Galvanize

What is operational resilience?

Table of contents

More than just business continuity ...

During World War II, the British government coined the slogan "Keep calm and carry on" to encourage persistence in the face of challenge.

The sentiment behind that saying is just as relevant in modern business, although we can boil it down to operational resilience.

Operational resilience is an organization's ability to withstand and recover from sudden disruption. Once, that idea was synonymous with business continuity or disaster recovery. But thanks to business digitalization, operational resilience has evolved into something deeper: a blend of business continuity, vendor risk management, cybersecurity, and more.

This eBook explores how risk assurance professionals can approach operational resilience. What do boards and regulators want to know about it? Which part of the enterprise "owns" operational resilience? What's the actual oversight and testing needed to quantify it?

As businesses move further into a landscape of increased risk, digital operations, interdependence, and oversight, understanding the answers to those questions will become more important.

What is operational resilience?

One useful description of operational resilience comes from the Bank of England.[1]

It published a paper in 2019 that framed operational resilience as the ability to keep providing "important business services." The paper states that firms must "consider the chain of activities which make up a business service, from taking on an obligation to delivery of the service, and determine which part of the chain is critical to delivery."

In other words, operational resilience is an organization's ability to keep providing services to customers, despite a sudden disruption. To achieve this, the organization needs a clear sense of what its mission-critical services are, and the circumstances where it might fail to deliver. Then the organization can develop and implement mitigation plans to reduce the risk of delivery failure.

In the past, those mitigation plans would include steps like setting aside inventory reserves or raw materials, building redundant data centers, maintaining enough cash to meet liquidity needs, or cross-training personnel on key tasks.

Those are all still important steps to ensure operational resilience. But thanks to advances in technology and the digital transformation of business processes, how you manage your own business as you deliver services has changed dramatically—and so has the scope of what operational resilience actually involves.

RELIANCE ON THIRD PARTIES INCREASES RISK

Today, organizations rely far more on third parties to execute their mission-critical functions: payroll, email, data storage, invoicing, data analytics, email marketing, cybersecurity, customer relationship management, and many more duties can now be—and frequently are—outsourced.

So, you can boost liquidity reserves if recession is looming; buy raw materials before a shortage; or cross-train key personnel before a pandemic. But:

+ How do you "boost" an outsourced payroll function?
+ How do you train key personnel to keep working when your data storage vendor is disabled?
+ Why pay for a backup cloud communication service, if saving money was the goal of using your primary cloud service?

[1] **Bank of England,** *2019, Building operational resilience: Impact tolerances for important business services*

The digital transformation of business processes has expanded the risks around operational resilience. If the execution of your own business processes depends on using technology or services provided by others, then a huge part of operational resilience becomes cybersecurity and vendor risk management.

This is the operational resilience challenge that organizations face today: a blurry mess of cybersecurity, vendor management, and business continuity risk. Any failure in that "chain of activities" could cause enormous disruption and impact business objectives, as evidenced in the below case study.

CASE STUDY

Virtual Care Provider

Virtual Care Provider Inc. (VCPI) is an IT services firm that provides data storage, email services, billing, and other back-office functions to more than 110 nursing homes across the US.

VCPI was struck by ransomware in 2019. The hackers demanded $14 million, which VCPI didn't have. As a result, VCPI was paralyzed for weeks—and so were its nursing home customers. Some couldn't access patient records; others couldn't use email systems; still more couldn't process their billing for government reimbursement. More troubling, this also risked lives, with electronic health record and critical medication administration data also frozen/unable to be accessed.

An investigation into the attack revealed that the hackers had also taken advantage of malware that had infiltrated VCPI back in 2018. Obviously, a solid operational resilience plan, incorporating cybersecurity strategy and tactics, would have helped with this crisis.

What regulators are saying

Not surprisingly, banking regulators were the first to treat operational resilience as a significant concern.

After the crippling events of the 2008 global financial crisis, banking regulators don't simply want financial firms to have the liquidity to cover surprise losses—they want them to keep working no matter what, so the financial system remains stable.

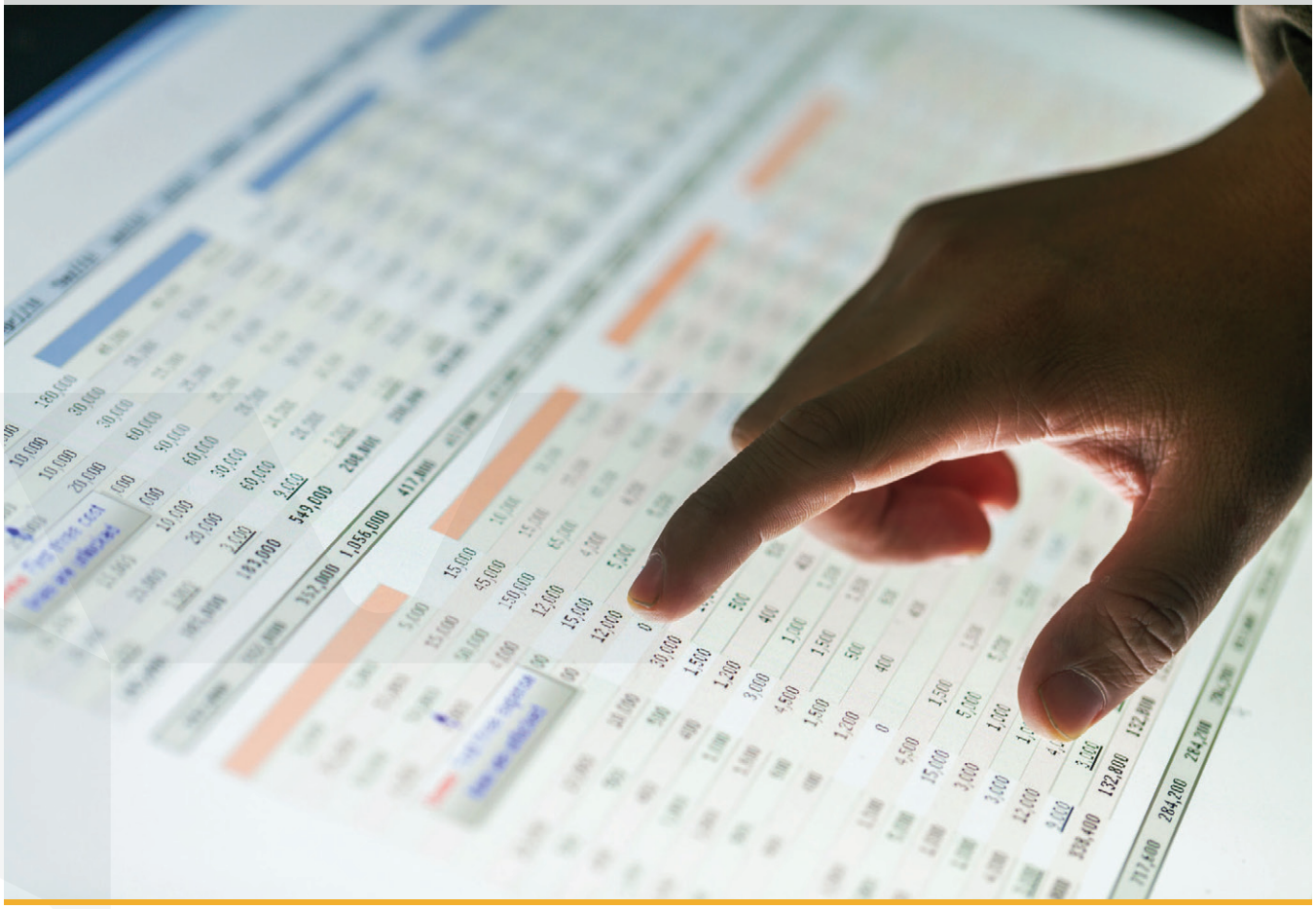
Financial firms are subject to more cybersecurity threats than other companies,[2] and they rely on a host of tech vendors and other business partners to keep operations going. So almost inevitably, as banking regulators have paid more attention to operational resilience, that concept has veered into questions about cybersecurity and vendor risk management.

For example, the Financial Stability Board first cited banks' reliance on tech vendors as a potential operational risk in 2017.[3] US banking regulators want to expand their regulatory reviews to include examinations of banks' technology partners directly.[4]

The Bank of England is revising its regulatory framework to make banks' operational resilience the foundation of financial system stability. The Basel Committee on Banking Supervision has a working group on operational resilience that is expected to publish a paper soon proposing new metrics for operational resilience.[5]

The Monetary Authority of Singapore (MAS) is a good example of how regulators are approaching the issue. In 2019 it released two discussion papers that proposed reforms to the agency's Technology Risk Management Guidelines and its Business Continuity Management Guidelines.[6] Taken together, those reforms are aimed at improving financial firms' operational resilience; MAS even says so in its call for comment. (The telling point is that MAS split operational resilience into its component parts of technology risk and business continuity.)

[2] **Markets Insider,** *2019, Cyber attacks are 300 times as likely to hit financial firms than other companies*
[3] **Financial Stability Board,** *2019, Third-party dependencies in cloud services*
[4] **The Wall Street Journal,** *2019, Federal Reserve steps up scrutiny of tech firms that serve banks*
[5] **BIS,** *2020, Basel committee meets to review vulnerabilities and emerging risks, advance supervisory initiatives and promote Basel III implementation*
[6] **Monetary Authority of Singapore,** *2019, MAS consults on proposed enhancements to technology risk and business continuity management guidelines*



WHAT ALL THIS REGULATORY ACTIVITY MEANS FOR OPERATIONAL RESILIENCE

Although the banking sector has been heavily focused on operational resilience, regulators of other industries will turn their attention to the issue eventually.

In fact, contractors for the US military must already meet the standards of NIST 800-171, a framework that governs cybersecurity among contractors' third parties. And the Department of Homeland Security leans heavily on critical infrastructure industries (banking, telecommunications, and utilities) to improve their resilience, as well.[7]

Consider the nursing home example from earlier. Nursing homes are already very regulated and they represent an important audience to public officials: the elderly relatives of taxpayers who expect reliable, effective care. As more and more industries become vulnerable to sudden disruptions that leave consumers angry (or even in physical danger), regulators will start asking about threats to operational resilience.

Ultimately, operational resilience won't remain a matter of regulatory compliance. It started that way in the banking sector, as so many risk management issues do. But as organizations integrate their operations more closely with those of vendors and customers, eventually the ability to withstand disruptions will be a crucial strategic driver, no matter what the regulators say.

[7] **Department of Homeland Security,** *2019, A guide to critical infrastructure security and resilience*

Assessing operational resilience

Assessing operational resilience involves many concepts audit teams already know, applied in new ways.

Some of the most important include:

- **Criticality.** This defines the organization's most important business services. For example, the sudden failure of an outsourced payroll function won't disable your ability to keep operating; but failure of email, data storage, or transportation systems might.
- **Mapping.** An audit team can map and identify all the connections the organization has with its vendors and customers—physical, legal, and technological—to understand how delivery of business services might go wrong.
- **Impact tolerance.** This is the maximum disruption the organization can withstand (including the longest duration of disruption) while still delivering important business operations.
- **Testing.** Audit teams must see how well an organization can stay within its impact tolerance—how well the organization can continue to operate even during a disruption. It includes testing how disruption might affect the organization's customers or other market participants.
- **Monitoring.** Critical business systems and assets must be monitored. (In the new world of cloud-based vendors providing systems for your own mission-critical business processes, this can include monitoring vendors' performance and cybersecurity.)
- **Reporting.** When a disruption does happen, senior executives need to understand the nature of the threat and respond quickly to keep operations running.

None of those steps should feel unfamiliar, even if some of them take traditional auditing concepts to new levels of sophistication.

For example, impact tolerance is similar to risk tolerance, but not identical. Risk tolerance asks the question, "How much residual risk are we willing to accept that an adverse event might happen?" and typically either the board or the C-suite decide that. Impact tolerance asks, "How much disruption can we handle once the adverse event has happened?" and customers, regulators, or business partners might have at least some say in the answer.

Testing is another example. An airline might test business continuity processes to see how quickly it can revive an inoperative ticket processing system. A test of operational resilience, however, would try to measure whether so many customers miss flights at the airline's major hub that the airline needs a fail-over secondary system.

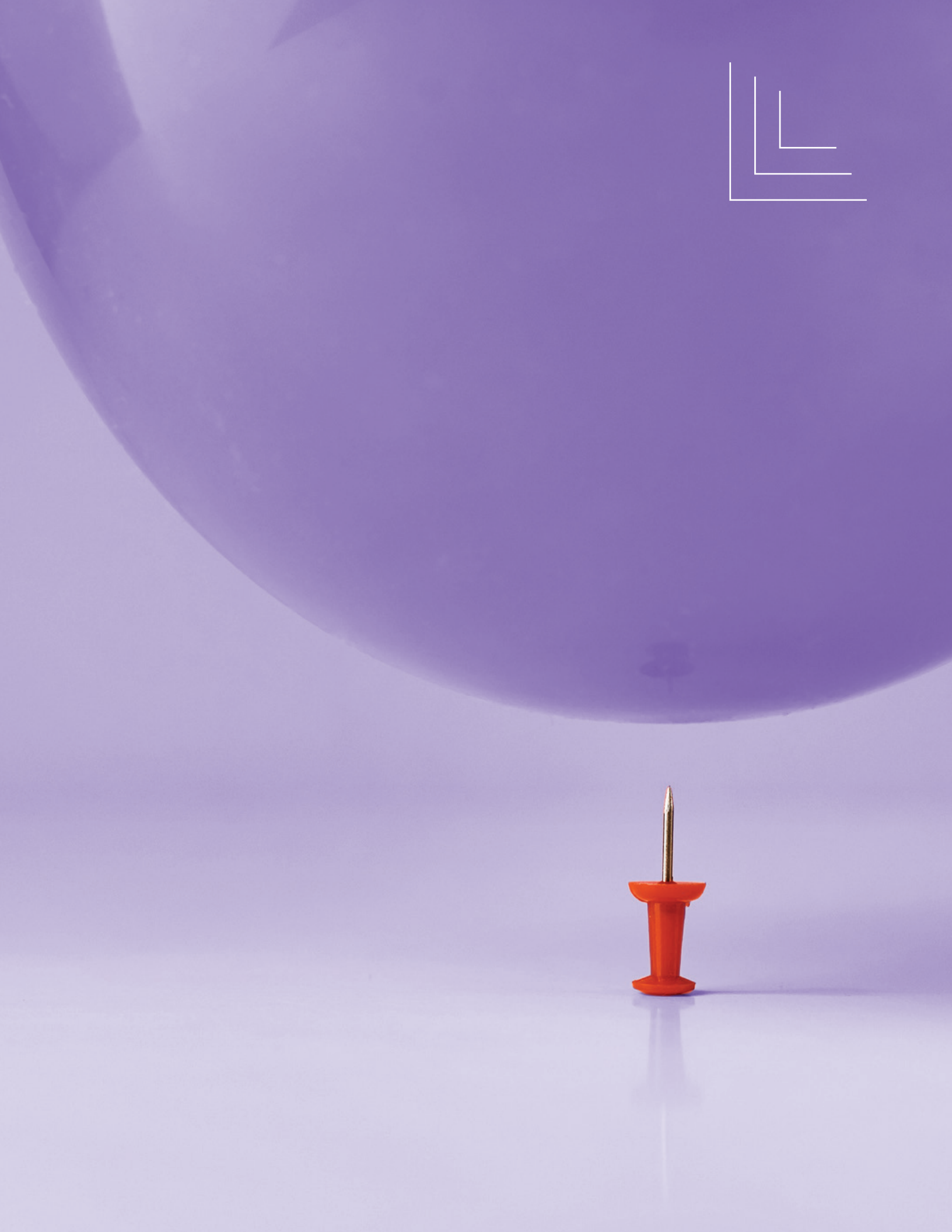
All this nuance calls out a key point. Operational risk management only seeks to keep threats to operations at some acceptably low level of risk. Operational resilience tries to assess and document how well the organization will continue to operate should an adverse risk happen anyway.

That's the difference between these two related, but still distinct, concepts. To put all of this into practice, audit teams will need to rely on technology. There are simply too many moving pieces to manage the work manually.

Mapping all the connection paths between your vendors and customers requires coordination among multiple departments. Testing impact tolerances and documenting the results requires the same. Above all, developing operational resilience is an inter-disciplinary challenge, involving communication among many locations and business functions.

Dedicated technology is essential in achieving these objectives. It provides a single source of information, and a unified understanding of risks and mitigation tactics.

Operational resilience tries to assess and document how well the organization will continue to operate should an adverse risk happen anyway.



Who owns operational resilience?

One of the most difficult questions to answer might be how to govern operational resilience, and what role various risk assurance and management functions play.

Is this internal audit's responsibility? No, although operational resilience doesn't work well without audit's participation.

Is it the compliance department's responsibility? Not really. (Although for financial firms and other highly regulated businesses, compliance plays an important role if there are regulatory obligations to attest to resilience.)

Is this something for operating executives in the first line of defense? Somewhat yes, but one can't reasonably expect most first line of defense executives to monitor all threats to resilience or know what an acceptable impact tolerance is.

Many argue that no single function will own operational resilience, instead proposing that oversight will need to be assigned among several senior executives. They would work collectively to understand the organization's resilience against various threats, and to assure that its resilience rises to whatever standards are dictated by the board, regulators, customers, business partners, or other stakeholders.

Another view is that a chief risk officer would take responsibility for operational resilience, including any regulatory compliance obligations around liquidity risk, data availability, vendor cybersecurity, and other third-party risk management issues. That's a very "financial services" way to view operational resilience, where many firms already have chief risk officers or heads of operational risk management. (It may not be easily applied to other sectors.)

What is clear is that:

+ The board will need to assure that operational resilience gets the attention it deserves, with accountability assigned to executives in a way that makes sense for the organization.
+ Internal audit will play a crucial supporting role as it assesses operational resilience, recommends changes to policy, processes, or controls as necessary, and documents progress on those remediation steps.
+ Technology to coordinate all the assessments, testing, monitoring, documenting, and reporting will be crucial. Effective use of technology to measure operational resilience is the key to improving it.

WHAT BECOMES IMPORTANT FOR AUDIT

As audit and risk management teams help their organizations to understand and develop operational resilience, the tools and techniques you use will need to be ready to meet this new type of challenge.

Collaboration. As audit teams map the organization's important business services to the key people, third parties, and IT systems that make those services possible, they'll need to communicate with a wide range of people across the organization. The same is true for subsequent tasks like defining impact tolerance, testing disruption scenarios, and implementing remediation. Collaborative tools to keep those conversations moving and to document decisions or data will be crucial.

Vendor risk assessments. An enormous part of operational resilience will be understanding the risks your vendors pose by conducting thorough vendor risk assessments. For example, audit teams might want to develop risk assessment questionnaires based on trusted risk management frameworks, and then work with operating units to assure that assessments are completed quickly and efficiently.

Testing. Testing the effects of disruption on your own business and others is more complex than the usual testing of business processes. Audit teams might need to develop new types of testing and will need to document results carefully so they can be reported to regulators or others who want to see how the organization is assuring its resilience. (This is where a single repository of data becomes essential.)

Monitoring. Monitoring will also be more complex. Operational resilience might involve multiple types of monitoring at the same time: everything from cybersecurity vulnerability scans against your Tier 1 vendors, to external feeds of data about availability of key raw materials, to changing liquidity requirements from regulators amid a financial crisis. All of that information will need to feed into the organization's key operational risk metrics.

Issue management. As organizations start to tackle operational resilience, they're likely to find a large number of weaknesses, unanswered questions, or other items that need attention. So that time-honored audit duty of developing an action plan and monitoring progress (including notification alerts for when input is due, and escalation procedures if business units don't respond within defined time frames) will be just as important as ever—even if the nature of the weaknesses and remediation steps is something the organization hasn't addressed before.

Conclusion

Recall that phrase from the introduction, that organizations must understand the "chain of activities" that allows them to do business.

That's always been so, but digital technology has allowed organizations to chain themselves together more tightly than ever before—to vendors, customers, and other participants in whatever market they occupy.

Those tight bonds can bring enormous efficiency, but also great risk. Operational resilience tries to assure that when disruption does happen, the chains don't leave everyone paralyzed.

Audit and risk management teams will be fundamental to helping their organizations achieve the ability to keep calm and carry on. Nothing is new—risk assessments, testing, documentation, remediation—but the execution of these steps will be more sophisticated. Audit leaders will need effective technology that lets them participate fully in making the organization more resilient against whatever disruptions are lurking around the next corner.

Audit and risk management teams will be fundamental to helping their organizations achieve the ability to keep calm and carry on.

For an assessment of how your organization can integrate Galvanize technology to achieve your business continuity goals and ensure operational resilience, call 1-888-669-4225, email info@wegalvanize.com, or visit wegalvanize.com

Galvanize

ABOUT THE AUTHOR

Matt Kelly

CEO, Radical Compliance

Matt Kelly is an independent compliance industry analyst and consultant who studies and writes about corporate compliance, governance, and risk management issues.

He maintains a blog, RadicalCompliance.com, where he shares his thoughts on business issues, and regularly speaks on compliance, governance, and risk topics.

In 2018 he won a Reader's Choice award from JD Supra as one of the Top 10 authors on corporate compliance. Before starting Radical Compliance, Matt was editor of Compliance Week, from 2006-2015.

ABOUT GALVANIZE

Galvanize delivers enterprise governance SaaS solutions that help governments and the world's largest companies quantify risk, stamp out fraud, and optimize performance.

Our integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—are used at all levels of the enterprise to help maximize growth opportunities by identifying and mitigating risk, protecting profits, and accelerating performance.

wegalvanize.com