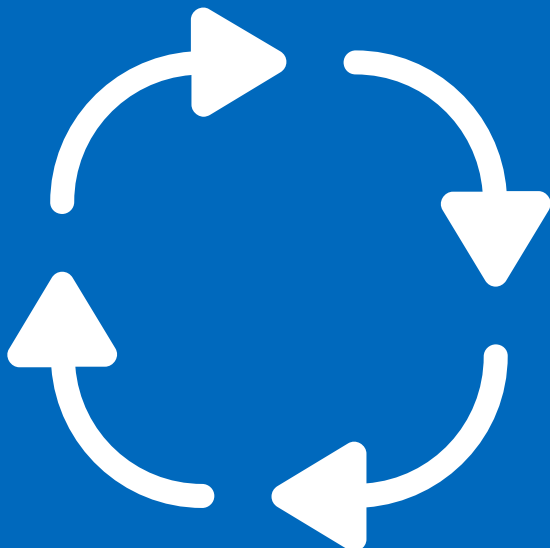


What Is Resilience Management?



Defining resilience management

In the business world, we define resilience as the ability to recover quickly from a crisis and to bounce back better. What then are the set of business processes responsible for ensuring that that happens? That's resilience management, the process of integrating all of an organization's protective activities.

Resilience management, as we commonly understand it, consists of two primary areas:

- 1 readiness or preparedness
- 2 and response.

Both areas fall under the unified resilience management structure.

Examining the rise of resilience management

Resilience management might appear to us today as a new field in business management. But it has a lengthy history, going back to the introduction of the first business computer systems.

Like today's systems, the business computer systems of the past served the purpose of integrating mission-critical data. They offered significant productivity gains. However, they also introduced new points of failure.

As a result, disaster recovery plans – the first resilience management outputs – began to crop up in IT departments.

Regulators also began taking an interest, beginning in the U.S. financial services industry, home to a high concentration of corporate data centers. The Office of the Comptroller of Currency, for instance, issued a circular in the early 1980s, compelling U.S. banks to have formal disaster recovery plans with provisions for their off-site assets.

In the 1990s, policymakers and regulators in public healthcare, telecommunications, and government services also intervened, with legislation like the Health Insurance Portability and Accountability Act (HIPAA) (1996) and Telecommunications Act (1996).

Both pieces required organizations to have IT disaster recovery provisions to ensure the availability of systems and the security of customer records respectively.

Meanwhile, in the government services sector, a significant Executive Order mandated heads of federal departments and agencies to ensure the continuity of essential functions by (a) safekeeping essential resources and records and (b) developing emergency operating capabilities.

Why resilience management now?

What about today?

Just like in the past, historic crises and/or major technological developments have a way of bringing resilience management to the fore. We've experience both with the pandemic and the increasing rise of service dependencies on cloud-based technologies.

In particular, the risk businesses face of disruption, realized during the pandemic, has only intensified, given the widespread adoption of digital solutions and the increasing use of outsourced service providers.


Add to the mix, organizations, since the pandemic, are functioning in a completely different operational environment, often having fundamentally changed the way they interact with technology, customers, and their own employees.


It's this need to adapt to (and accelerate) the pace of change that increases the risk of disruption, particularly to digital capabilities.

However, it's the same need to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and brand equity that makes resilience management more important than ever before.

The benefits of resilience management

So, how do resilience management activities help, actually? Well, some of the key benefits of resilience management include:

 **Resilience management enables proactive organizational decision making.** Resilience management helps to improve the management of information. Relevant information is made available to decision makers in a timely manner, helping to facilitate proactive decision making.

 **Resilience management helps to control or prevent abrupt disruptions and accelerates recovery should disruptions happen.** Proactive decisions are made before incidents occur. As a result of resilience management initiatives, then, companies get the benefit of controlling abrupt disruptions – or preventing them altogether.

Should those disruptions happen anyway, resilience management ensures that organizations are able to respond and recover quickly. Benefits such as information management, improved collaboration, and better decision making, therefore, serve the purpose of accelerating recovery when disruptions do occur.



Resilience management mitigates risks to service-delivery dependencies. As noted, the number of service-delivery dependencies a given company has keeps increasing. By providing visibility into those dependencies, as resilience management seeks to do, risk is mitigated.




Resilience management tamps down on cyber risk. One of the primary risk vectors companies face today is cyber and ransomware risk. By highlighting these vulnerabilities, resilience management forces companies to act to ensure cyber risk has been mitigated. The same applies to digital services that have not been outsourced.




Resilience management helps companies adjust to operating in different environments. As noted, the pandemic has precipitated stark changes in the way businesses interact with technology, customers, and their own employees. These changes can invite new risks. Resilience management, by uncovering these risks, can help companies address new threats.

What are the different types of resilience management?

Resilience management offers myriad benefits because of the number of modalities it encompasses. The main types of resilience management include:

 **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.

 **Organizational resilience.** The broad category of resilience management known as organizational resilience refers to the ability of an enterprise to absorb change and adapt to a new environment.



Cyber resilience. According to the National Institute of Standards and Technology, cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. A set of capabilities, cyber resiliency enables companies to pursue those business objectives dependent on cyber resources in a contested cyber environment.



The difference between operational resilience and organizational resilience

Often, the modalities, or types, of resilience management overlap. Nevertheless, it's important to understand some of the salient differences.

For instance, organizational resilience deals more broadly with the ability of an enterprise to absorb change and adapt to a new environment.

On the other hand, operational resilience relates to 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.

The difference between operational resilience and business continuity management

How, then, does operational resilience contrast with the related field of business continuity management?

One of the differences between business continuity and operational resilience is that practitioners of the former are 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 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.

The role of digital technology in achieving key resilience management aims

So, how to achieve resilience management aims in your business? Integrated resilience management software helps implement resilience management practices expeditiously, scale programs, and ensure constant improvement.

The capabilities that matter include:



Platform-first. A resilience workplace should be able to consolidate all your resilience data in one secure, centrally governed platform, as opposed to the typical practice of running different point solutions for communication, collaboration, risk, incident management, safety, security, business continuity planning, and more.

The platform-first approach also cuts down on integration work (and costs), while avoiding the user experience messiness so common in this field.



Automation. Getting started quickly is important, but your resilience management platform should also make life easier for you and your team when it's up and running, as well. Needed to make that happen is a platform with a powerful workflow engine. This engine should allow Managers to automate key resilience tasks, by building their own workflows with notifications, business rules, approvals, and much more.



Included GRC Module. You can get better bang for your buck with a resilience management platform that includes Governance, Risk, & Compliance (GRC) functionality. Why? Besides avoiding redundancy, such a Module will work to manage cyber, emergency, and security threats, risks, and treatments based on industry best-practice guidelines and ISO standards, as well.



Integrations. Besides including a GRC Module, a resilience management platform should also come equipped with a full range of integration options. Indeed, the platform, to garner better ROI, should be deliberately architected to play well with other resilience-enhancing technologies.



BIA. The BIA remains a mainstay exercise in resilience management. And so, your resilience management platform should work with forward-looking Managers to make that exercise more agile and pleasurable for all involved. To that end, the platform should make the BIA process as simple and efficient as possible, with the aim of promoting greater usability across the entire organization.



Dynamic planning. The resilience management platform itself should function as a plan. That way when customers need to develop their business continuity plans (BCPs) or other resilience assets, all the data they have previously entered seamlessly comes together. Managers, then, won't have to go sifting through documents to find the data they need. And the risk of someone referencing an out-of-date BCP during a crisis is removed.



Enhanced exercise management. Plans, of course, must be exercised. To facilitate exercising, resilience management software should provide exercise dashboards that navigate users and their teams through each stage of an exercise. That will help ensure that everyone understands what needs to be completed and when.

Finally, resilience management, after the experience of the pandemic, is a mantra in business circles, as the ability to prepare for, recover quickly from, and bounce back better from a crisis becomes mission critical.

As this article has noted, there are many approaches to and aspects of resilience management. But key to getting resilience management right is having the appropriate digital tools for getting best-practice resilience management activities up and running. For more on the capabilities needed to ensure resilience, download our **Buyer's Guide to Resilience Management Software.**



Like what you read? Follow Noggin on social media



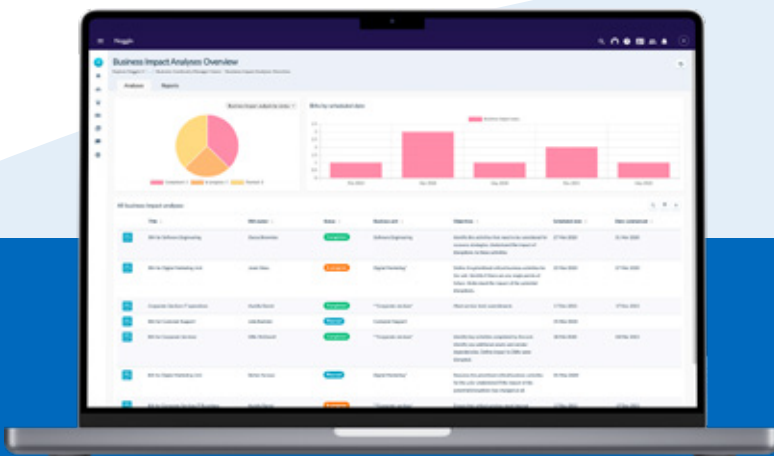
@teamnoggin



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