests of all the participants of the financial system in entirety.

Firms should look beyond financial services for examples as they prepare for a step change in their resilience frameworks. There are proven examples from industries like manufacturing, retail, logistics and the airline industry that are able to tolerate risk and guarantee high availability of their core services, irrespective of disruptions

Finally, this a tough challenge for all banks to tackle and there is a clear need for collaboration and cooperation to build resilience of the financial services industry as a whole. Cultural transformation within organisations needs to play a significant role as a precursor to the creation of a strong and solid operational resilience foundation on which banks can face future uncertainty with much more confidence.



References

- <https://av.sc.com/corp-en/content/docs/discussion-paper-operational-resilience.pdf>
- www.gfma.org/WorkArea/DownloadAsset.aspx?id=1028
- <https://www.swift.com/resource/building-uk-financial-sectors-operational-resilience>
- <http://www.eachccp.eu/wp-content/uploads/2018/10/EACH-response-UK-PRA-FCA-and-BoE-DP-on-Building-the-UK-financial-sectors-operational-resilience-OCT18.pdf>
- <https://www.world-exchanges.org/storage/app/media/regulatory-affairs/Recent%20publications%202018/WFE%20Response%20to%20BoE%20on%20Operational%20Resilience%20-%205%20October%202018.pdf>
- <https://www.eba.europa.eu/documents/10180/2373079/Slavka+Eley+-+Speech+on+the+Regulatory+Framework+for+Mitigating+Key+Resilience+Risks+270918.pdf>
- <https://bnpparibasgt.taleo.net/careersection/gt/jobdetail.ftl?job=IT-110618-002-CR&lang=en>
- <https://www.out-law.com/en/articles/2018/june/cyber-stress-tests-payments-2019/>
- <https://finadium.com/boe-committee-setting-standards-with-stress-tests-for-cyber-resilience/>
- <https://in.reuters.com/article/us-boe-banks-regulator/boe-to-ensure-banks-recover-quickly-from-it-troubles-idINKBN1J90WE>
- <https://www.bankinfosecurity.asia/rbi-issues-new-cybersecurity-guidance-a-9169>
- <https://www.pwc.co.uk/financial-services/assets/pdf/fpc-plans-operational-resilience-stress-testing.pdf>
- [https://www.ey.com/Publication/vwLUAssets/ey-response-to-building-the-uk-financial-sectors-operational-resilience/\\$FILE/ey-response-to-building-the-uk-financial-sectors-operational-resilience.pdf](https://www.ey.com/Publication/vwLUAssets/ey-response-to-building-the-uk-financial-sectors-operational-resilience/$FILE/ey-response-to-building-the-uk-financial-sectors-operational-resilience.pdf)
- <https://www.ft.com/content/0dca8946-05c8-11e8-9e12-af73e8db3c71>
- [https://www.icao.int/MID/Documents/2017/ACAC-ICAO%20GNSS%20Workshop/Cyber%20Security%20\[Compatibility%20Mode\].pdf](https://www.icao.int/MID/Documents/2017/ACAC-ICAO%20GNSS%20Workshop/Cyber%20Security%20[Compatibility%20Mode].pdf)
- <https://www.sita.aero/pressroom/news-releases/sita-completes-iso-certification-for-information-security-at-changi-airport>
- https://www.caa.co.uk/uploadedFiles/CAA/Content/Accordion/Standard_Content/Commercial/Airports/Files/Increasing%20airport%20resilience%20seminar%20paper.pdf
- https://www.strategyand.pwc.com/media/uploads/Strategyand_Managing-Airport-Disruption.pdf
- https://ac.els-cdn.com/S1877705818301838/1-s2.0-S1877705818301838-main.pdf?_tid=760043ac-715a-4230-8acc-f11960f883dd&acdnat=1543829303_41a67b6c942a586df298609a72b75588
- <https://www.fiercepharma.com/pharma/sanofi-s-shift-to-robots-and-digital-twins-at-u-s-biologics-site-costs-95-jobs>

For more information, contact askus@infosys.com



© 2019 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.