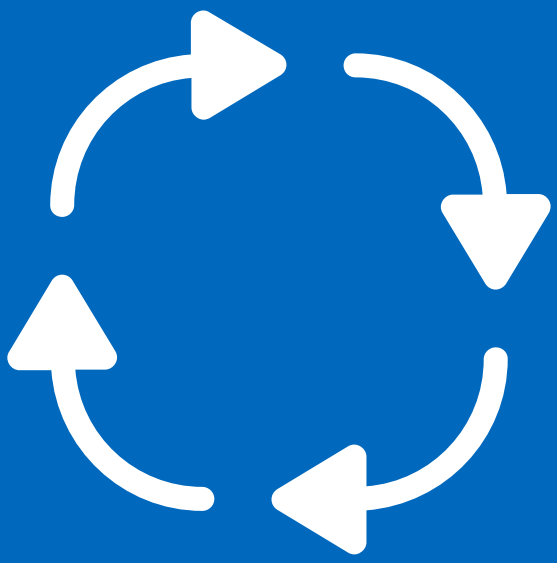
noggin | Business Continuity

Operational Resilience Versus Business Continuity: What's the difference?



No, operational resilience isn't business continuity "done well."

Resilience has become a mantra across the business world. And operational resilience, in particular, has emerged as a key corporate objective in the post-COVID era. Despite its rapid uptick in popularity, though, operational resilience isn't well understood, at least according to relevant survey data.

BCI's Operational Resilience Report 2022[i], for one, concluded that many of so-called operational resilience programs were, in fact, following the ISO 22316 organizational resilience standard rather than operational resilience best practices.

That's not all. Some organizations were confusing operational resilience with business continuity "done well".

So, why does it matter?

For starters, the fields of operational resilience and business continuity, despite their clear overlaps, are distinct. Practitioners would do well to acknowledge the very real differences, rather than risk undermining the viability of their resilience aims.

What, then, are the key differences? This subsequent guide lays them out, before making the case for a digital, integrated resilience workspace to address resilience needs.

Defining operational resilience

So, what's operational resilience, anyway?

Central bank and key financial services regulator, the Bank of England (BoE) defines operational resilience as the ability of firms, and the financial sector as a whole, to absorb and adapt to shocks and disruptions, rather than contribute to them[ii].

Albeit a sectoral definition, this characterization of what operational resilience is extends the purview of the field beyond that of business continuity and disaster recovery.

This latter point is taken up in the Gartner definition of operational resilience.

Gartner defines operational resilience as initiatives that expand business continuity management programs to focus on the impacts, connected risk appetite, and tolerance levels for disruption of product or service delivery to internal and external stakeholders, e.g., employees, customers, citizens, and partners.

The resilience-related initiatives in question coordinate the management of risk assessments, risk monitoring, and execution of controls that impact workforce, processes, facilities, technology, and third parties across the following risk domains used in the business delivery and value realization process:


Security (cyber and physical)


Safety


Privacy


Continuity of operations


Reliability

Understanding the importance of operational resilience

The definitions above begin to clue us in on the importance of operational resilience as a business practice. That being said, it's still important to spell out why exactly operational resilience is important.

Why is it?

Organizations have more dependencies on service delivery than ever before. The risk of disruption has only intensified in recent years, given the widespread adoption of digital solutions and the increasing use of outsourced service providers.

Organizations, after all, have continued to develop business services to meet growing customer expectations. And it's this need to adapt to (and accelerate) the pace of change that increases the risk of disruption, particularly to IT-related capabilities. These are the capabilities most susceptible to sophisticated cyber and ransomware attacks.

Add to the mix, organizations, due to the pandemic, have been trying to manage a significantly different operating environment. That's fundamentally changed the way businesses interact with technology, customers, and their own employees.

Climate change, for its part, is also set to test infrastructural resilience to physical risks while disrupting operations through changes in market sentiment and economic models.

These factors make operational resilience more important than ever; for, not only do organizations have to prevent disruption, but they must also adapt to change.

Regulatory environment shifts increase the salience of operational resilience.

Another major factor in the rising importance of operational resilience is the uptick in operational resilience-related regulations. Again, the BoE stands out as one of the first major regulators to mandate operational resilience standards.

What's more, the regulatory path paved by the BoE has been taken up by other national and supranational regulators, as well.

Which ones?

The Australian Prudential Regulation Authority (APRA) released draft Prudential Standard CPS 230, focusing on operational risk management. The U.S. Federal Reserve released a joint regulatory paper on Sound Practices to Strengthen Operational Resilience. And in the EU, the Digital Operational Resilience Act (DORA) seeks to align the approach to managing ICT and cyber risk in the financial sector across all EU member states.

What do the policies, regulations, and proposals consist of? Well, they, by in large, seek to uplevel the operational resilience of individual firms, so that no firm can pose a systemic risk to the wider business sector. The operational resilience principles they propound tend either to be copied from or mirror those issued by the Basel Committee on Banking Supervision, principles which are clustered across the following seven categories:


Governance


Operational risk management


Business continuity planning and testing


Mapping of interdependencies of critical operations


Third-party dependency


Incident management


Resilient ICT

What does it all mean? For many, these new rules and proposals don't (and won't) replace existing requirements – particularly the traditional requirement to maintain an up-to-date business continuity plan.

Rather, this new compliance environment represents a shift in how regulators and policymakers think organizations should be addressing the threat of disruption.

That means organizations should now assume that disruption will happen and prepare to recover.

This is a clear change in focus away from protecting individual organizations and their reputation to preventing incidents from impacting consumers and wider markets.

What about business continuity?

How does this contrast with business continuity, though?

Even with the rise in importance of operational resilience, business continuity practitioners will remain responsible for the management of prioritized activities, i.e., those activities that make critical products and services happen. These activities are discovered during the Business Impact Analysis (BIA) process.

Indeed, business continuity focuses on getting processes back up and running in an agreed timescale, with the Recovery Time Objective (RTO) focusing on the time it takes to get a process back up and running following a disruption.

Where this differs from operational resilience is that the latter field is concerned with the management of critical products and services. These are defined as products or services provided by an organization, or another organization on behalf of the organization to one or more clients, which if disrupted cause intolerable harm to the customers or pose risk to the soundness, stability, or resilience of the organization or the market in which it operates.

As a result, operational resilience measures should focus on getting a process up and running before that process causes intolerable harm to the business, its customers, or the market. An impact tolerance goes a step further with a service-based objective focus on preventing harm to customers and risk to the market in which they operate.

Getting your operational resilience program off the ground

As intuitive as these definitions are, survey data still suggest that organizations aren't getting operational resilience programs right. Specifically, many have experienced challenges in introducing operational resilience into their organizations, with lack of knowledge being the reason most often cited.

What's going on?

Well, nearly half of the organizations BCI surveyed said a lack of headcount and staff time was a "critical" or "major" challenge to implementing operational resilience programs. And with operational resilience itself still a relatively new concept, even experts contend that a comprehensive knowledge base will only come out once regulators have learned themselves what best practice is.

Nevertheless, the resilience threat still grows. Organizations, even those not currently facing compliance pressure, must act expeditiously to achieve and maintain operational resilience.

What should they do?

Here are the established steps to achieving operational resilience:

1 Identify critical products and services.

Before you can start prioritizing actions to improve operational resilience, you must define the most important services your organization delivers to its customers. Regulators use a variety of terms to refer to this concept, including important business services, critical operations or functions, and products and services.

Whatever the exact terminology, though, the meaning is clear: organizations must define their strategic, top-level services that are significant enough that disruption could cause excessive harm to customers and markets – or may even lead to an organization's failure.

2 Set impact tolerances.

Impact tolerances are the point in time (or decreased capacity of) when disruptions to an important business service cause unacceptable harm to a customer, the broader market, or irrecoverably threatens an organization's viability.

At their core, impact tolerances represent "lines in the sand" that organizations do not want to cross, because the consequences could be catastrophic to customers, markets, or the organization itself.

3 Conduct end-to-end mapping and identify interconnections.

End-to-end mapping is the process by which an organization identifies the people, technologies, information, facilities, third parties, and processes required to deliver an important business service and uses that information to determine where risks and single points of failure exist.

Why does it matter? Once an organization understands its most important business services and identifies appropriate impact tolerances, it can then map them from beginning to end.

Regulatory requirements work similarly by stating what resources need to be considered. These include identifying the people, technologies, processes, data, facilities, third parties, interconnections, and dependencies between all resource types.

The goal of mapping your services is to gain a better understanding of and clearer visibility into all the resources required for service delivery and, ultimately, to be able to identify where they may be single points of failure, limited redundancies, or concentration risk.

4 Perform scenario testing of plausible scenarios.

Plausible scenarios are realistic events that could disrupt the delivery of a business service's outcomes leading to unacceptable impact. Plausible scenarios should be severe; they should prevent an organization from being able to recover within service-specific impact tolerances.

Developing severe, yet plausible scenarios is a core element of operational resilience thinking. Scenarios are used to develop testing plans and provide concrete examples of situations that could cause an organization to exceed its impact tolerances.

Using plausible scenarios to develop testing plans helps organizations understand the most appropriate type and frequency of scenario testing and allow for more robust and tailored planning.

5 Integrate Third-Party Risk Management (TPRM) into resilience initiatives.

Third-Party Risk Management is a form of risk management that focuses on identifying and reducing risks relating to the use of third parties. Organizations must understand the role third parties play in the delivery of their important business services.

Why does it matter? The growth of dependencies on third-party providers, the potential for concentration risk, as well as intra-organization dependencies, have also created a need for organizations to consider TPRM as part of any resilience program.

Risk management is important, here, because failure to assess third-party risk exposes an organization to supply-chain attacks, data breaches, and reputational damage.

Resilience and operational risk standards and regulations all acknowledge the need to identify critical third parties but vary in the level of scrutiny of controls and mitigations mandated. Organizations must capture the contributions of third parties as part of the delivery of a critical product or service and should also understand the level of risk that a third party introduces if resilience and continuity arrangements are inadequate.

Implementing best practices with a digital resilience workspace

These best practices, however, won't implement themselves without intervention. And with time being such a critical factor, organizations must look to digital platforms that will help them get their operational resilience programs off the ground expeditiously.

What should a digital resilience platform do? The platform should enable users to:


Identify critical products and services


Define and set impact tolerances


Map the critical products and services


Define and test plausible scenarios


Visualize key operational resilience metrics

Why a digital platform, though? Couldn't manual processes and systems work just, as well?

Well, there's increased ROI to be garnered for going digital. A digital workspace, in particular, brings together all the tools and information needed to do resilience work. This centralization enables the best possible collaboration between team and stakeholders responsible for resilience activities, with the platform providing:


Workspaces for individuals


Workspaces for teams to collaborate around planning, risk management, and more


Workspaces for everyone engaged on an incident

Having that workspace be integrated, i.e., covering not only resilience but also business continuity, risk and compliance, security operations, threat intelligence, incident and crisis management, and situational awareness, also has its value – and not just financial ROI.

For one, all the capabilities you will need are in one place, meaning resilience data and information are consolidated, available throughout their entire lifecycle. This cuts down on information silos, consolidates reporting and analysis, while, of course, lowering the total cost of ownership.

Users also receive a consistent experience. They can manage any type of event with familiar tools and (powerful) workflows.

Not just any type of event, either. Users can also use the digital workspace in question to manage any scale of event – from routine, business as usual to full-bore crisis.

Finally, a fully functioning operational resilience program, in this era of compounding crises, will likely be the difference between business success and lights out. But getting such a program off the ground requires understanding what operational resilience is and what it's not, i.e., business continuity done well.

Over the course of this guide, we have sought to unpack the key differences between the two fields, lay out best-practice operational resilience measures, and identify what digital resilience management software capabilities are needed to get your operational resilience program up and running quickly.

With resilience challenges (and opportunities) emerging daily, it's now incumbent on all firms, whether they're in heavily regulated industries or not, to heed these learnings and develop the capability to foresee, prepare for, and adapt to disruptions, while maintaining continuous operations and safeguarding people, assets, and your reputation. For, if recent history is any guide, your competitors likely will.

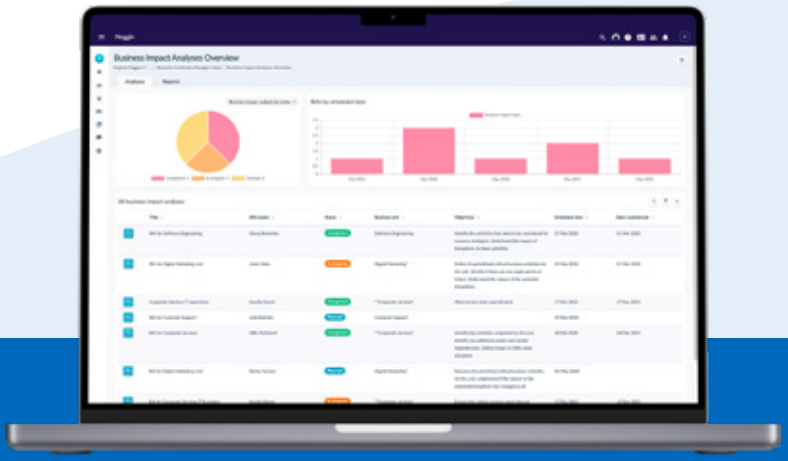
Sources

i. *BCI: BCI Operational Resilience Report 2022. Available at https://www.thebci.org/resource/bci-operational-resilience-report-2022.html.*

ii. *Bank of England: Operational resilience of the financial sector. Available at https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector.*

Like what you read? Follow Noggin on social media

@teamnoggin facebook.com/teamnoggin linkedin.com/company/noggin-it



noggin
for Business Continuity

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Business Continuity gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Business Continuity solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: **www.noggin.io**
or contact: **sales@noggin.io**