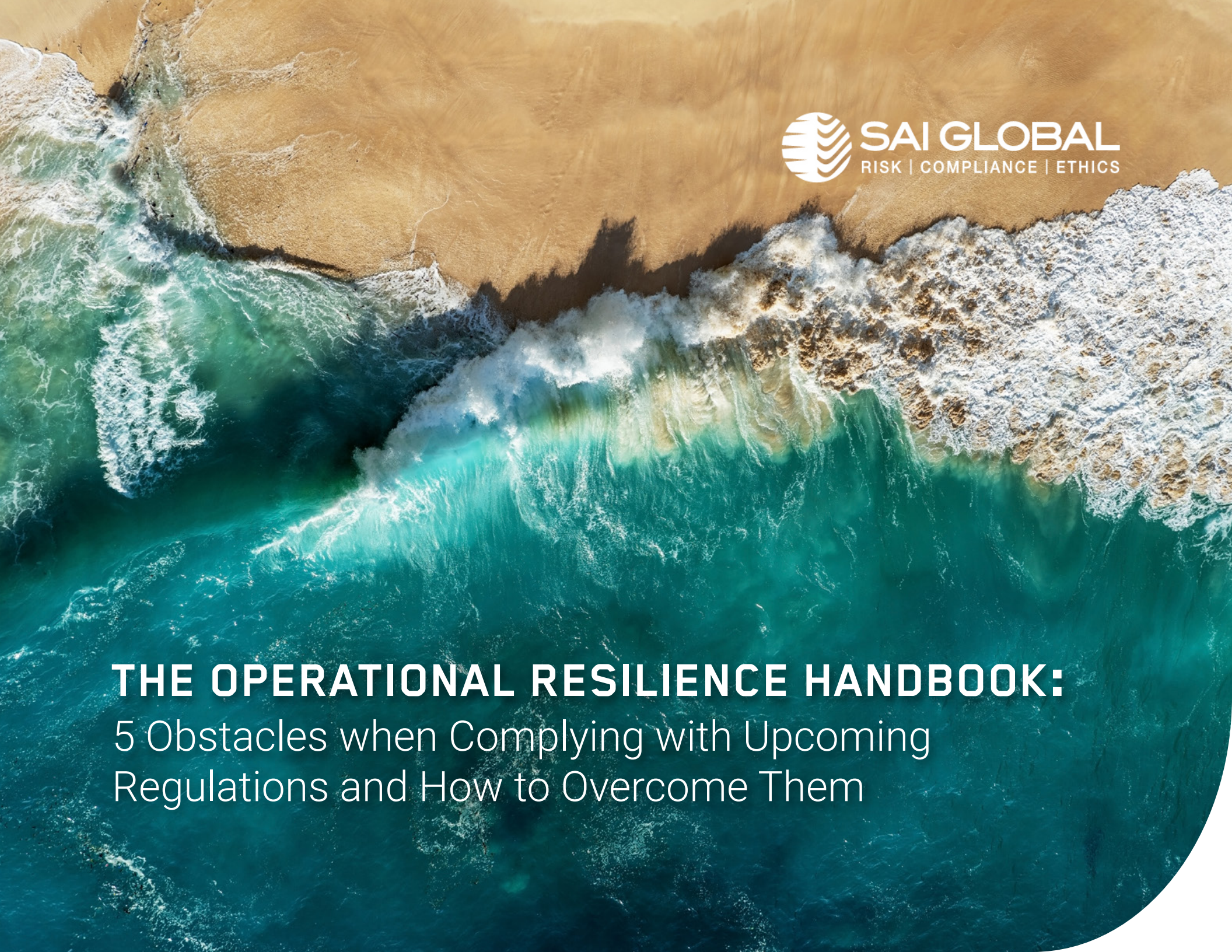



# THE OPERATIONAL RESILIENCE HANDBOOK:

## 5 Obstacles when Complying with Upcoming Regulations and How to Overcome Them

**Recent operational failures in the financial services sector are driving regulators to force firms and financial market infrastructures (FMIs) up the maturity curve of risk management. By outlining a framework that connects the dots between risk and recovery, regulators are guiding the finance sector along a path to operational resilience. However, the realities of risk management processes and infrastructure within many firms will create obstacles to adopting that framework.**

As many banks and FMIs have learned the hard way [1], the best risk management practices ultimately prove meaningless if the company can't recover from an incident that results in a business disruption. To protect consumers and strengthen the overall financial stability of the United Kingdom (UK), financial market regulators under the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) (henceforth referred to collectively as "the Authorities") are collaborating on policies that will knit operational resilience into the regulatory framework of financial firms.

The Authorities' have made it clear this is not a check the box exercise and they expect financial firms to remain within their impact tolerances even through severe disruption scenarios. Although these policies are intended for financial firms in the UK, we anticipate this regulatory focus will not end at the UK border and will expand to firms globally. Similar to how the General Data Protection Regulation (GDPR) impacts organizations worldwide, financial firms worldwide cannot afford to delay or ignore these transformative regulations and must take steps now to prepare.

Within the discussion papers Building the UK financial sector's operational resilience [2] and Building operational resilience: Impact tolerances for important business services [3] regulators define the importance of operational resilience in the following manner:

"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 – in terms of people, processes and organisational culture – to adapt and recover when things go wrong."

"Looking at the systems and processes on the basis of the business services they support may bring more transparency to and improve the quality of decision making, thereby improving resilience."

"The result of implementing the proposals should be that when a disruption occurs, firms and FMIs will have robust and reliable arrangements in place to deal with it. These arrangements will have been previously tested. Firms and FMIs will also be able to show that they are operationally resilient, both to themselves and to the supervisory authorities."

---

[1] *IT Failures in the Financial Services Sector, House of Commons, 28 Oct. 2019, publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf.*

[2] *Building the UK Financial Sector's Operational Resilience, Bank of England and the Financial Conduct Authority (FCA), July 2018, www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.*

[3] *Building Operational Resilience: Impact Tolerances for Important Business Services, Bank of England and the Financial Conduct Authority (FCA), Dec. 2019, www.fca.org.uk/publication/consultation/cp19-32.pdf.*

To improve resilience, regulators advise financial firms to do the following:

- Identify important business services (defined as services that would harm consumers, market integrity and/or financial soundness if interrupted for too long);
- Determine impact tolerances (the length of time those services can be interrupted before they impact internal and external stakeholders);
- Map the systems and processes that support these important business services; and
- Test whether the systems and processes mapped to "important business services" can recover within the stated impact tolerances.

The framework offers a roadmap to strengthening continuity practices and by extension, operational resiliency. Many companies will have their work cut out for them to adopt the framework, but the investment will be worth it as research has shown that companies with mature resilience practices have higher valuations, customer satisfaction ratings, and employee satisfaction than those that don't.

"Research has shown that companies with mature resilience practices have higher valuations, customer satisfaction ratings, and employee satisfaction than those that don't."

We recently surveyed risk and business continuity professionals from over 200 organizations about their firms' business continuity management practices. Based on the answers to our 2020 Business Continuity Benchmark Study [4] , and our ongoing work with client firms, we've identified five common issues that may interfere with building operational resilience:

---

[4] *Addressing the COVID-19 gap: How Business Continuity professionals can propel business forward, SAI Global, 30, April 2020. https://www.saiglobal.com/hub/blog/download-the-2020-business-continuity-benchmark-report*

# 1. The company's risk culture is siloed.

It is the role of business continuity to ensure the resiliency of an organization, and recent events have highlighted the importance of integrating business continuity within risk management efforts. However, most companies are not that far along the resilience maturity curve. Of the companies we surveyed in January and February of 2020, only 10% have vendor risk, cyber risk, and business continuity under one umbrella. More than a third identified integrating the three areas as a "long term goal." Even more concerning, nearly 40% responded that integration of risk and business continuity is "not realistic."

The increased regulatory focus on operational resilience of financial firms will force closer collaboration between risk and continuity practitioners. The proposed operational resilience framework requires that companies focus the risk lens on business services. Regulators are not concerned with profitability, but with whether or not in the face of a business disruption consumers can still go to the bank and pull out cash from the ATM 24/7; whether they can make payments to loved ones in a foreign country; whether they can pay their mortgages; whether their data is protected.

The scope involved in refocusing risk to consider impacts to important business services will be considerable, especially for larger firms that have thousands of business processes crossing hundreds of business units. Risk and business continuity managers won't get by with assigning scores to threats and then putting their respective risk assessments and business impact assessments (BIAs) on a shelf—they'll need to articulate and test how those threats would impact the ability of the business to deliver important services. Recovery response programs and business continuity programs (BCPs) will need to overlap in order to effectively track, test and report on the resilience of interconnected IT systems and business processes.

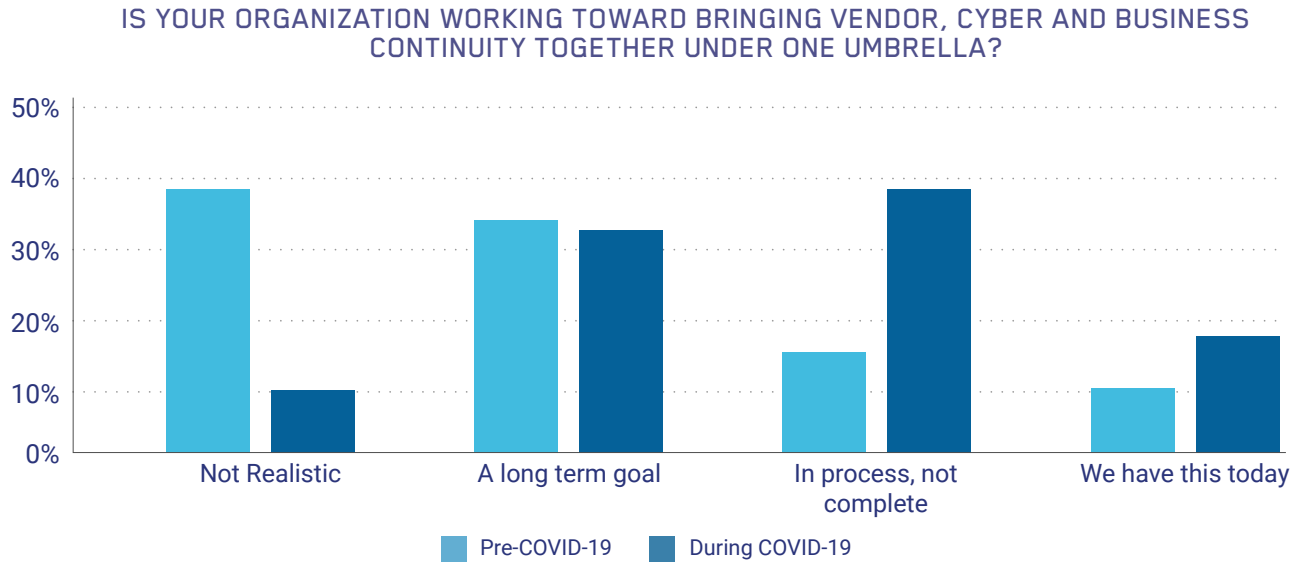
"Risk and business continuity managers won't get by with assigning scores to threats and then putting their respective risk assessments and business impact assessments (BIAs) on a shelf—they'll need to articulate and test how those threats would impact the ability of the business to deliver important services."

Companies will need the ability to understand, at any given time, what material risks are coming in and how they link back to the products and services the business is selling, the IT assets supporting the customer's journey, and the processes throughout the organization that may or may not let the customer down. They will need to be able to stress test IT assets and business processes to ensure they can support products and services in the face of a disruption.

Chief Information Security Officers (CISOs), for example, need to understand that a server impacts a specific business process. Chief Privacy Officers (CPOs) need to understand how breaches of certain third party service provider systems can interrupt services to customers. Chief Marketing Officers (CMOs) need to understand how reputational risks can severely impact business continuity in a matter of hours.

Disparate risk management point solutions are effective tools for the risk disciplines they support, but they keep plans and data in silos and therefore block information sharing that is critical to collaboration between risk and business continuity. In addition, threats are constantly evolving, and so too should disaster recovery and business continuity programs. In a siloed risk environment utilizing multiple software platforms, various parties will not be on the same page or timeline with regards to documenting and testing emerging threats and their potential impacts on the organization.

The COVID-19 pandemic forced organizations to recognize these inefficiencies and gaps and when we conducted a second survey in March 2020, the number of respondents who said bringing vendor, cyber and business continuity together under one umbrella is not realistic dropped by 35% from 39% to 10%.

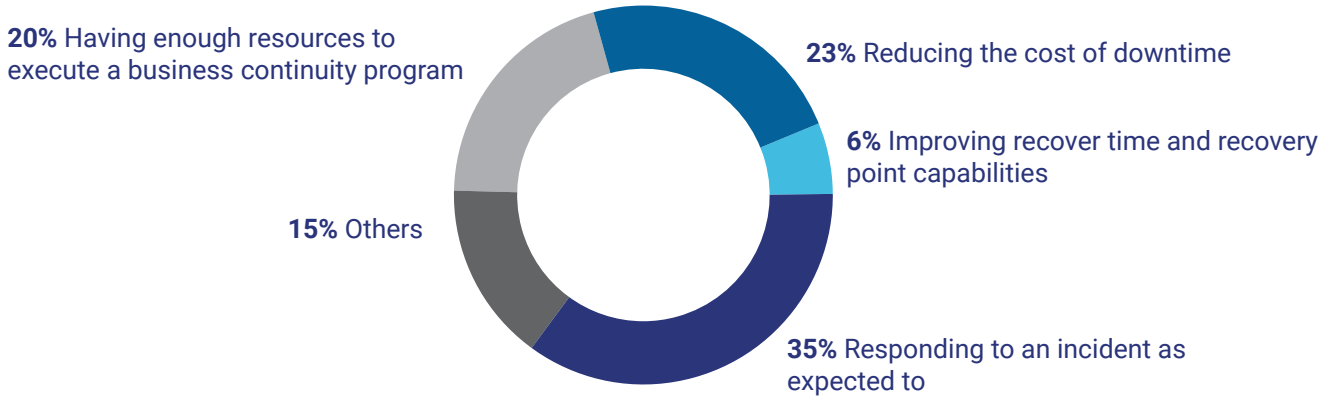



Adopting an integrated business continuity management into a larger risk management platform can connect the dots between all risk stakeholders (including third party risk, cyber risk and operational risk) as well as business continuity. A business continuity management (BCM) platform puts everyone on the same page and enables the company to center risk management efforts on the IT assets, third party vendors and critical business processes that support important business services. It can also help facilitate a culture of operational resilience throughout by providing a holistic view of the risk environment.

# 2. Continuity and recovery testing and exercising is inconsistent or incomplete.

When we asked risk and business continuity managers "What is the most important measure of success for your role?" the top response was "responding to an incident as expected to," followed by "reducing the cost of downtime" and "improving recovery time and recovery point capabilities." In other words, professional success hinges on whether or not their BCPs and disaster recovery plans work.

WHAT IS THE MOST IMPORTANT MEASURE OF SUCCESS FOR YOUR ROLE?




The cornerstone of resiliency is testing and exercising, and the risk and continuity professionals we surveyed voiced their vested interest in doing it well—yet it remains a chronic area of weakness for many firms. Some firms simply create business continuity and disaster recovery plans and put them on a shelf. The majority of firms take that approach a step further with tabletop exercises where internal company stakeholders walk through recovery playbooks and crisis management plans under a variety of scenarios. However, tabletop exercises often don't go far enough to test resiliency.

Testing, where companies deliberately interrupt IT systems or processes to test whether redundant systems can take over within the Recovery Time Objectives (RTOs) specified, are generally more effective at testing resilience of systems and processes than tabletop exercises alone. However, they are also more complex and expensive and therefore usually limited to disaster recovery testing of IT assets. Where many companies fall short is testing recovery of business processes. It won't matter if the systems come back up if there are no people online to do the work. A company that limits testing to IT assets hasn't proved resiliency, it has only proved that IT systems can come back up quickly.

It can be difficult to get executive buy-in for testing because of cost; in some cases, there is also considerable risk that if the test fails it will cause a service disruption that impacts customers. It's no surprise, therefore, that the vast majority of our clients test business processes through tabletop exercises. Companies can gauge the effectiveness of tabletop exercise protocols by the number of failures that the exercises reveal. If the company runs a tabletop exercise and failures occur, that is okay. The goal of a test is to uncover problems that will hinder operational resilience during a business disruption so you can identify and fix them before a real disruption occurs.

There are a number of common failures that are exposed through effective tabletop exercises. The risk and business continuity managers we surveyed identified "cyber breaches" and "third party vendor risk" as their number one and number two threats, respectively. When we facilitate tabletop exercises and tests with clients, they are surprised at other critical issues that tend to bubble up, including the following:

Communication failures: Stakeholders often discover they can't communicate with each other during an incident to know what is going on and to be able to give alternative instructions during the recovery process. For example, if the police gets notice of a dirty bomb, and subsequently evacuates buildings and severs all cellular communications within a 10-block radius, evacuated employees have no immediate way to communicate with each other when cell phones don't work.

Primary and backup data centers too close: We conducted a tabletop exercise with a client using the dirty bomb scenario, and participants realized that their backup data center was in the same 10 city block as their primary office, which would leave them with no way to access information systems at all. (Best practice dictates that primary and secondary data centers be at least 10 miles apart.)

No end user validation of IT systems: Often after a disaster recovery test, IT systems are brought back up and only the CIO is notified. The operational end users aren't asked to log in with their user IDs to test the system and validate that recovery of each component was complete.

As operational resilience becomes more scrutinized, regulators will expect companies to report on how testing and exercising "outcomes" demonstrate resilience. In order to demonstrate resilience within the Authorities' proposed operational resilience framework, firms will be asked to triage and test all systems and processes critical to delivering their "important business services." Companies that currently test from a scenario based, loss-of-IT-asset approach will need to expand testing to include disruption of business processes.

Companies that are utilizing a number of risk management point solutions may find they need a BCM platform that integrates business continuity management with each of the primary risk management disciplines, so they have a more holistic view of how threats impact the entire enterprise. A centralized solution facilitates the creation of effective testing packages and test scripts that relate to specific impacts, versus just scenarios.

BCM solutions can also facilitate after-action reporting on testing and exercising. When conducting tabletop and disaster recovery exercises, it's important to catch all the timing information to recover against RTOs specified by BIAs. With each step of the recovery testing, a robust BCM system will record and track every start and stop of the clock to evidence that testing was done and where the organization is with regards to recovery time capability (RTC).

Regulators understand that every company will experience a business disruption at some point. Testing reports can serve as a company's "get out of jail free" card with regulators. Examiners will be seeking outcomes, meaning they want to know what worked well and what didn't during testing and how the company responded to address any failures. If the company can demonstrate that testing was comprehensive, that results were good across multiple areas of the business, and weaknesses were identified and addressed, it may give regulators assurance that reasonable actions were taken to withstand the disruption and the company will avoid fines and sanctions.

# 3. Third party vendor risk management is ineffective.

Financial firms have become increasingly reliant on third party technologies and infrastructure (such as the Cloud, CMS systems or ATM machines) to deliver their important business services, and regulators want to ensure that companies maintain appropriate oversight of those third parties. Some organizations have tens of thousands of vendors, so the scope of third party risk can be quite significant. Regulators are also concerned that industry-wide dependencies have developed on a concentrated number of providers dominating certain services, which puts the entire financial system at risk if they fail.

Authorities made it clear in their joint consultation paper Outsourcing and third party risk management[5] that firms are responsible for ensuring that the failure of third party service providers don't interfere with the delivery of important business services, and they should monitor vendors accordingly:

"The PRA expects firms to exercise their access, audit and information rights in respect of material outsourcing arrangements in an outcomes-focused way to assess whether the service provider is providing the relevant service effectively and in compliance with the firm's legal and regulatory obligations and expectations, including as regards operational resilience."

Our survey respondents listed third party vendor risk as a top concern, yet nearly 25% of those same professionals responded that they don't have a vendor risk program at all and another 23% reported that they don't factor vendor risk into their business continuity programs. These responses are aligned with what we've observed working with clients, and we are concerned that vendor risk management is a chronically weak link in the operational resilience chain.

HOW DOES VENDOR RISK FACTOR INTO YOUR BUSINESS CONTINUITY PROGRAM?

**25%** We don't have a vendor risk program

**23%** Vendor risk is entirely separate

**6%** We share a vendor database

**26%** Vendor risk is part of our BIAs

**19%** Vendor risk and business continuity management are combined

[5] *Outsourcing and Third Party Risk Management, Bank of England, Dec. 2019, www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf?la=en&hash=4766BFA4EA8C278BFBE77CADB37C8F34308C97D5.*

## “Vendor risk management is a chronically weak link in the operational resilience chain.”

Contract management is key to third party vendor risk management, and a primary area of weakness. An alarming number of the companies we work with do not consistently have service level agreements (SLAs) with vendors that spell out acceptable impact tolerances for disruption of technologies or critical services. Even when they do have SLAs in place that specify impact tolerances, few companies cross reference to ensure that SLA tolerances are aligned to the RTOs of the business processes they support.

Authorities are also seeking collaborative business continuity planning and testing with third parties that support important business services, whether those vendors are technology service providers (TSP) or business process outsourcers (BPO). In the discussion paper mentioned above, they advise that written agreements for material outsourcing should outline “the requirements for both parties to implement and test business contingency plans, which should take account of firms’ impact tolerances for important business services. This should include a commitment on both parties to support the testing of such plans.”

We hear from companies that their vendors are often reluctant to test and exercise with them. That’s unfortunate, because one of the most reliable ways to know if key vendor recovery times align with the RTOs of the processes those vendors support is to participate in their disaster recovery or tabletop exercises. (Generally speaking, if a vendor does their own internal disaster recovery and business continuity well, they are eager to engage in joint testing.)

If joint testing exercises aren’t feasible, companies can conduct due diligence document reviews instead. Following are examples of information to request:

- Disaster recovery and business continuity plans;
- System and Organisation Control (SOC) reports;
- RTO/Recovery Point Objective (RPO) of products or services provided by the vendor; and/or
- Frequency of testing and testing outcomes with lessons learned.

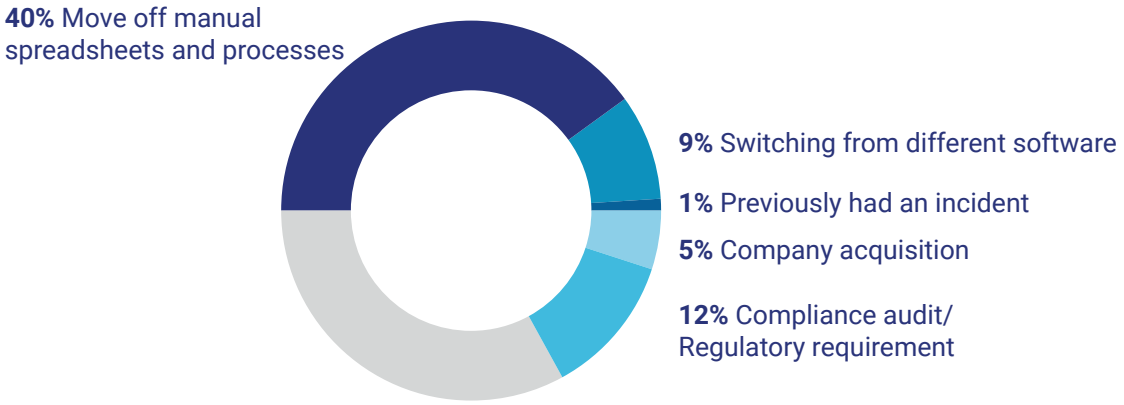
Not every vendor will be willing or able to deliver this information, so companies should expect cooperation in varying degrees. Keep in mind if a vendor refuses to share testing results, it may be a red flag they aren’t testing and exercising consistently or are hiding deficiencies.

The goal of documentation reviews is to get a sense of how vendors are testing and managing their business continuity programs, to measure those disclosures against the company’s internal BCP requirements, and then assess for gaps (such as inadequate testing or an inability to achieve RTOs). When gaps are discovered, companies should document them and if necessary, issue findings to the vendor. If the risk is moderate, third party vendor relationship managers can work with the vendor in question to develop a contingency plan to resolve those deficiencies. If the risk is high, the board may need to be informed so they can review the situation and decide whether the level of risk relative to the criticality of the vendor is acceptable.

# 4. Disparate risk management platforms provide a fractured lens of the risk environment.

Nearly 38% of the risk and continuity professionals we surveyed reported that they don't use software to manage business continuity efforts. Among those we surveyed who do use it, 40% reported that they adopted BCM software to "move off of manual spreadsheets and processes," versus trying to acquire a fulsome perspective of the risk environment. Yet "important business services" are going to be impacted by every type of risk and by business processes across the entire firm, which will require tools that tie risk to recovery and map processes to risk and control frameworks. A 360-degree view of the risk environment can help organically drive operational resilience.

IF YOU HAVE A BUSINESS CONTINUITY SOFTWARE SOLUTION TODAY, WHAT WAS THE MAIN DRIVER TO ADOPT IT?




"A 360-degree view of the risk environment can help organically drive operational resilience."

Most risk management software solutions on the market today are siloed by discipline: the platform any given bank uses to manage operational risk is likely different from the solutions they use for cyber security risk management and third party risk management and GDPR. While many of these risk management solutions are excellent tools for the functions they serve, what they can't deliver is an integrated environment for managing risk and business continuity.

Chief Risk Officers (CROs) routinely ask us "How do we actually make decisions and take action from what we are seeing?" They want risk tied to recovery so they can identify upward scaling risk that is resulting from the confluence of several low-level factors impacting tolerance. They want reporting dashboards that help them visualize gaps so they can make informed decisions and understand business impacts. They want real time data so they can identify emerging material risks and immediately pick up the phone to relevant risk managers and direct them to workflow those risks back down into the organization. They want audit trails that demonstrate to executives how a risk was identified in London and by the time New York came online the risk was already de-escalated and closed out.

Regulatory examiners want push button audit trails too, that provide history logs and evidence of where the company is in the risk mitigation process across all areas of the business. If a company can't easily identify the point(s) of failure that caused a business disruption, the regulator is going to leave a letter on the desk. Tools such as email, PowerPoint, and Excel pivot tables are notorious for manual processes, formulaic errors, version discrepancies, and disconnected or redundant data sets—all of which lead to bad MI or BI and a lengthy timescale to prove. When a company must search various risk platforms or Excel spreadsheets or emails to find evidence for an examiner, they've lost the regulator's interest and the benefit of the doubt.

Examiners also want to see that a company's risk and continuity management programs are advancing in maturity year-over-year; it's reasonable to assume they'll want operational resilience to mature as well. Regardless of where a company sits on the maturity curves of risk management and operational resilience, if they can demonstrate that they have a holistic view of their risk landscape, that they are working through a plan to address gaps and are progressing in a timely way, that often satisfies the examiner. It's difficult to demonstrate overall maturity through disparate disconnected risk management platforms or Excel spreadsheets.

# 5. Underestimating the resilience maturity curve.

We meet with companies every day that are choosing to bide their time until operational resilience is formally legislated. It's become a game of chance: "We'll see how long we can get by without spending for upgraded software" or "How big are the teeth really going to be when the regulator does turn up?" or "I bet we won't be the first ones to be sanctioned for this." Our survey results bear this out: 50% of survey respondents reported that business continuity spending will not change in 2020, and 72% reported that their BCP team size will stay the same.

HOW WILL YOUR ORGANIZATIONAL SPEND ON BUSINESS CONTINUITY CHANGE IN 2020?

**7%** It will increase significantly

**35%** It will increase slightly

**50%** It won't change

**7%** It will decrease slightly

**1%** It will decrease significantly

We've acquired several clients in the past who came to us in a rush to purchase and implement an integrated governance, risk and compliance (GRC) software solution, because they'd come under fire from regulators due to a serious breach of risk management. Signing a deal for software can be a check-the-box to get regulators off a company's back for a couple of months, because the investment shows a commitment to improvement. But ultimately, the software is only as effective as the processes and programs it supports.

A key factor in the success of implementing software is establishing realistic expectations. The road to operational resilience is a journey that cannot be completed overnight. To reach maturity in risk management with a full GRC platform can take 3.5 - 4 years. It's not realistic to have that complete by the end of your onboarding. Instead set the goal of adopting and piloting an integrated GRC platform for your first 6 to 12 months. Once the software is in place and end users are trained, the system needs to operate for three or four fiscal quarters before it can deliver the kind of actionable data that risk managers can use to identify true vulnerabilities and evidence where the company has mitigated risk. By allowing your organization to set the solution and provide feedback, you can identify functionalities to add and to make to other APIs (such as currency exchanges). Rushing an implementation to meet a regulatory deadline, put the risk management culture of your company at risk. Instead, allow time to learn the software and how it forces best practices, facilitates better communication between stakeholders, and provides high-quality actionable data.

The operational resilience framework outlined by the authorities is widening the aperture of risk management to include the processes and systems that support important business services. That framework will require a whole new way of identifying and triaging risks as well as a risk culture that links business continuity oversight with risk management.

There's no downside to investing in operational resilience, and a BCM solution is a good starting point to begin the process of integrating business continuity with risk management. The most efficient way to test BCM software is to keep the scope small in the beginning by piloting the solution in one area of risk management. For example, if a regulator has advised "tighter control of third party service providers" then begin utilizing BCM software for third party risk management. Piloting the solution is key to gaining internal stakeholder buy-in. A strong pilot will demonstrate usability, drive configurations that fit company culture, and obtain quick wins for the organization (by demonstrating improved third party vendor oversight for example).

"It's never too early to invest in strengthening risk management and business continuity programs."

It's never too early to invest in strengthening risk management and business continuity programs. Don't wait for operational resilience proposals to be legislated into policies before you act. Operational resilience is not an end state, it is a fluid on-going process that can take years to build.

# Achieve Operational Resilience with Risk & Continuity


SAI360 Business Continuity Management enables organizations to quickly deploy a scalable solution with built-in best practices and analytics that evaluate operations and identify gaps to ensure resilience and provide the confidence that your organization can recover quickly and efficiently through any business disruption.

SAI360 Business Continuity Management is the cornerstone of a risk management platform. The intuitive solution is built on a best practices framework with automated processes for business impact assessments, crisis management and disaster recovery plans, along with analytics dashboards that can be up and running in days.

**Request your custom demo today, so we can build resilience together.**


## ABOUT SAI GLOBAL

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our **SAI360 platform** in action, **request a free demo**.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific. For more information visit **www.saiglobal.com/risk.**