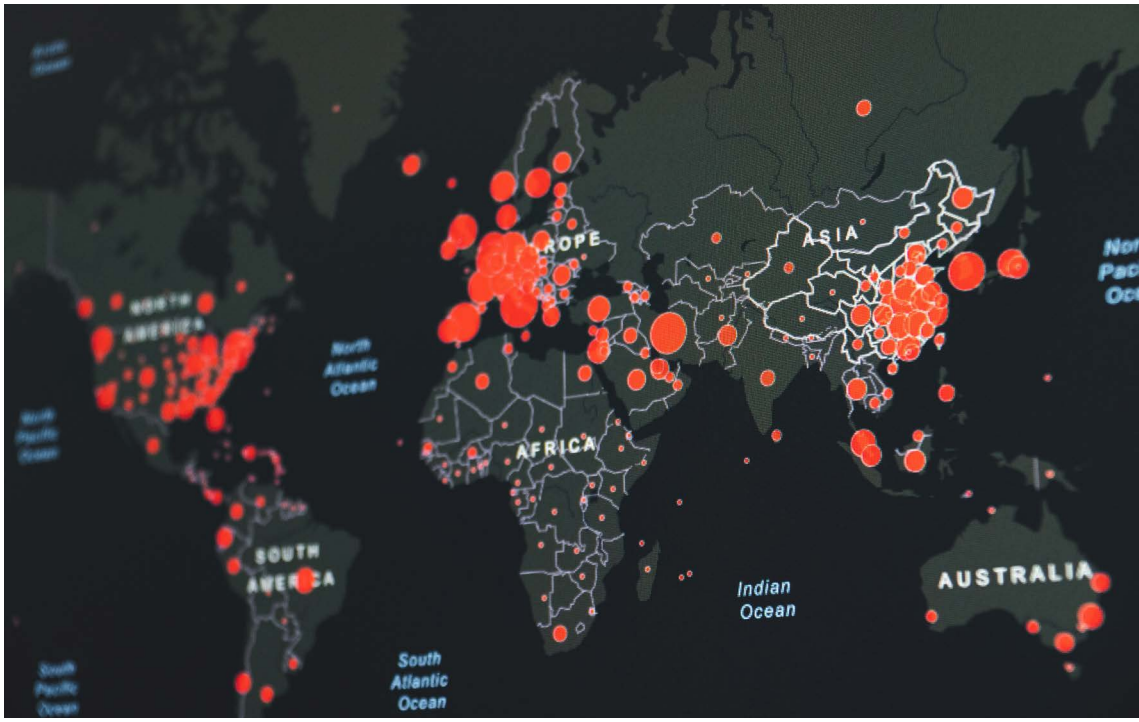
Operational resilience

What it means and how to achieve it

Risk Universe by RiskBusiness



This report will look in detail at what is meant by operational resilience and how firms should address the following key components which collectively make up an operational resiliency programme:

- Business continuity planning (entities, processes and locations/assets)
- Disaster recovery (business applications, data centres and hardware)
- Evacuation planning
- Crisis management planning

Each component has a different focus, and it is useful to contemplate these differences when designing or evaluating your own programme. Business continuity focuses on keeping the business going; disaster recovery focuses on keeping IT-related assets going; evacuation planning looks at how to keep people safe or get them to safety; while crisis management determines how management responds to any form of crisis.

A fire might require evacuation, crisis management and business continuity, while a system defect may require disaster recovery and business continuity. Bad press coverage may require crisis management, but not require any business continuity, disaster recovery or evacuation planning.

WHAT IS MEANT BY OPERATIONAL RESILIENCE?

The UK's Financial Conduct Authority (FCA) defines operational resilience as "the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from operational disruption."

The past two years have certainly presented the industry with plenty of operational disruption to respond to, recover and learn from. Though it may feel like the pandemic is a distant memory for some parts of the world, many nations are still implementing lockdowns and are yet to return to business as usual.

As should always be the case, firms are updating and adapting their operational resilience efforts to meet today's challenges. "Achieving operational

resilience requires an ability to continuously assess and react to our changing environment and circumstances," says Mike Finlay, CEO of RiskBusiness. "We are still dealing with the impact of Covid, with many offices still relying heavily on remote working. The Russia-Ukraine conflict has created additional complexities with firms being required to keep on top of increasing sanctions and disruptions to supply chains. Recent extreme weather conditions in Europe, the UK and the US have resulted in staff working from home again, while the political and economic crisis in Sri Lanka has seen branch operations reduced to one day a week in many locations. Operational resilience isn't a new concept of course, but is something firms should always be thinking about; building a framework of defence that protects our ability to operate though all eventualities - including scenarios we have already experienced and those that are lurking in the unknown."

REGULATION AROUND OPERATIONAL RESILIENCE

The global pandemic has had an operational impact on every area of business, with finance being no exception. Financial regulators are focussing on areas of weakness exposed by Covid and other recent events. New regulation is currently being developed in the UK and EU to address the growing reliance on digital capabilities, in particular those provided by third-party organisations; plus fraud prevention, IT security, cybercrime and incident management.

In March 2021, the UK's Financial Conduct Authority and Prudential Regulation Authority released a joint statement on operational resilience requirements:

"The policy requires firms and FMIs to set, and take actions to meet, standards of operational resilience that incorporate the public interest as represented by supervisory authorities' objectives. Firms and FMIs should focus on their important business services and ensure they have the ability to remain within impact tolerances in severe but plausible (or extreme) scenarios. Firms will be required to map the resources, people, processes, technology and facilities necessary to deliver important business services, irrespective of whether or not they use third parties in the delivery of these services, and test their ability to remain within their impact tolerances."

In October 2020, US financial regulators (Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency) also released a joint paper on operational resilience:

"In recent years, firms have experienced significant challenges from a wide range of disruptive events including technology-based failures, cyber incidents, pandemic outbreaks, and natural disasters. While advances in technology have improved firms' ability to identify and recover from various types of disruptions, increasingly sophisticated cyber threats and growing reliance on third parties continue to expose firms to a range of operational risks. These operational risks underscore the importance for firms of all sizes to strengthen their operational resilience.

The global pandemic has had an operational impact on every area of business, with finance being no exception

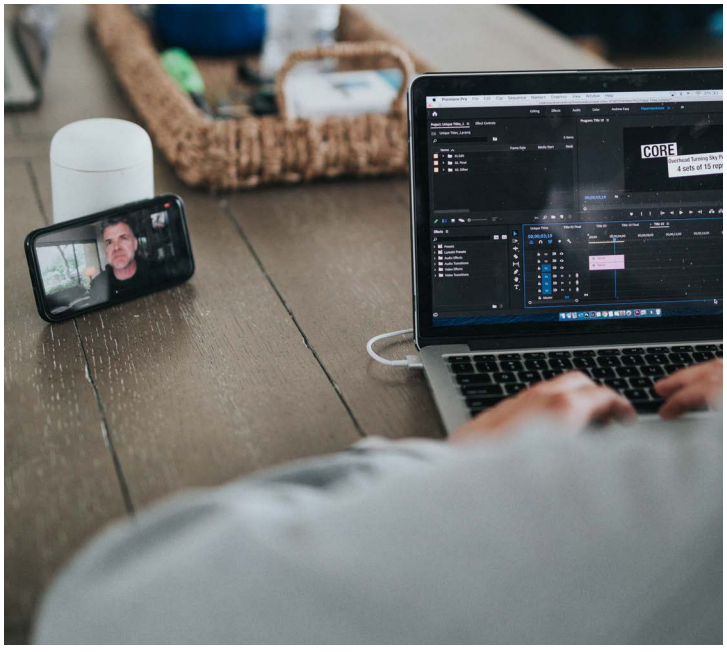
The focus is on how the firm's staff continue to deliver business services and products

While potential hazards may not be prevented, the agencies consider that a flexible operational resilience approach can enhance the ability of firms to prepare, adapt, withstand, and recover from disruptions and to continue operations."

Many other regulators around the globe have released similar statements since 2020 in an attempt to shore up the world's financial system against future global risk events. In this report, we look at four key areas for firms to address in their objective to achieve greater operational resilience.

1 BUSINESS CONTINUITY PLANNING

Business continuity planning (or, as it is often referred to, business continuity management) refers to the framework put in place by firms to ensure that entities, processes and assets/locations are protected and able to function in the event of a disaster or risk event. Covid proved that many day-to-day functions can continue to operate using remote capabilities (more on this in Disaster Recovery below) and that hybrid office/home working options can work effectively.



The focus is on how the firm's staff continue to deliver business services and products to the firm's clients in an effective and controlled manner without significant service or quality depredation. A comprehensive business continuity plan typically addresses loss of staff, process failures or processes which cannot be performed, IT and equipment failures, offices and facility loss, and local area disruptions or closures, etc.

An integral part of protecting a firm's entities and processes is ensuring that contingencies are in place in the event of any external or third-party services experiencing an outage or disruption. This has become an area of focus for many financial regulators of late, particularly in the area of digital resilience.

DORA AND THE UK EQUIVALENT

The EU has provisionally agreed to pass the Digital Operational Resilience Act (DORA) which has similar objectives to proposed regulation in the UK. Both DORA and the UK equivalent aim to mitigate risks posed to financial stability by the heavy reliance of financial firms on a small number of third-party providers.

CRITICAL THIRD PARTIES

Firms depend too heavily on a handful of suppliers who provide critical services

(such as cloud service providers). If any of these providers were to suffer a major outage or data breach (like the recent Solar Winds attack for example) it could pose a systemic risk to the entire global financial system.

In an attempt to address this risk, EU and UK regulators want to be able to directly oversee the services provided by Critical Third Parties. In the UK, HM Treasury will determine which third parties qualify as "critical," using input from financial regulators, the third parties themselves and the firms who use their services. The Bank of England and the FCA have released a discussion paper which sets out how the supervisory authorities could use their proposed powers to assess and strengthen the resilience of services provided by critical third parties to firms, with the objective of reducing the risk of systemic disruption.

AUSTRALIA: REACTING TO THE ASX OUTAGE

Elsewhere in the world, third parties are also getting the full regulator treatment. The Australian Securities and Investments Commission (ASIC) published a report in November 2021 which detailed the regulator's expectations for the industry when dealing with a major disruption to services. The report was published as a response to a specific market outage and other operational incidents that affected the Australia Stock Exchange (ASX) equity market in November 2020.

ASX relies on technology provided by Nasdaq to complete trade transactions. The outage, which resulted in an almost a day-long halt to trading, was caused by a software fault that affected the tailor-made combinations (TMC) order book. Though ASIC found that the ASX did follow its procedures for incident management during the event, it concluded that "further

CASE STUDY

UKRAINIAN BANKING SYSTEM

The Ukrainian banking system provides a great working example of how financial institutions must continuously adapt in order to maintain operational resilience. In an opinion column for *FinTech Magazine*, Hanna Khrystianovych, Ukrainian national and fintech program manager at Sigma Software Group, talks about how the financial industry has learned from risk events over the years: "Since 1991, when Ukraine became an independent and free state, we have faced two revolutions, global financial crisis, the annexation of the Crimean peninsula and the war in the East, and the Covid-19 pandemic," she says. "Every two to four years, Ukrainians have witnessed some shocking events that have influenced their lives at an extreme level."

She describes the preceding events as like a "warm-up" exercise for banks, in particular the cyber attacks that bombarded Ukraine in the lead-up to the Russian invasion. "As Mykhailo Fedorov, Vice Prime Minister of Ukraine and Minister of Digital Transformation mentioned, we were ready for it," writes Khrystianovych. "There was fast and open communication with their audience. Clients received transparent information on social media about what was going on, what these attacks were and what measures were being used to cope with them."

When the tanks finally crossed the border on February 24th, banks were ready to revert back to the contingencies they had honed during the Covid-19 pandemic, such as remote working. Regulation allowing the use of cloud services in banking was quickly implemented, allowing institutions to access services via the EU, the UK, the United States, Canada and other countries. Measures were put in place to prevent a run on the banks, such as cash withdrawal limits and a state-backed guarantee on all deposits. As the conflict continued, further measures were taken to help protect access to cash, such as extending the expiry dates on debit cards and allowing cash withdrawals at petrol stations, pharmacies and other retail outlets. "Due to the decentralisation measures that had been introduced by banks, many ATMs and branches continued their work in safer places across Ukraine which also served to reassure people," says Khrystianovych.

Read the full article

work is required by ASX and other stakeholders to enable sustained trading to continue on alternative trading venues in the event of a market outage."

Even in jurisdictions where regulators are not currently focussing on third-party risk management, firms should still be conscious of how they may be impacted by risk events within their supply chain and build this into their business continuity framework.

2 DISASTER RECOVERY PLANNING

Disaster recovery planning refers to policies, procedures and facilities - including business applications, data centres, hardware and communication infrastructure - remain operational after a disaster. A "disaster" might refer to a natural disaster or weather event, or anything else that poses a potential risk to network systems such as a system outage, error or failure, a terrorist attack, cyber incident, or indeed, a pandemic.

The global pandemic had a huge impact on the way IT systems are used and accessed by both employees and consumers across the globe. We have all come to expect a great deal more from the applications and systems we use in our jobs and everyday lives. Activities that were once simply a convenient option, such as online food shopping and internet banking, became essential services for many overnight, meaning firms had to cope with a sudden and considerable increase in online traffic.

INCREASED NETWORK CAPACITY

Many firms struggled to manage the surge in users on remote access networks in March 2020 as swathes of individuals attempted to work from home for the first time. Hopefully, the past two years have allowed IT teams to amass the required resources to recover from an event like Covid - or any other disaster which would impact the ability of the workforce to be physically present on site.

LESSONS LEARNED FROM COVID

To ensure core operations are able to function in the event of a disaster, it's important that a business impact assessment is completed to identify the following:

- which areas of the business are essential for it to operate;
- the minimum number of employees required to keep these areas operational;
- the essential systems and service providers needed by those employees to carry out their role; and
- alternate access devices and mechanisms necessary for staff to utilise the firm's IT facilities.

Firms whose operations were impacted the least by the disruption caused by Covid were those who recognised the threat early and deployed disaster recovery plans quickly. Most disaster scenarios involve the need to access essential systems remotely, so this is an area firms should have invested heavily in post-Covid.

A "disaster" might refer to a natural disaster or weather event, or anything else that poses a potential risk

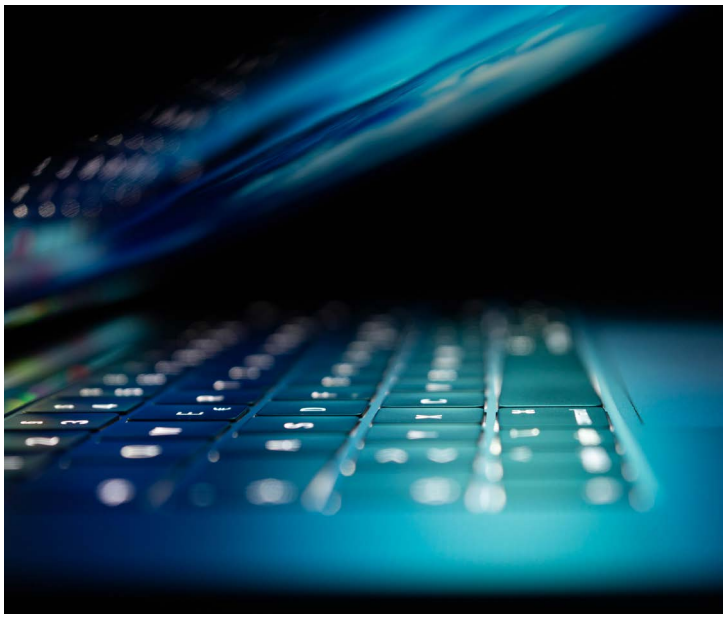
Managing the ongoing threat to cyber security is a huge component of operational resilience

THE CYBER THREAT

The cyber threat grows with every passing year, so a firm's operational resilience and disaster recovery efforts must incorporate the potential for malicious cyber attacks. In January 2022, ahead of Russia's invasion of Ukraine, the UK's National Cyber Security Centre (NCSC) published a warning to all UK organisations to bolster their cyber defences.

"In the five months since that guidance was published, we have seen significant cyber activity in Ukraine, with sustained intent from Russia to destroy or disrupt Ukrainian government and military systems," says the NCSC. "This has had effects beyond Ukraine's borders; the UK government stated Russia was behind a cyber attack on a global communications company, on the eve of the invasion, which affected wind farms and internet users in central Europe."

Managing the ongoing threat to cyber security is a huge component of operational resilience and should be an ongoing priority for firms, not a short-term effort, post-disaster. Important business service areas within financial firms are inherently linked to IT and cyber capabilities, which puts a great deal of stress onto IT departments. "Cyber security teams were already under mounting pressure in the months leading up to the invasion of Ukraine: handling a global pandemic, a rise in ransomware attacks and the Log4j vulnerability, alongside the usual levels of ongoing malign cyber activity," says the NCSC. "These extended periods of intense pressure on cyber security teams raise the risk of poor wellbeing and even burnout, with a potential associated rise in unsafe behaviours and errors." As such, the NCSC has released guidelines on maintaining a sustainable strengthened cyber security posture.



3 EVACUATION PLANNING

Evacuation procedures in a post-pandemic world must take into consideration the impact of flexible working. Many companies still make use of remote access, with some offering it as an optional job perk. A recent YouGov survey of UK finance workers revealed just 14% saw the office as their main place of work, with 44% following a hybrid model and 42% working solely from home. This presents a challenge when it comes to managing who is on the premises at any given time. The following measures should be considered to ensure all individuals are accounted for in the event of an emergency evacuation:

- Ensure all members of staff and visitors sign in/out on arrival/exit
- Enforce a centralised, mandatory booking system for those who are choosing hybrid working
- Hybrid/remote staff should be routinely briefed on evacuation procedures (not just onsite staff)
- Onsite attendance should be double-checked through a daily roll-call.

The pandemic has also presented some challenges regarding the evacuation process while maintaining recommended social distancing guidelines. Many jurisdictions have now removed the obligation to maintain a set distance from others to reduce Covid-19 transmission. However, in some cities in China such as Beijing - where a "dynamic-zero Covid" policy is currently in place - restrictions remain. Evacuation procedures must therefore take local guidelines into consideration and also the safety of vulnerable or at-risk individuals, particularly when gathering staff at an assembly point.

"Separate evacuation plans are required for every building within the firm's network," says Finlay. "This should include corporate offices as well as each individual retail branch. Distributing a company-wide evacuation plan that is not tailored to each location is not sufficient and will not address idiosyncrasies between locations."

Evacuation procedures must therefore take local guidelines into consideration and also the safety of vulnerable individuals

4 CRISIS MANAGEMENT PLANNING

Getting through a crisis relatively unscathed is heavily dependent on a well-oiled crisis management plan. A crisis can be anything from a natural disaster or terrorist attack to a PR scandal or a global pandemic. Not all crises in banking are necessarily solely financial, so firms should be prepared to call on a range of skills and resources. Every firm should have a crisis management committee in place; a group of individuals who can work together to limit the damage caused, while under the extreme pressure often created by intense public scrutiny.

WHO SHOULD SIT ON A CRISIS MANAGEMENT COMMITTEE?

The crisis management committee or crisis management team should include individuals from all departments of the company, as well as external advisors such as a PR expert, to ensure a 360-degree view of the situation. The committee might include the following people:

- Department heads
- Board of directors including the CEO
- PR/media advisors (external)
- Marketing and communications team (internal)
- Human resources
- Risk management and compliance functions

It may be that not all members of the team will be needed for every crisis, but this should be assessed on a case-by-case basis.

Mobilising the crisis committee can be challenging in a semi-remote or fully remote office environment. This fractured way of working makes it even more important to ensure all members are aware of their presence on the committee and fully understand what is required of them in the event the committee must be

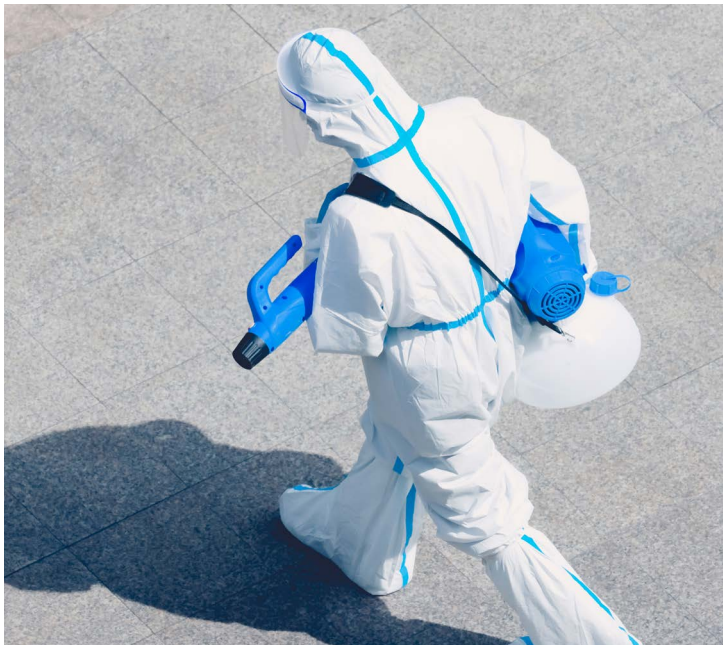
In recent years, the most common type of crisis is usually one that impacts the firm's public image

deployed. This should be regularly reviewed as part of wider operational resilience measures.

BUILDING A CRISIS MANAGEMENT PLAN

When planning for a crisis, the crisis management committee is responsible for the following areas:

- Identifying potential crises and subsequent risks to the firm
- Identifying and obtaining the required resources to respond to these potential crises
- Communicating with all internal and external stakeholders to understand their concerns and to ensure any potential vulnerabilities are identified and addressed
- Creating a comprehensive crisis management plan which can be accessed by key stakeholders and all committee members.



During the actual event of a crisis, the committee should be responsible for the following:

- Identifying the crisis
- Alerting the firm, including all members of the committee to the crisis
- Assessing the current and potential impact of the crisis on the firm
- Activating the crisis response
- Communicating the crisis to stakeholders and maintaining communication on the situation throughout
- Arranging necessary resources such as first aid, shelter, food, external expertise or any assistance required by employees (this is not exhaustive and details should be addressed within your crisis management plan)

Post-crisis responsibilities of the committee should include:

- Conducting a review to identify which areas of the response were successful and which were unsuccessful
- Using information gleaned from the review to revise the crisis management plan
- Replacing/replenishing any resources used during the event
- Communicating any changes made to the previous crisis management to relevant persons
- Rehearsing/stress testing the new crisis management plan and making any required changes before circulating to the relevant persons.

Just as a "disaster" is a vague term which could refer to a variety of events impacting a business, so too is the term "crisis." In recent years, the most common - and perhaps most damaging - type of crisis is usually one that impacts the firm's public image, i.e. an adverse event or scandal which is of interest to the wider public.

There are few (if any) financial institutions that have escaped public scrutiny for misconduct in recent years, but Wells Fargo in particular has seen a great deal of negative press of late. In 2016 it was blighted by a colossal fake accounts scandal and has since had several other high-profile crises, including a lawsuit claiming the bank discriminates against and deliberately targets black and latino borrowers when denying loan applications.

One of the key lessons learned from Wells Fargo's fake account scandal in particular is the need for firms to act quickly when issues are detected. The Senate Banking Committee, who questioned then-CEO John Stumpf, highlighted a distinct lack of action by the board, who had been aware of the situation since 2013.

CRITICISM OF THE TERM "OPERATIONAL RESILIENCE"

The terms addressed in this report inevitably are interconnected and overlap in many areas. Operational resilience is a relatively new umbrella term which appears to have seen increased usage as a reaction to recent threats to the global financial system and increased digitalisation - and as an acknowledgement of the importance of operational risk management and mitigation (led in most-part by the UK's FCA.)

A recent article by Helen Molyneux, who is director of Cambridge Risk Solutions and a business continuity professional, discusses some interesting observations about the notion of operational resilience, particularly as a distinct area of regulation and the subsequent required documentation.

Molyneux's article looks specifically at the Business Continuity Institute's Operational Resilience Report, which examines how different organisations across many sectors understand the term operational resilience: "Significant mention is made of the FCA approach to operational resilience and business continuity within the recent BCI report, with a surprising amount of deference to the FCA approach," she writes. "Having worked with a start-up challenger bank, it is obvious that the guidelines and requirements are causing duplication of effort and, possibly, the creation of yet more siloed thinking. Despite demonstrating that an effective approach to business continuity completely mapped into the operational resilience requirements, the bank simply did not have the confidence to merge the approach, and insisted on maintaining a separate set of documentation to satisfy the requirements for operational resilience, thus creating needless duplication, and increased likelihood of errors, and a lack of joined up thinking leading, possibly, to a reduction in resilience."

Achieving operational resilience, argues RiskBusiness' Mike Finlay, should really be

One of the key lessons learned from Wells Fargo's fake account scandal in particular is the need for firms to act quickly

the point at which all of the areas mentioned above are seen to be aligned and working towards the same outcomes. "Business continuity and disaster recovery have always worked hand-in-hand; but recent events have perhaps redirected our focus towards the wider impact of disruption to day-to-day operations and the importance of ensuring the firm is ready to react to operational risks, contain the damage and deploy the necessary contingencies. Operational resilience measures shouldn't be about duplicating the work of these departments; it should be about ensuring they are all aligned and aware of how their roles interact."

RESOURCES

Financial Conduct Authority and Prudential Regulation Authority joint statement on operational resilience requirements:
https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=D6335BA4712B414730C697DC8BEB353F3EE5A628

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency joint paper on operational resilience:
https://www.fdic.gov/news/press-releases/2020/pr20122.html

The Bank of England and the FCA discussion paper:
https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector

Australian Securities and Investments Commission (ASIC) report on the ASX outage:
https://download.asic.gov.au/media/scvil04f/rep708-published-24-november-2021.pdf

UK's National Cyber Security Centre (NCSC) warning to all UK organisations:
https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

NCSC guidelines on maintaining a sustainable strengthened cyber security posture:
https://www.ncsc.gov.uk/guidance/maintaining-a-sustainable-strengthened-cyber-security-posture

The Business Continuity Institute's Operational Resilience Report:
https://www.thebci.org/news/bci-operational-resilience-report-2022.html

About Risk Universe

Risk Universe by RiskBusiness provides in-depth analysis, reviews and research on areas of interest within the broader governance, risk, audit and compliance landscape, designed to provide proactive, 360° intelligence for informed decision making across the enterprise.

About RiskBusiness

RiskBusiness is an international governance, risk, audit and compliance (GRAC) solution provider, delivering risk content, risk intelligence, risk tools and risk advisory services to its clients. It is an association of like-minded industry professionals, who have the aim of furthering the risk management discipline to enable better risk-reward decision making.

Risk management is an evolving discipline, which has developed in close partnership with the industry. RiskBusiness has, both as individuals and collectively, a depth of established relationships with leading players and regulators in the operational risk field. We are also active participants in industry working groups and contribute thought leadership through publications and education.

RiskBusiness was founded in 2003 and today has principal locations in Birmingham, London, Buenos Aries, Amsterdam, Hong Kong, New York, Singapore, Toronto, and Zurich. To learn more, visit **www.riskbusiness.com**

Contacts

Carrie Cook, Editor:
carrie.cook@riskbusiness.com

General enquiries:
info@riskbusiness.com

Risk Universe
by RiskBusiness

www.riskbusiness.com