everbridge
infiniteblue

Building an executable business continuity plan

Table of contents

Introduction

Today, organizations face an increasingly complex and dynamic risk landscape, with more frequent, severe, and concurrent disruptions than in the past. We developed this guide to help executive leadership and corporate risk professionals understand business continuity principles and best practices, assess their current level of readiness, and set a course for true enterprise resilience.

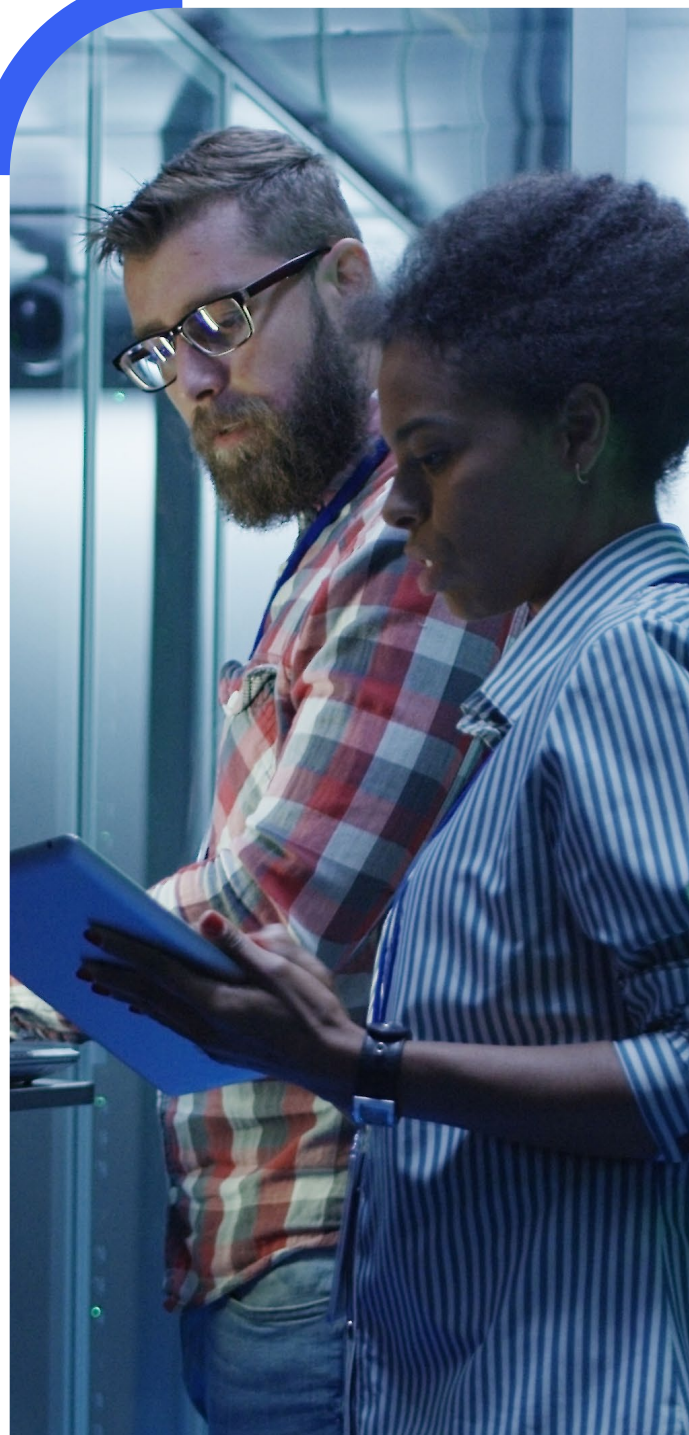
The first edition of this guide, published in 2021, quickly became a go-to resource for business continuity and disaster recovery (BCDR) practitioners. Since that time, the pandemic, escalating weather events, supply chain disruptions, and new regulatory regimes have led to important changes to the way organizations manage risk and resilience. This edition reflects that new thinking and draws insights from the past four tumultuous years.

Business continuity

What is business continuity?

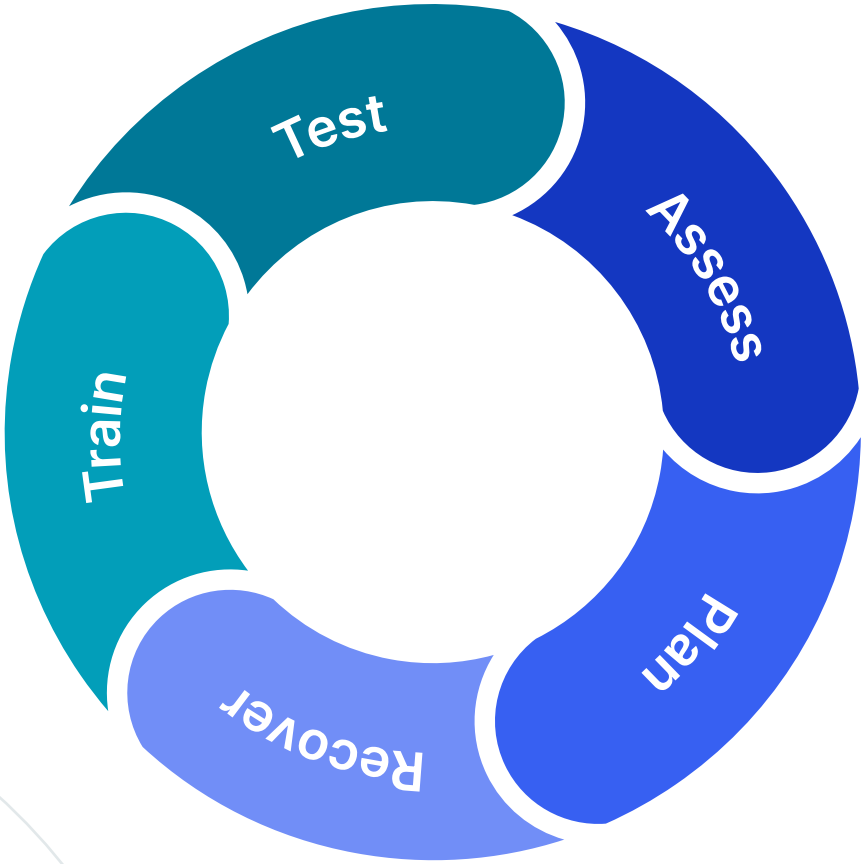
Business Continuity (BC) refers to the processes, protocols, and plans that allow organizations to manage potential disruptions and return to normal operations. The International Standards Organization (ISO) defines Business Continuity Management (BCM) as:

> "A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities."



Business continuity management lifecycle

The following illustrates the business continuity management lifecycle which, at a high level, consists of five phases.



- **Assess:** Identify and prioritize business processes and inventory the resources required for daily operations.
- **Plan:** Identify and prioritize risk mitigation and incident response strategies for specific scenarios.
- **Recover:** Outline the steps to return to normal operations should an incident occur. This is often referred to as Disaster Recovery.
- **Train:** Train the teams that will be integral to executing the plan. This is also an opportunity to increase plan awareness throughout an organization.
- **Test:** Tabletop and full-scale exercises that help validate, promote, and identify gaps in plans.

Business processes & inventory

The first step in building a BC plan involves identifying the high-level work performed in each department. It is important to note that disparate functions within a single department may be split along expertise and functionality.

PROCESSES: The following is an example of a business process inventory for a single department. The number of processes will vary, however, four or five is typical:

Finance Department

- Process 1 - Accounts Payable
- Process 2 - Accounts Receivable
- Process 3 - General Ledger
- Process 4 - Taxes

DEPENDENCIES AND RESOURCES: The following are typically needed to support business processes:

- **Applications –** This includes cloud and hosted applications, but not everyday office software, such as browsers, Google Suite, and MS Office.
- **Vendors/Suppliers –** These are third parties that may provide a service or a resource critical to the delivery of a process.
- **Specialized Equipment –** This includes any equipment needed for essential functions. When identifying equipment for a business continuity management plan, particular attention should be paid to items with long lead times and/or are highly customized and difficult to replace or source.
- **Just in Time Inventory –** These include high turnover items that a business process is dependent on. This could be custom printed stock, personal protective equipment (PPE), branded cardstock, or raw materials needed for manufacturing but are typically maintained in a consistently low inventory.

Business Impact Analysis (BIA)

A BIA prioritizes all business processes, assesses the impact of disruptions on each, and, in turn, the overall business.

The following are the major impact categories. Although these are typical across industry, not all apply to every organization:

- Brand/reputation
- Direct financial loss
- Operational compliance and regulatory
- Legal and contractual
- Customer Impact
- Life/Health/Safety

Once the impacts of potential disruptions are understood, it is easier to define the processes needed to prevent or mitigate losses.

There are three general categories of BIAs:

Product BIAs. These help organizations prioritize which products and services to protect and recover if there is a disruption.

Process BIAs. These identify which processes that must be performed regardless of circumstances.

Technology Impact Assessments. These identify critical IT assets that must be protected and restored to resume operations.

A BIA Questionnaire allows department leaders to identify the potential impacts if the business functions are interrupted. This exercise can help organizations determine what should be prioritized based on estimated recovery times, the potential cost, dependencies, gaps, and other criteria. For large, complex organizations, business continuity software can streamline and enhance this process.

The final BIA should identify the products, processes, and technology with the greatest operational and financial impacts and must be restored first.

Risk assessment

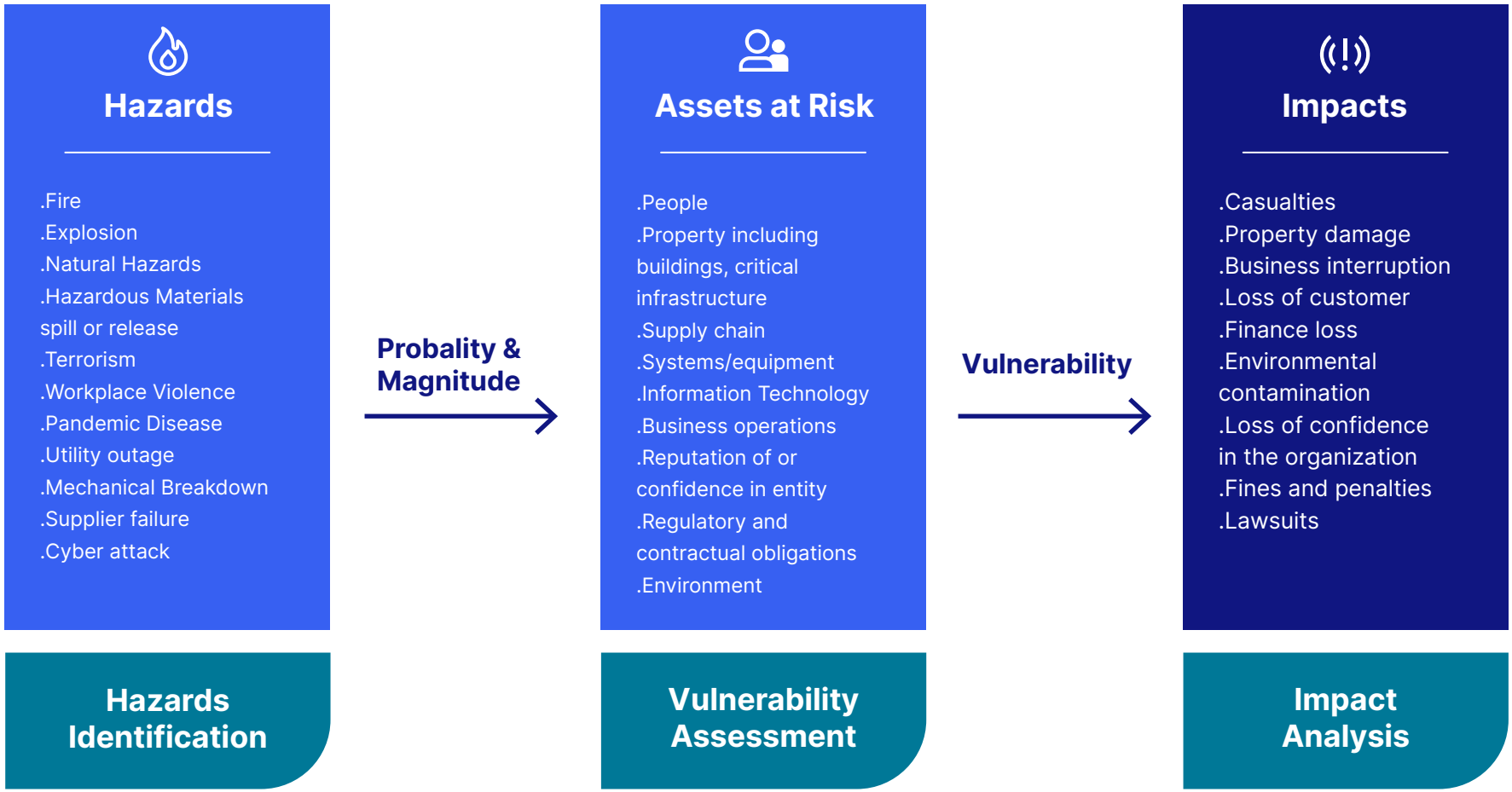
If the BIA reveals what may be impacted by an incident, the risk assessment identifies potential hazards, how likely they are to occur, and what can be done to prevent or mitigate a disruption. This phase also uncovers weaknesses in critical processes and procedures.

Developing a risk assessment

Absent a software solution, the easiest way to begin a risk assessment is by listing potential incidents, based on the type of business, location, assets, past events, and other factors. Examples could include:

- Ransomware/cyber breach
- Pandemic/disease outbreak
- Natural disasters
- Supply chain failure

This tool from ready.gov provides a framework for developing a risk assessment.



Once hazards are identified, organizations can then incorporate a recovery strategy for each scenario within its plan. Off-the-shelf flow chart tools are useful in this process.

Risk control

Risk controls are strategies that are already in place to reduce the likelihood of specific incidents and, should they occur, limit their impact. Methods typically include:

- **Preventive controls:** These controls are put in place at the root cause. Examples include system passwords, locked doors, and machinery maintenance.
- **Detective controls:** These rely on information analysis to detect that a risk is present.
- **Reactive controls:** These reduce the impact of a risk should it occur.

Risk treatment

With risks identified, these are proposed strategies to prevent them or mitigate their impact.

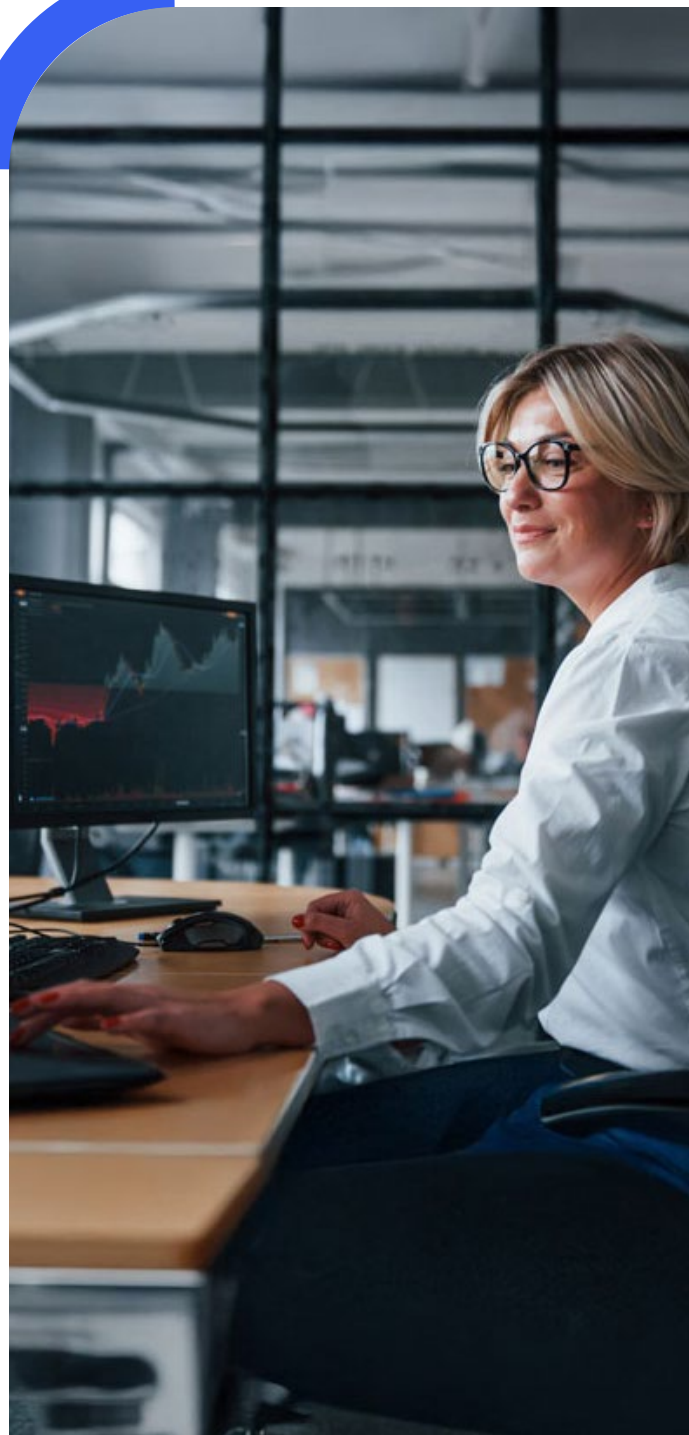
- **Avoid:** Eliminate the risk or threat. For example, secure alternate power supplies to combat outages.
- **Transfer:** Shift the risk to a third party, such as insurance or a vendor.
- **Mitigate:** Reduce the risk's likelihood or impact by, for example, installing fire suppression equipment.
- **Accept:** Acknowledge the risk and take no action unless it occurs.
- **Exploit:** Use an identified risk to improve an underlying technology or process.

Recovery strategies

With the BIA and risk assessment complete, recovery strategies must be developed, starting with the most critical processes. The scenario-based recovery approach focuses on the four major impacts to an organization.

- **Loss of Technology -** If the business unit lost the applications needed for the process, how would it be remediated? Is there other software they can use? Can it be done manually? Or are they so dependent on that application that there is no workaround?
- **Loss of Staff -** What would the business unit do if a significant percentage of their staff was unable to perform their duties? Remediation strategies might include using a vendor, transfer to another department, or cross training.
- **Loss of Facility -** Where is the work being done? What happens if that location is lost? Strategies should include transfer to another site, work from home, or outsource to a vendor.
- **Loss of Vendor -** Can the work be transferred in-house or to another vendor?

Each scenario should have multiple recovery strategies, timeframes, high-level steps needed, and resources required.



Exercising & testing

A business continuity plan should be tested regularly. And, while it may be impossible to simulate a flood or large-scale disaster, each step in a recovery process can be tested.

The four most common exercises are:

01 **Desktop walkthroughs and workshops.** During a desktop walkthrough or workshop, a team goes through a scenario and each team member relates how he or she would respond. These exercises are particularly effective for younger business continuity programs as they help familiarize team members with the plan and identity gaps.

02 **Tabletop exercise.** Third-party facilitators are often used for tabletop exercises so all members of the continuity program can participate. They will guide the team through the scenario while each team member explains his or her recovery process and responsibilities. An independent expert can also provide recommendations for improvement.

03 **Functional exercise.** This tests a team's ability to perform their duties in a simulated operational environment. This type of exercise helps to test specific team members, procedures, or resources, such as communications and notifications.

04 **Full-scale exercise.** These simulate real life incidents. While costly and time consuming, full-scale exercises are typically the most rigorous and effective and are important for regulated industries, such as public utilities.

Functional exercise example of a pandemic plan

Using the COVID-19 pandemic as an example

01 Pretend the office is closed immediately, send one IT person home.

02 Record how long it took them to get there and, once they've arrived, have them turn on their laptop and sign into any necessary applications.

03 Have an employee in the office shut down their computer work with the remote IT person to get it up and running on a VPN (or whatever you have set up in the case of a permanent working from home situation).

04 Walk through how you will notify employees. Will you email, call, use Slack, etc.? How many employees normally work from home vs. the office? Depending on work location, certain employees may need a specific method of communication.

05 Decide what guidelines you will set for employees that need to be in the office. Determine how often you communicate updates to your employees.

06 Imagine a key person in your plan gets COVID-19, who will fill in for them? What important data do they have access to and are they the only ones who can access it?

The risk assessment and BIA can be used to prioritize scenarios and exercises. BCM software can typically help run exercises and provide real-time data on the results.

After the exercise is complete, an analysis of the activity, including an anonymous survey of the participants, can serve as a guide for enhancing the plan, identifying gaps, any issues, or lessons learned and improving the plan and recovery strategies for future exercises.

Executing your BC plan

BC plans should not be owned by any one individual–it is critical that people across departments are invested and engaged. Having clearly defined roles before an incident occurs can result in greater coordination and a more effective response.

The diagram below shows the most common roles in an incident or disaster:

Learning

After an incident, resilient organizations take the time to analyze the response, collect feedback, and identify ways to improve the business continuity plan for future incidents.

Similarly, at least once a year, organizations should review critical processes, assets, risks, and response and recovery plans, and update the plan as appropriate.

Operational resilience

Since the financial crisis of 2008, the United Kingdom and the European Union have implemented a number of measures to minimize the likelihood or impact of events on organizations. They focused, primarily, on a combination of planning, strategy, and technology.

These steps–some of which are encompassed by BCP–were codified in the Operational Resilience guidelines set forth by the Bank of England for the financial conduct authority (FCA) and Prudential Regulation Authority (PRA) for the UK and the Digital Operational Resilience Act (DORA) for the EU.

Enacted to better understand the importance of business services' reliance on the IT security of banks, insurers, and other financial entities, the frameworks set forth by these measures can serve as a guide for all organizations—no matter their industry–to gain clarity over dependencies and improve information sharing.

Operational Resilience pillars under FCA/PRA

- Identify Importance Business Services (IBS)
- Define impact tolerances
- Map IBS dependencies
- Scenario testing, validation, and remediation
- Identify vulnerabilities
- Document communication strategy

Operational Resilience pillars under DORA

- Risk management
- Incident reporting
- Digital Operational Resilience testing
- Scenario testing, validation, and remediation
- ICT third-party risk
- Information and intelligence sharing

The importance of an agile organization and flexible infrastructure

Since the first edition of this guide, business continuity management has taken a significant step forward. This has largely been driven by the need for organizations to navigate the pandemic, supply chain disruptions, workforce challenges, cyber-attacks, weather events, and other threats. In addition to the rising volume, frequency, and severity of incidents, business continuity professionals are increasingly required to manage multiple incidents at once, a phenomenon commonly referred to as polycrisis or compounding crises.

Given this, it is impossible to plan for every event or combination of events. Companies may have to confront disruptions that are impossible to foresee.

In this environment, companies should plan for the most likely scenarios and build a flexible infrastructure that allows them to respond to almost anything. This includes threat intelligence and early warning capabilities; continuously updated data personnel, customer, and financial data; timely and reliable communications across the organization and up the chain of command; and an agile approach to response.

everbridge
infiniteblue

BC in the Cloud

Award-winning, business continuity and disaster recovery management software, BC in the Cloud is trusted by organizations worldwide to anticipate, collaborate, communicate, rise above business disruptions, and achieve true enterprise resilience.

About Everbridge

Everbridge, Inc. empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today's unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry's most comprehensive risk data to Keep People Safe and Organizations Running™.

Visit Everbridge.com

Read our company blog

Follow us on LinkedIn

Follow us on Twitter

Get in touch to learn about Everbridge, empowering resilience.

everbridge