Why You Need More Than a BCM Plan to Be Truly Resilient

riskonnect.
Integrated Risk Management Solutions™

Intro

Having a well-documented business continuity plan is a good initial step towards operational resilience, but in today's modern dynamic business environment relying solely on a static plan is simply not sufficient to detect vulnerabilities, minimise impact, and recover quickly from a crisis.

With the help of technology, the art of business continuity planning & operational resilience has evolved over time to include a variety of tools and techniques to ensure plans are fully documented and regularly tested and updated. Firms must also ensure response plans and communication channels are well established, whilst keeping an eye out for threats, risks, and potential crises.

In this eBook, we explain how BCM & operational resilience technology enables firms to automate BCM planning and align processes with resilience guidelines and standards to ensure true long-term resilience. We detail how advanced techniques like business process modelling, business impact assessments, advanced threat intelligence, crisis management, and emergency notification tools all contribute to overall resilience. Plus, we'll demonstrate how other business processes like ERM, third-party risk management, incident management, and robust cyber security practices will also bolster your resilience efforts.

Start building a more resilient, adaptive, and sustainable organisation today - discover how you can transform your approach to resilience and position your organisation to not just survive but thrive in a crisis.

What is operational resilience?

Operational resilience is a business's ability to withstand, adapt to, and recover from unexpected disruptions affecting people, processes, and technology. It goes beyond traditional business continuity management and operational risk management to help leaders futureproof their businesses and ensure longevity.

In today's volatile business environment - characterised by cyber threats, natural disasters, system failures, and global pandemics - operational resilience has become crucial for long-term sustainability. More recently, governments and regulators have introduced operational resilience guidelines to stipulate that business - such as financial services, water, gas, electric, and telecoms providers – must have mandatory operational resilience plans in place to protect critical infrastructure and minimise the impact of unexpected events and downtime on consumers and the wider economy.

Organisations that prioritise operational resilience are better equipped to:

1. Minimise the impact of unexpected incidents.
2. Protect their reputation.
3. Remain operational during a crisis or downtime.
4. Return to normal operations quickly.

By embedding operational resilience into their operations, businesses can ensure continuity of operations providing assurance to leadership and the board.

Why BCM Plans are Only the Foundation of Operational Resilience

Business continuity management (BCM) plans are an essential part of operational resilience – but they are not the only factor. Although BCM plans serve as a foundation, if these plans remain static, untested, unrevised, or unsupported by regular business impact assessments (BIAs), they fall short of meeting modern resilience needs. Organisations must treat BCM plans as living documents that are part of an automated process, revisiting and testing them regularly and analysing them for gaps to ensure they remain effective and relevant.

To further strengthen resilience plans, firms must also strive to anticipate and prevent unexpected events through best practice risk management, control setting, adequate governance & policies, external threat intelligence monitoring, and third-party risk management.

Firms must also have adequate measures in place to respond to incidents and crises quickly, like best practice incident management procedures with automated escalation and case management, and emergency notification tools and back up communication channels.

Limitations of Static BCM Plans

BCM plans that remain static documents without regular testing, revision, or Business Impact Analyses (BIAs) are inadequate for maintaining operations during a crisis. Paper-based or spreadsheet-driven systems are prone to human error and inefficiencies, and they lack scalability. Manual processes often result in outdated plans that fail to reflect current organisational structures or risks.

Common issues include:

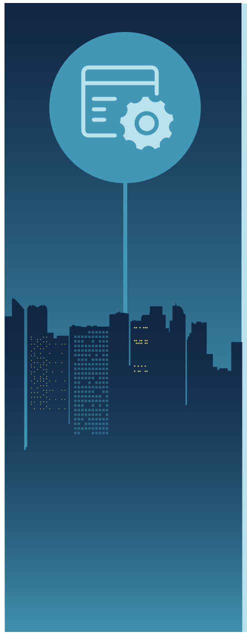
1. Insufficient scenario and vulnerability testing.
2. Inadequate awareness among staff.
3. No regular review process – leaving plans outdated.
4. No links to threat intelligence sources.
5. Failure to integrate with other business functions, policies and procedures.
6. Lack of continuous improvement.
7. Time-consuming and resource-intensive processes.
8. Prone to human error and inconsistencies.
9. Challenges in coordinating across departments.
10. Limited visibility into interdependencies.
11. Slow response times during actual crises.
12. Inefficient tracking and reporting of plan execution.

To be effective, BCM plans must be living documents that form part of an automated process that can evolve with the organisation and its environment.

Why Operational Resilience Requires more than a Business Continuity Plan

While creating static BCM plans for critical processes is a crucial first step towards operational resilience, it is merely the beginning. True operational resilience encompasses a wide range of practices and technology capabilities that enable an organisation to anticipate, prevent, respond to, and recover from disruptions.

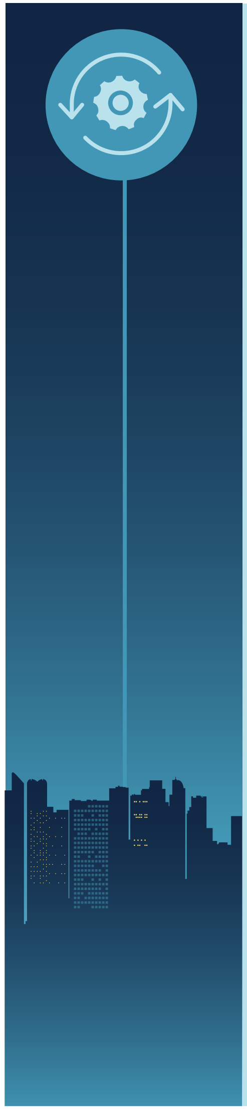
Let's explore the critical components and processes that contribute to comprehensive operational resilience. Here are 14 tried and tested processes that organisations can implement to boost resiliency:



1. Document and Automate BCM Plans Using Software

The first critical step to improve operational resilience is to capture your critical business processes and document your BCM plans. Most firms use BCM software to help them identify critical business processes, build a business process register, and formulate their BCM plans - using best-practice templates to ensure consistency.

These software platforms support Business continuity teams to determine key metrics such as Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), Work Recovery Times (WRTs), and Maximum Tolerable Downtimes (MTDs) – enabling them to set realistic recovery timelines. These systems can trigger BCM plans based on logged incidents, send mass notifications, and track recovery status in real-time.

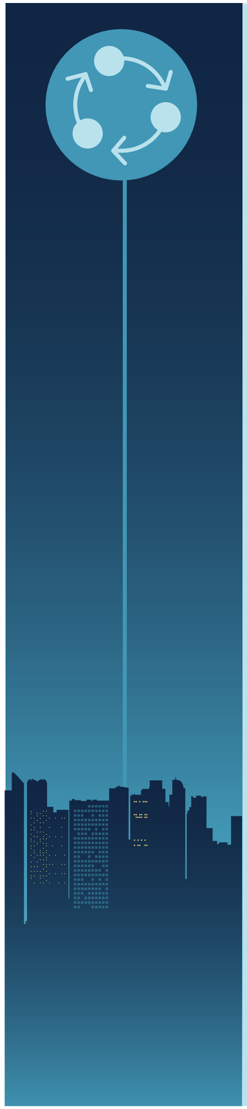


2. Automate BCM Plan Updates

BCM plans shouldn’t be static documents, they should be updated regularly - ensuring critical information such as processes, procedures, risk assessments, recovery strategies, and contact lists are always up-to-date and readily accessible. Automating this process using BCM software reduces the risk of human error and eliminates the time-consuming nature of manual updates, allowing teams to focus on strategic resilience planning rather than administrative tasks. Automated notifications alert staff when plans need to be checked or revised, and all changes are documented in the platform – plans can be mapped to your active directory ensuring plan owners are always current.

Resilience software typically allows for real-time tracking of changes to BCM plans, ensuring that all stakeholders are notified of updates. It also supports version control, enabling organisations to track and manage updates to plans over time. Additionally, BCM software often includes automated reminders for scheduled reviews and tests, helping ensure that plans remain current and aligned with any changes in the organisation's structure, operations, or external environment.

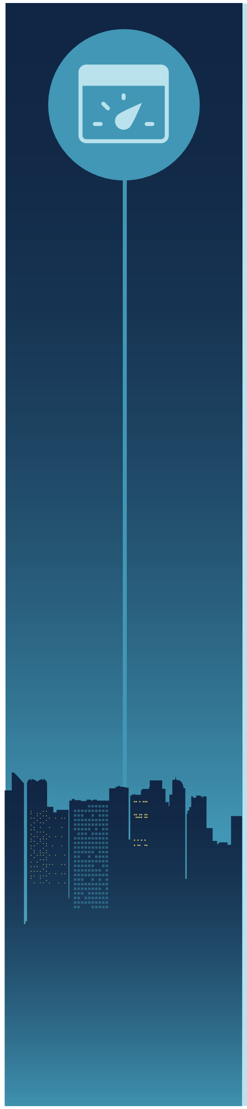
By implementing a BCM solution to automate vital aspects of their BCM plans, businesses can continuously refine their continuity strategies and BCM plans based on the latest information, organisational structure, and emerging risks. This proactive approach to BCM planning enhances an organisation's ability to respond effectively to disruptions, minimising downtime and maintaining critical operations. Ultimately, automating BCM plan updates transforms static documents into living, evolving frameworks that significantly bolster operational resilience.



3. Business Process Modelling

To boost resilience, firms should build a digital process model of their business to get a clear understanding of operational dependencies and potential impacts. Business Process Modelling (BPM) serves as an architectural blueprint for operational resilience - offering a comprehensive visualisation of an organisation's intricate process workflows and dependencies. This powerful tool goes beyond simple flowcharts - providing a dynamic representation of end-to-end processes and highlighting potential bottlenecks and gaps in your impact tolerance. By meticulously capturing each step in a business process, and mapping dependencies, organisations can quantify the cost and resource implications of potential disruptions with unprecedented accuracy. This level of detail enables leaders to make data-driven decisions during crises - effectively prioritising recovery efforts based on a clear understanding of operational impacts.

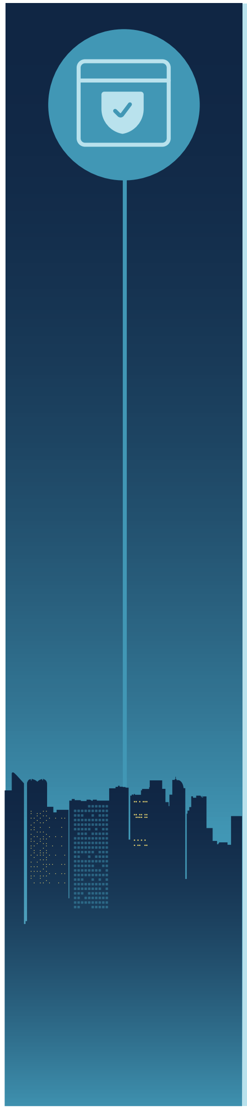
BPM is not just a static snapshot of operations, but a dynamic process that supports continuous improvement efforts. It allows teams to identify inefficiencies, streamline operations, and proactively address vulnerabilities before they escalate into major disruptions. The insights gained from comprehensive process modelling empower firms to optimise resource allocation, enhance productivity, and build more robust, resilient processes.



4. Business Impact Assessments (BIAs)

Business Impact Assessments (BIAs) are a cornerstone of operational resilience - providing a systematic approach for firms to understand and evaluate the potential consequences of disruptions on their key operations. By identifying critical business functions and processes, assessing the impact of disruptions over time, determining resource requirements for recovery, and establishing recovery priorities, BIAs enable organisations to make informed decisions about risk mitigation and resource allocation.

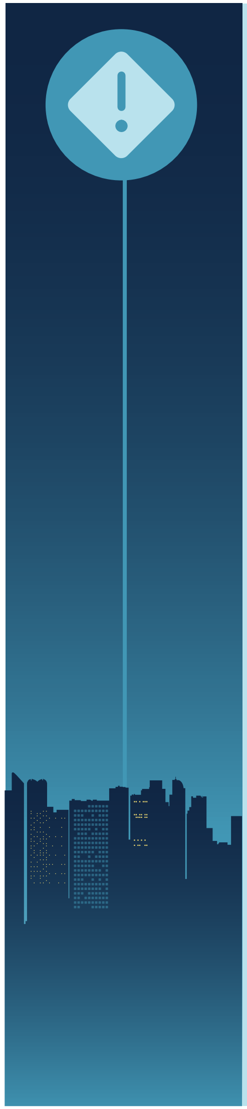
By pinpointing specific business activities that need to be prioritised for recovery, BIAs allow organisations to allocate resources efficiently and prepare effective contingency plans. The use of BCM software can significantly streamline the BIA process by using automated workflows to send and circulate BIA forms – with all data flowing into the platform. This makes it easier to identify gaps in recovery processes and allocate resources effectively. This technology-driven approach enables organisations to conduct more frequent and comprehensive impact assessments, ensuring that their resilience strategies remain up-to-date and aligned with evolving business needs, potential threats, regulatory requirements, and resilience standards.



5. Scenario and Vulnerability Testing

Scenario and vulnerability testing are critical components of a robust operational resilience strategy, providing organisations with invaluable insights into their preparedness for potential disruptions. This proactive process involves developing realistic crisis scenarios that mirror the complex challenges businesses may face, from cyberattacks, system downtime and natural disasters to supply chain disruptions and pandemics. By simulating these disruptions in a controlled environment, organisations can rigorously test their response capabilities - uncovering weaknesses in current plans and processes that might otherwise remain hidden until a real crisis strikes.

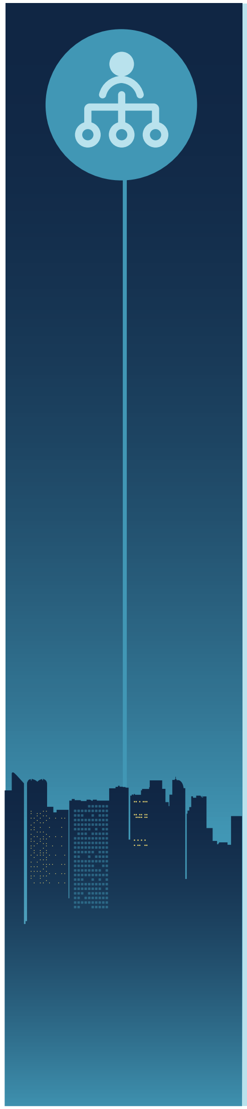
This comprehensive testing not only identifies gaps in preparedness but also helps to refine BCM plans, ensuring that contingency plans are practical, effective, and adaptable to various situations. These exercises enable staff to gain experience in crisis management and decision-making under pressure - ensuring that when a real disruption occurs, they are well-prepared to execute plans efficiently. Insights gained from these tests drive continuous improvement by highlighting gaps and vulnerabilities. When carried out using BCM software, scenario and vulnerability testing can transform static plans into dynamic, evolving frameworks that enhance an organisation's overall operational resilience, fostering a culture of preparedness and adaptability.



6. Enterprise Risk Management

Ensuring your organisation has a best-practice Enterprise Risk Management (ERM) program is another way to strengthen organisational resilience. By proactively identifying, managing and mitigating risk, firms can safeguard the organisation from potential issues before they occur.

Organisations should establish an active risk register – capturing key risks and their likelihood and impact. They should set Key Risk Indicators (KRIs) and monitor risk levels against their risk appetite. They should conduct regular risk assessments to understand risk exposure and set controls to reduce risk. Controls should be regularly checked and tested to ensure they are effective. When risk reaches an intolerable level there should be clearly defined escalation routes to ensure rising risk levels are dealt with promptly and addressed - and mitigating actions should be fully documented. Many firms use risk management software to streamline and automate this process - providing a centralised framework for identifying, assessing, and understanding risks in real time - these platforms enable businesses to prioritise vulnerabilities that could disrupt operations to move beyond reactive crisis management to strategic risk mitigation.

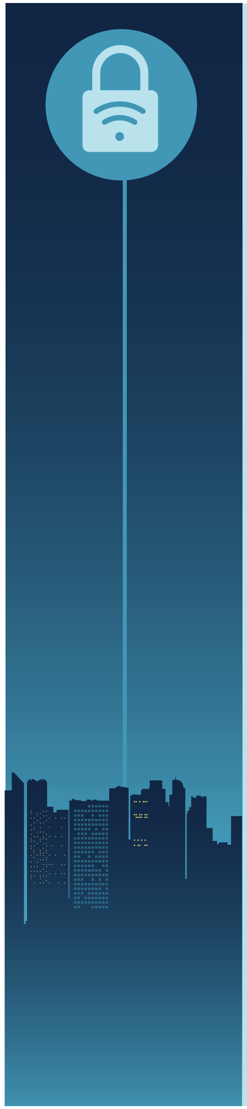


7. Third-Party Risk Management

Organisations increasingly rely on a network of third-party vendors, suppliers, and service providers to run their operations - opening them up to a variety of third-party risks. When a supplier fails to provide their service or product, it can severely impact operations affecting overall resilience.

Many organisations utilise specialist third party or vendor risk management tools to monitor supplier performance, compare vendors, and understand the associated risks. Staff build a vendor log within the solution using online forms to capture key details for each supplier regarding contract length, cost, relationship owner, and any SLA's or KPI's. This makes it easy for decision makers to compare vendors and allows them to set controls with automatic notifications to monitor performance against KPI's and SLA's.

Firms can use the vendor risk platform to automate key tasks including supplier onboarding, vendor risk assessments, questionnaires, and surveys - with all results logged in the system against the relevant vendor. Any potential risks can also be logged against each vendor and monitored on an on-going basis. Some solutions allow you to pull in live transactional & operational data relating to supplier performance from other systems & data sources - allowing risk teams to automatically monitor supplier performance against KPI's and SLA's and receive notifications of poor performance so it can be addressed. Some TPRM platforms even integrate with third-party risk intelligence sources enabling firms to get foresight of any convictions, financial difficulties, data breaches, and breaking news stories about potential or current vendors.



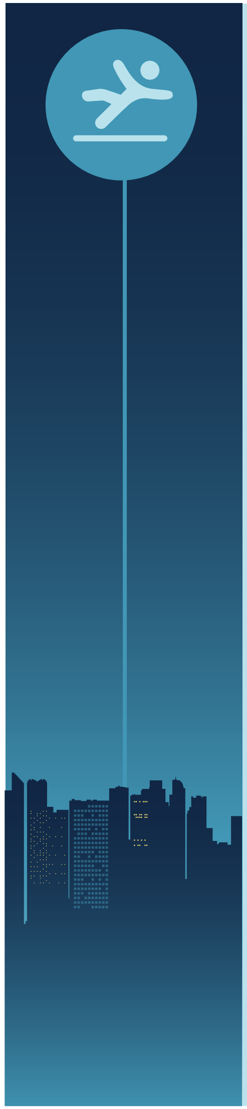
8. Cyber & IT Risk Management

With many organisations relying on a variety of digital systems and software applications to run their businesses, protecting those systems and ensuring they remain operational is essential to remain resilient.

Teams must effectively manage cyber risk by maintaining a cyber risk register, carrying out regular risk assessments, and setting the appropriate controls. These controls should be checked and tested regularly for their effectiveness. Cyber risks relating to third party providers should also be carefully managed and monitored with regular vendor risk assessments. Firms should also establish clear IT policies relating to data privacy and equipment & internet usage to maintain IT security standards.

A clear cyber incident process should also be established to ensure staff can log potential cyber incidents quickly and that they are escalated and resolved in a timely manner. Firms should also implement defined processes to comply with relevant data privacy laws like GDPR, HIPAA, ISO 27001, NIST, CPS 234, and SOC 2, and they should also formalise a procedure to facilitate and document any cyber audits.

Implementing these vital IT security and cyber risk management processes is essential to safeguard the organisation and ensure that vital digital systems and platforms remain operational – building overall resilience.

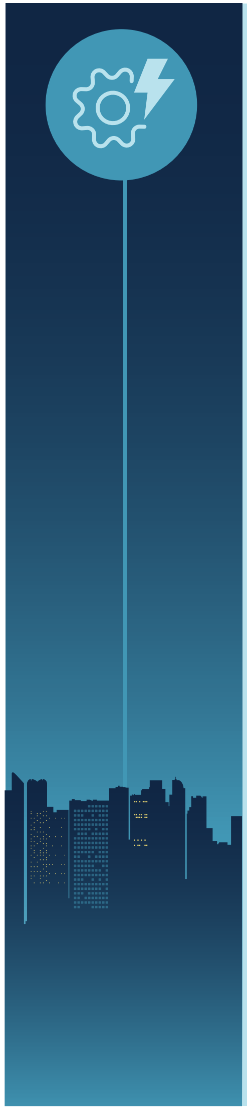


9. Incident Management

Building an effective incident response and crisis management process is a vital component of operational resilience. Your organisation must establish clear protocols for detecting, reporting, and successfully responding to incidents to minimise their impact and ensure swift recovery.

Most firms use an incident management platform to automate the incident management process. Staff can log incidents, hazards and near misses via online forms and all data feeds into the platform. Forms can be customised based on the type of incident logged to ensure relevant details are captured – staff can even upload evidence such as photos & documents. Predefined workflows ensure the incident is promptly categorised, triaged and escalated to the relevant teams, and case management workflows facilitate thorough investigation and root cause analysis to ensure each incident is resolved in a timely manner.

Analysing historic incident & near-miss data is also a great way to pre-empt future risk events and incidents. From major incidents such as cyber-attacks & outages to minor incidents such as slips & trips, by analysing the data, organisations can delve into what risks caused the incident and what steps they can take to prevent future occurrences – boosting resilience and safeguarding your organisations reputation.

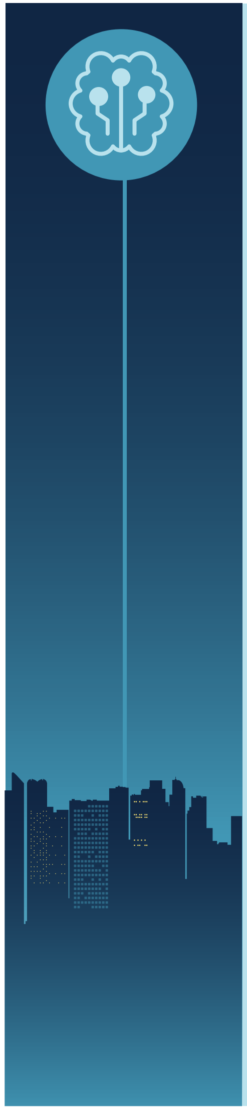


10. Crisis Management Plans

To further bolster resilience efforts, many firms also use software to formulate crisis management plans. Organisations can use software to build incident response templates and quickly transform plans into actionable checklists to mobilise and inform teams on the best course of action and appropriate next steps.

Firms can create incident response plans based on different types of incidents - ensuring the organisation is ready when a crisis strikes. Automated workflows are used to communicate key information and inform the right people. All tasks and actions can be tracked and monitored through a variety of dashboards & reports – providing leadership with clear visibility of the incident status and progression of the response plan.

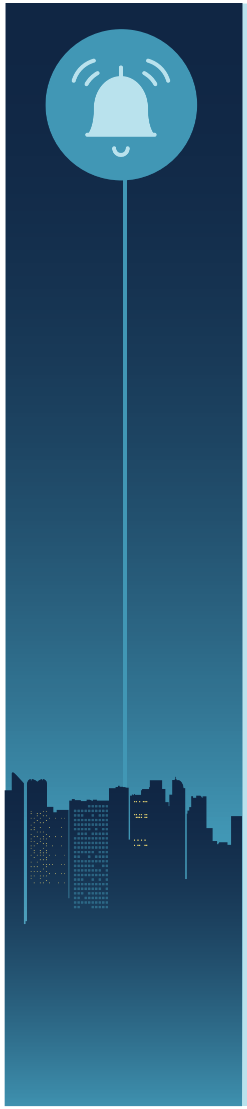
Many solutions also offer a mobile app with encrypted chat. This enables teams to complete actions and tasks on the move to speed up incident response times. These solutions often offer backup communication channels that can be used when primary communication channels like email are down – ensuring response teams can easily communicate with staff of all levels and collaborate on recovery plans.



11. External Threat Intelligence

To be proactive in their resilience planning, many firms choose to subscribe to external threat intelligence feeds from specialist content providers. This vital source of information enables them to get visibility of potential global threats and take the appropriate action before business operations are impacted. Whether it is a weather warning, a natural disaster, civil unrest, crime, the potential for sabotage via a cyber-attack or data breach, or geopolitical factors that could impact operations – firms can benefit from having foresight of these events. The tool pulls in information from global data sources like news feeds, federal government agencies, social media, and more to provide a complete overview of potential threats.

Feeds can usually be customised by geography, threat type and severity level – making it easy for firms to zero in on the factors that could impact them by viewing a live threat map. These feeds usually flow directly into the firms BCM and resilience planning tool, and automated workflows and alerts are used to notify the appropriate staff when a threat meets specific criteria. From there, teams can easily create a new incident or send a mass notification to address the threat. With all readiness and response activities managed in one central platform, businesses can get foresight of threats, streamline processes, and reduce manual workload.



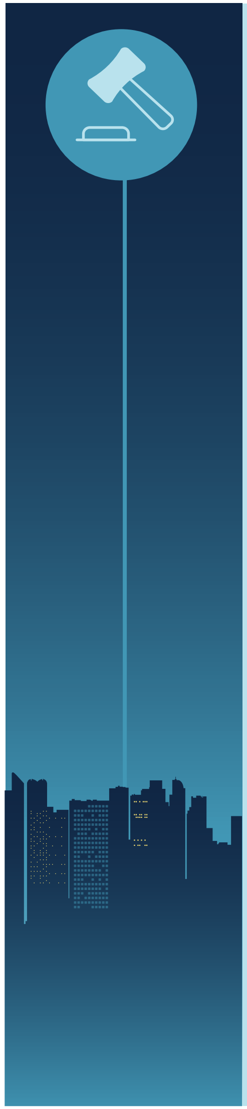
12. Emergency Notification Tools

Being resilient is not just about proactively preventing a crisis, it also requires an organisation to be able to respond quickly when a crisis strikes. That is why resilient firms implement emergency notification software to help them to communicate with staff effectively in an emergency and share information and updates. These solutions enable firms to centralise readiness and response activities in one platform.

Firms can create templated emergency communication messaging and holding statements to expedite communications and push tailored messages to geographic locations, facilities, teams, roles, and more – based on the appropriate time zone.

These solutions also provide a variety of back up communication channels (including voice messages, emails, SMS and WhatsApp) in case your primary channels are disrupted. The solutions can also send emergency mobile communications and teams can view sent messages and track delivery and response status. Firms can also record the status and safety of employees with easy-to-use survey response features.

Using an emergency notification platform will allow for tailored messaging to those named in a specific response plan. Some systems can integrate with your IT and HR systems to ensure contact information is accurate. This kind of tool builds resilience by speeding up response and recovery time while providing assurance to leadership teams.

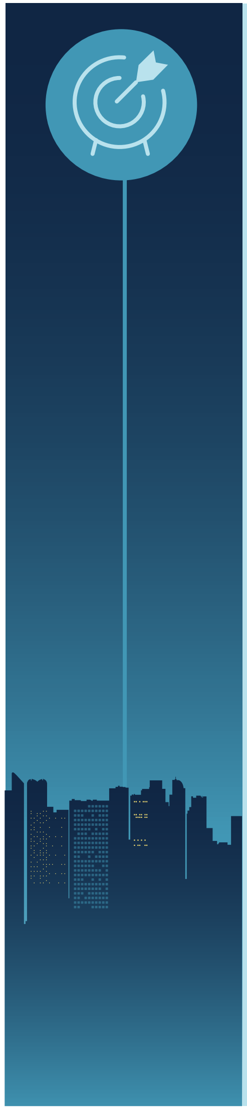


13. Compliance

Although not necessarily directly associated with resilience, ensuring the organisation is compliant with any mandatory regulations can promote resilience and longevity. In some sectors like financial services, gambling, and healthcare, they must comply with regulations to legally operate across different jurisdictions. Similarly, some companies must remain certified to certain standards like ISO standards, anti-slavery laws, or data privacy guidelines to win contracts. They must be able to provide proof of certification or compliance, or they risk losing vital business opportunities.

Firms must build an obligations library of applicable regulations and standards, carefully documenting each requirement and the process, procedure, or policy in place that proves compliance. They must formalise step-by-step processes and checks outlined in the requirements and provide documented evidence to regulators.

Managing regulatory change is also vital to remain compliant and ensure long-term resilience. Firms should scan the regulatory horizon for changes and map regulations and their requirements to the relevant processes, procedures, and policies, so when a change happens, they can quickly alter their existing procedures to comply - whilst fully documenting what was changed and when - to provide a complete audit trail for regulators. Many firms use GRC software to house their obligations library, automate compliance checks, and to manage regulatory change - as this ensures they have a best-practice process that aligns with regulatory requirements.



14. Aligning Your Strategy with Risk Management

Another surefire way to build overall resilience and ensure organisational success is to align risk management with your overall strategy. To ensure a successful resilient organisation, firms should map out a clear long-term strategy and break it down into smaller programs, actions, and tasks that will help them achieve their strategic goals. As each task is completed, this should be indicated at each level of the strategy, indicating progress.

Risks should be mapped out for each stage of the strategic plan so they can be carefully managed and controlled to ensure the strategy remains on track. Organisations don't have an infinite amount of money and resources to reduce every single risk they face. Aligning risk management with strategic goals will help firms to allocate money and manpower to the most pertinent risks that could affect their strategy – helping them to achieve success.

Aligning risk and strategic planning will also empower firms to take calculated risks where taking a potential risk could have long-term benefits for the organisation. Ultimately when risk management is aligned with your strategic vision it can help you achieve your strategic objectives, improve enterprise performance, and boost resilience.

Beyond BCM: The Multifaceted Nature of Operational Resilience

Achieving true operational resilience goes far beyond relying on a traditional business continuity management (BCM) plan. While a BCM plan is an essential starting point, the modern business environment demands a more dynamic, comprehensive approach that leverages technology, multiple processes, proactive threat oversight, and advanced techniques. By embracing tools and processes such as automated BCM software, business process modelling, business impact assessments, and external threat intelligence, organisations can ensure that their resilience strategies remain up-to-date, adaptable, agile, and effective. Regular scenario and vulnerability testing, along with integration of incident management and risk management practices, play a pivotal role in identifying potential weaknesses before they become critical. This proactive approach enables organisations to better anticipate, respond to, and recover from disruptions in a way that minimises impact and maintains operational stability.

A focus on continuous improvement, integration with other business functions, and an ability to respond quickly through automated notifications and crisis management tools all contribute to a business that is not only prepared for crises but can also recover quickly and even thrive in the face of adversity. By embedding resilience into the organisational culture and aligning it with broader strategic goals, businesses can safeguard their future, protect their reputation, and ensure long-term sustainability. Start integrating these resilience-building practices today, and empower your organisation to rise above disruptions, no matter their scale or nature.

riskonnect
Integrated Risk Management Solutions™

Implement Best-Practice BCM planning and Operational Resilience Strategies with Riskonnect

Riskonnect offers a whole suite of business continuity planning & operational resilience software capabilities to streamline and automate BCM planning and build resilience.

Use the platform to identify critical processes, formulate business continuity plans, automate plan updates, conduct BIAs, carry out scenario & vulnerability testing, and launch plans in a crisis. Add on features also include threat intelligence feeds, and crisis management and emergency notification capabilities.

Plus, you can further bolster your resilience efforts with best-practice risk management, third party risk, cyber risk, incident management, regulatory compliance, and strategic planning capabilities – all in one integrated platform!

Visit Website

Request Demo

riskonnect.com