noggin | Business Continuity

The Business Case for Integrated Resilience Management Software

The many facets of resilience management

Resilience is the ability of an organization to foresee, prepare for, and adapt to disruption while maintaining continuous operations and safeguarding its people, assets, and reputations[i]. Meanwhile, resilience management refers to the set of business processes needed to build such a capability by integrating all of an organization's protective activities.

Typically, the protective activities that go into resilience management vary depending on the disruption risk a given entity seeks to mitigate. What then are the main types of resilience management? They 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.

Digital resilience. An aspect of operational resilience, digital operational resilience refers to the ability of a business to build, assure, and review its operational integrity and reliability. Digital operational resilience is secured and maintained when a business boasts the full range of ICT-related capabilities needed to address the security of those network and information systems that support the continued provision of a business' services and their quality even through disruption.

These modalities, or types, of resilience management overlap. However, there are important distinctions between them.

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 more narrowly 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.

Meanwhile, business continuity practitioners are responsible for the management of prioritized activities, i.e., those activities that make critical products and services happen.

This differs from operational resilience in that the latter is more concerned with the management of critical products and services. Here, these critical products and services are those 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.

For their part, cyber and digital resilience tend to deal with ICT risk to digital assets. Those threats have historically included hardware and software failure, human error, spam, viruses, and malicious attacks. But they can also include natural disasters (e.g., fires, severe storms, and/or floods) that damage information assets.

Severe weather, of course, has typically been seen as a business or organizational resilience challenge, with organizational resilience covering all key threats to continuous business operations.

Resilience management must be holistic

The distinctions between the varying aspects of resilience management – operational, digital, cyber, etc. – seem like they might militate against an integrated approach to resilience. But in practice, resilience management to be effective must be holistic.

That means resilience management activities must work together to:

- Prevent disruption
- Anticipate and prepare for disruption
- Respond to and recover from disruption
- Withstand and sustain disruption

To do so, these activities must pull together what are typically distinct business enterprises including operations, technology, workforce, supply chain, data, finance, reputation, and customer experience. Resilience management itself must cover the following solution areas:

- Threat intelligence
- Incident and crisis management
- Situational awareness
- Business continuity
- Risk and compliance
- Security operations

Individual point solutions don't work well for resilience, and they get expensive quickly.

Of course, most businesses have end-to-end programs in place to address these matters. Not just that. Most businesses have point solutions in place for each solution area.

However, if resilience itself can only be achieved if all solution areas are working in harmony, why do so many companies operate in silos? This indeed is a keen challenge to building an integrated resilience capability to foresee, prepare for, and adapt to disruption, and precisely why so many organizations fail at the task.

Instead of uniting, they are actively dividing – meaning that when a risk that cuts across solution areas materializes, they aren't able to respond effectively. Why's that?

Well, having distinct point solutions for the varying aspects of resilience management means that you don't have all the capabilities you need in one place. More specifically, resilience data and information remain fragmented throughout the resilience lifecycle. Information remains siloed.

Point solutions themselves each have different user experiences, meaning a greater training lift for Resilience Managers when responding to cross-cutting crises as they will lack familiarity with tools and workflows.

Further, point solutions rarely manage different scales of event. They either manage routine or crisis, never the two, even though most crises can be sourced back to the day to day.

Most significantly in an age of strained budgets, having multiple point solutions, many of which do similar things and address similar risks, gets expensive quickly.

Total cost of ownership balloons when having to make crucial updates to multiple systems – rather than one. And lack of consolidated reporting and analysis means businesses still incur compliance risk or won't learn everything there is to learn from a disruption they've weathered as information will be strewn across multiple systems.

The business case for integrated resilience management software

That's because point solutions, by their very nature, pull against effective collaboration in resilience management. Collaboration, here, entails sharing information and advice, coordinating actions, communicating effectively, analyzing situations from multiple perspectives, considering different aspects and impacts of options, and supporting a whole team to be effective, productive, and healthy.

Why's collaboration so important to resilience? Well, effective collaboration helps:

- Risk and threat identification and assessment
- Situational awareness and understanding
- Decision making
- Planning that is comprehensive and practical
- Execution of plans and playbooks
- Communication across internal and external stakeholders
- Responding quickly

Of course, ensuring effective collaboration isn't the only thing integrated resilience management software does better than point solutions. What then is the business case for integrated resilience management software? It consists of the following:

- All the capabilities you need in one place
- Resilience data and information consolidated and available across the lifecycle
- Consistent user experience
- No information silos
- Manage any type of event with familiar tools and workflows
- Manage any scale of event from routine to crisis
- Consolidate reporting and analysis
- Lower total cost of ownership

Why a digital resilience workspace platform?

Not all integrated resilience management software solutions provide the same benefits, though. What then to look for?

For starters, look for a digital workspace. What's that?

A digital workspace brings together the tools and information you need to do resilience work and enables the best collaboration in the following resilience solution areas:


Threat intelligence


Incident and crisis management


Situational awareness


Business continuity


Risk and compliance


Security operations

And workspace? Well, a digital workspace can be provided for individuals, teams collaborating on planning, risk management, and more, as well as everyone else engaged in incident response.

Digital workspaces should be platforms, too. That way there's no need for different solutions for communications, risk, incident management, safety, security, BCP, etc.

A platform also means less integration work, cost, and user experience messiness. You also get to consolidate all resilience data in one secure, centrally-governed system; and you can integrate once with key corporate systems - HR, BI, Identity Management, GIS, and more.

What's more, no-code designers mean it is easily adapted as needs change. For example, teams can configure new modules easily to solve new use cases, including in-house.

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.

What other capabilities matter? Consider:

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"[ii].

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 – these are the key business benefits of resilience management software that should make your case for investment.

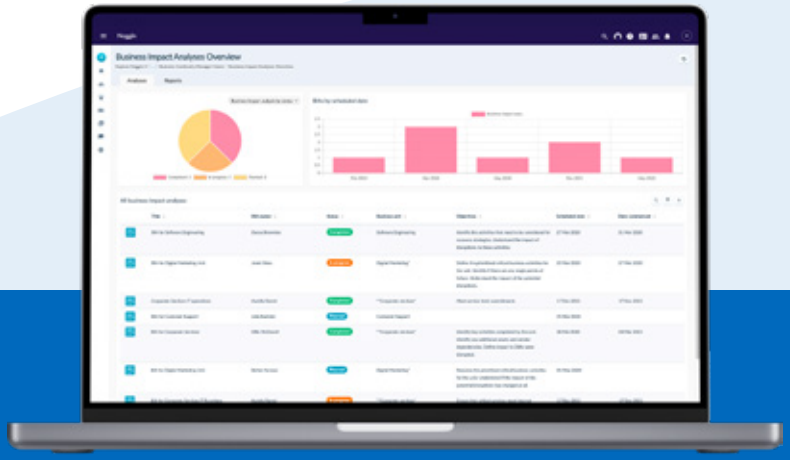
Sources

i. *Available at https://www.techtarget.com/searchcio/definition/business-resilience#:~:text=Business%20resilience%20is%20the%20ability,assets%20and%20overall%20brand%20equity.*

ii. *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.*

Like what you read? Follow Noggin on social media

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



noggin

for Risk Management

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

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