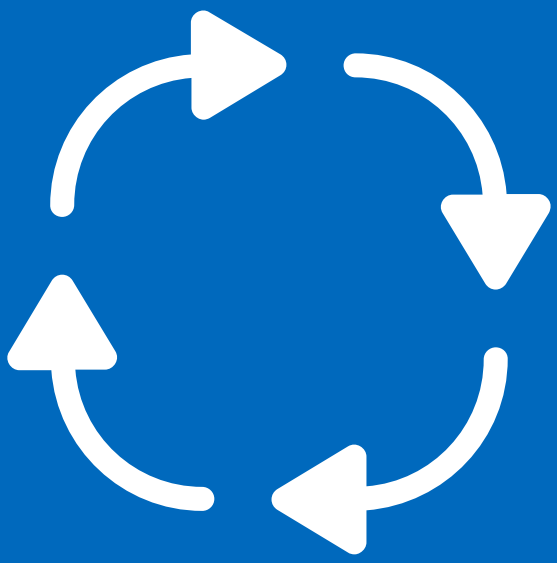
noggin | Business Continuity

# A Resilience Management Software Buyer's Guide



# Resilience management has never been more important.

Organizations have more dependencies than ever before. The risk they face of disruption, as a result, 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.

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

# Shifts in the regulatory environment also increase the salience of operational resilience.

Another major factor in the increased significance of resilience management is the rapid uptick in resilience-related regulations, particularly in the financial services sector. A few years ago, the Bank of England (BoE) stood out as one of the only major regulators to mandate operational resilience standards.

Now, however, the regulatory path paved by the BoE has been taken up by other national and supranational regulators, too.

The Australian Prudential Regulation Authority (APRA,) for one, 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 resilience of individual firms. That way no firm can pose a systemic risk to the wider business sector.

What's more, the resilience principles propounded 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? This new compliance environment represents a shift in how regulators and policymakers think organizations should be addressing the threat of disruption. In other words, organizations should now assume that disruption is inevitable and prepare to recover.

These assumptions mark a clear change in focus away from protecting individual organizations and their reputation to preventing incidents from impacting consumers and wider markets. And so, organizations must ask themselves if they have the capabilities in place to ensure compliance as well as build thriving resilience programs in order to quickly adapt to disruptions while maintaining continuous business operations.

# Resilience management software capabilities you need

To those that don't, likely the majority, an integrated resilience management workspace will help. Such an integrated digital solution covers all aspects of resilience management, including incident and crisis management, situational awareness, business continuity, risk and compliance, security operations, and threat intelligence.

Why integrated, though? Integrated resilience management technology ensures that all necessary capabilities are in one place. To put a finer point on it: resilience data, reporting, and analysis are all consolidated and available across their entire lifecycle.

Besides eliminating information silos, this level of integration provides a consistent user experience. Practitioners manage any type of event with familiar tools and workflows.

And not just any type, but any scale, as well – from routine to crisis, with the cumulative effect being the lowering of total cost of ownership (TCO).

But what capabilities matter most to achieve these resilience aims? This buyer's guide to resilience management software lays them out.

## 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.

That's not all, though.

Look for a platform that comes equipped with no-code designers. That makes it easier to adapt and change as needed, by configuring new Modules to solve novel use cases.

A library of configuration options and best-practice solution templates, with nothing to install and supportive of many devices and format, will also help you get started quicker – as will a responsive user interface, which enables you to design forms and workspaces once and then to access the same information and features across desktop, tablet, and mobile.

You should also be able to integrate the resilience management platform with key corporate systems, including for HR, BI, Identity Management, GIS, and more.

## 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.

Relevant capabilities to consider, here, include:

Automated BIA (Business Impact Analysis) reports, BCPs (Business Continuity Plans), and recovery-strategies' approval process

Automated notifications to prioritized business activity owners whenever the RTO (Recovery Time Objective) is changed on a business asset their activity is dependent on

Pre-configured workflow for incident escalations. Once an incident is created, and the severity changes from Critical, High, Medium to Low, different voice messages, emails, and SMS notifications are triggered.

And once a BIA or exercise is completed, the next one is automatically scheduled, removing the risk the user will forget it.

## Included GRC Module.

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.

What should such a Module look like? Well, the Module should enable customers to plan their objectives, set targets, manage all elements of standards' compliance, as well as schedule and record audits and inspections. Customers should also be able to manage non-compliances and corrective actions to drive continual improvement.

## 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.

It should do so through the easy connection and synchronization of data. Add to that, import, export, and API capabilities should also help to ensure that customers can always get their data when and where they need it, and that they can plug in their own systems (e.g., single sign-on, messaging, and mapping) into the resilience management platform.

## 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. To do so, the platform should have an easy step-by-step guide on its BIA dashboard to help guide stakeholders through the process.

The relevant functionality should look like this:

The BIA dashboard provides a helpful snapshot of the BIA, with key information such as status, due date, and who the owner of the BIA is.

Adding a new prioritized activity is easy. A simple, intuitive interface guides team members, highlighting what information needs to be entered, so that users won't find the process laborious or complicated.

Users can easily visualize which prioritized activities support their key product(s) and services.

The prioritized activities MTPD is automatically calculated for the user based upon the shortest time period from the impact assessments, where the impact reaches a critical level.

The RTO is also automatically calculated based on the minimum RTO of the activities' dependencies.

Prioritized business activity owners are automatically sent notification whenever the RTO is changed on a business asset their activity is dependent on.

It's easy to record any recommendations that have arisen as part of the BIA process; Managers can assign recommendations to a specific user, with a due date and priority level, and can even specify if the recommendation would be a long- or short-term resolution.

Once the BIA process has been completed, it only takes a few clicks to create a report and easily send it off to the Approver for sign off. That Approver will automatically be notified. Reports themselves can also be given a version number for auditing purposes.

## Dynamic planning.

Along these lines, resilience planning, as noted by industry experts, has also become more complex "as the range of possible threat scenarios keeps changing and expanding"[i].

As a result, the resilience management platform itself should function as a plan. That way when customers need to develop their BCPs or other plans, 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.

What's more, because the plan is in the platform, multiple stakeholders will be able to collaborate on the plan, which enables better engagement. All data associated with building the BCP will also be managed centrally, in a controlled way. Data, after all, only need be captured once and updated, removing the risk of duplication.

## 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.

From there, the platform's automation capabilities should ensure the correct teams and/or personnel are invited to participate in the exercise and receive regular updates via automated notifications throughout the exercise.

Once the exercise is activated, all users will then be able to see what type of exercise is being completed. And based upon the affected assets/activities, the recovery strategies required for the affected assets will automatically be populated for the team.

Built-in communication and collaboration tools, e.g., chat, email, SMS, and voice messages, will, then, make it easy to collaborate in real time, better coordinate responses, and keep everyone informed.

Resilience management software should also provide the capability to record meetings, minutes, and action items. This exercise management functionality should also mirror the platform's incident management functionality, to ensure a consistent user experiment that will give users the benefit of familiarity in the event of a crisis.

Finally, the resilience management platform should also facilitate greater self-management, increased accountability, and more agile response. That way the team keeps improvement and decision makers have line of sight into what's going on.

How to accomplish it?

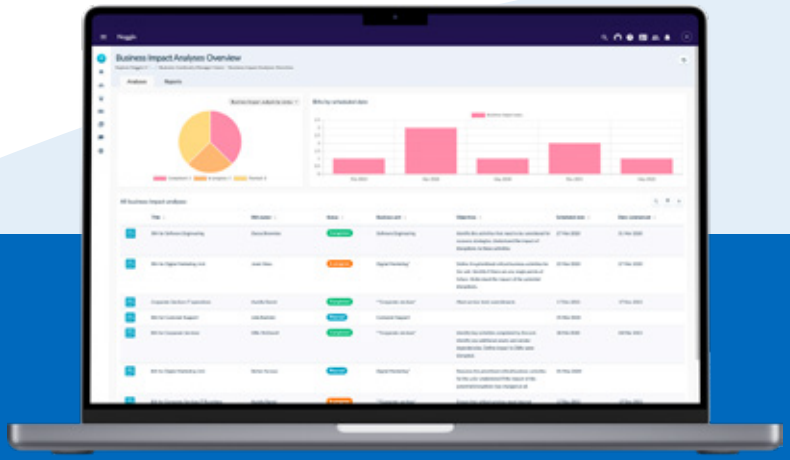
Your resilience management software should provide personalized user workspaces. Within these workspaces, users should be able to visualize outstanding tasks (whether BIA activity, incidents, exercises, etc.) that have been assigned to them, as well as any checklist actions items which still need to be actioned as part of the exercise or incident response.

The above is key. Not only should your resilience management software capitalize on the modernization of methodologies and tools in the provision of resilience and business continuity services, but it should also facilitate greater agility in the implementation of your programs, plans, and projects.

Paired with greater process automation, such a resilience management capability lends itself to improved efficiency. And with improved efficiency comes significant time (and cost) savings in response, recovery, and restoration.

## Sources

i. *Steve Culp, Forbes: Taking A New Look At Business Continuity Planning. Available at https://www.forbes.com/sites/steveculp/2021/10/04/taking-a-new-look-at-business-continuity-planning/?sh=5c08614e54aa.*



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**