ALLIEDUNIVERSAL®

There for you.

Resilience Planning Guide

Best practices to help your organization prepare for the unthinkable

aus.com

Contents

Legal Disclaimer

The Resilience Planning Guide is based on Allied Universal's operating and industry knowledge and resources and is not based on knowledge of the reader's property, assets or operations, including risks associated therewith. This material is provided for general informational purposes only. Allied Universal® makes no warranties, express or implied, in connection with the information contained herein. Any recommendations in this Guide describe approaches that may mitigate risk in some settings, and are not intended to imply or provide assurance that risk will be mitigated or eliminated. No set of security measures can prevent all risks.

Allied Universal does not assume and specifically disclaims any responsibility or liability regarding or any security risks, hazards, dangers, or threats to your facility, assets, or stakeholders, and shall not be held responsible or liable for any loss, costs, or damages of any kind or nature whatsoever related to the use of this Guide or any information provided herein.

Purpose and Introduction

An unexpected incident can cause havoc for an organization and its people, so in a world where change is constant and uncertainty seems to linger, organizational resilience is a strategic imperative. Whether facing natural disasters, economic downturns, deliberate attacks, or unexpected global crises, the ability to adapt, recover and thrive has never been more critical. A well-documented, tested and socialized crisis plan can save organizations from lost revenue and even loss of life.

Welcome to the Allied Universal Resilience Planning Guide, where we provide recognized best practices to set you up for success in the face of crisis. This isn't just another manual to read once and discard—it's a document meant to foster communication within your organization and team to help you prepare to stand strong against whatever challenges come your way.

Resilience isn't built overnight, nor is it a one-size-fits-all solution. It's a dynamic process that requires foresight, planning, support and action. Whether you're a seasoned security leader, a community organizer or an individual seeking to navigate life's uncertainties with grace, this playbook offers something for everyone.

Throughout this guide we'll delve into the principles of resilience and equip you with tips and best practices to create a culture that values preparedness at all levels. We have based our conversation and tips around our risk-based approach to security, which asks three vital questions as outlined in the graphic to the right.

So, if you're ready to embark on a journey of discovery, resilience and transformation, turn the page and let's begin. Together, we'll unlock the secrets of resilience and forge a future where no challenge is too great to overcome.

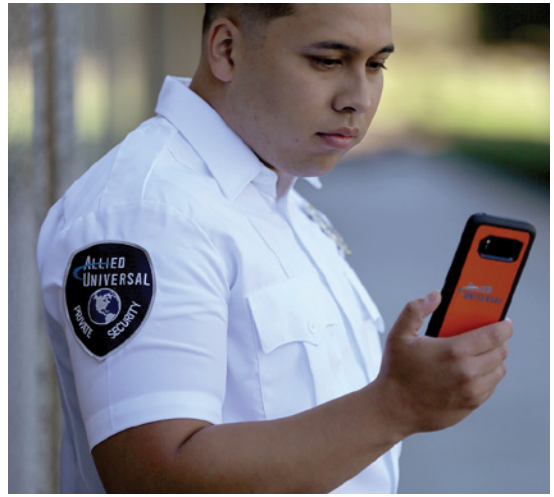
The time for resilience is now. Let's rise to the occasion together.

The Case for Resilience

Investing in people, process and technology to bolster resilience is a prudent decision to safeguard against potential disruptions and a strategic move that can yield significant financial returns. We dug into the research and found some key statistics and data points that underscore the value of building proactive resilience plans within your organization:

> According to the National Institute of Building Sciences, for every $1 spent on hazard mitigation, businesses can expect savings of $6 in future disaster recovery costs. This statistic highlights the cost-effectiveness of proactive resilience measures.
>
> (source: https://www.nibs.org/projects/natural-hazard-mitigation-saves-2019-report)

> Boston Consulting Group (BCG) notes that companies with robust resilience strategies can reduce costs associated with disruptions by up to 55% due to the introduction of efficient operational risk management and recovery processes.



Research indicates that companies that recover quickly from a disruption see less than half the shareholder value destruction compared to those with slower recovery times. Specifically, firms that recover quickly experience a 10% drop in shareholder value in the year following a disruption, compared to a 25% drop for those recovering more slowly.

(Source: https://web-assets.bcg.com/c1/4e/c27232db4084a30e64d42068f122/bcg-becoming-an-all-weather-company-sep-2020.pdf)

Cybercrime Magazine reported that the global cost of cybercrime is expected to grow by 15% per year, reaching $10.5 trillion annually by 2025. Investing in cyber resilience not only mitigates these costs but also protects against the reputational damage associated with data breaches.

(Source: https://cybersecurityventures.com/cybersecurity-almanac-2023/)

Research by McKinsey found that companies that actively invest in resilience can reduce disruption costs significantly, highlighting the importance of resilience in maintaining smooth operational flows and meeting customer demands.

World Security Report

As part of our ongoing security conversation, Allied Universal asked 1,775 chief security officers (CSOs) from large, global companies what threats and security mitigation strategies they are focused on.

The results were published in our first-ever *World Security Report*. The biggest takeaway? The world is an increasingly dangerous place, and companies face complex, multi-dimensional hazards and threats.

Planning for resilience requires us to contemplate the world and our organization's place in it with an eye toward what is happening now and what could happen in the future. Our *World Security Report* highlights several concerns that continue to create challenges for organizational security teams and can act as a roadmap to some of the "what if" scenarios you should consider.

Economic Unrest and Social Stability

In North America, 49% of CSOs say that economic unrest will be the biggest security-impacting hazard in 2024. This unrest is often exacerbated by domestic and international events that lead to increased risks of civil disturbances and social unrest.

Cyber-Physical Security Integration

The report underscores the growing interconnection between cyber and physical security. With 90% of CSOs saying that cyber threats pose challenges to their physical security systems, it's crucial for organizations to adopt integrated security solutions. This involves enhancing cybersecurity measures and ensuring physical security systems are resilient to cyber-attacks.

Internal Threats and Insider Risk Management

89% of organizations have experienced internal threats, including the misuse of company resources and data leaks. Given the potential for insider threats to escalate during politically and financially charged times, organizations should consider implementing stringent insider risk management protocols.

Preparedness and Response

The *World Security Report* highlights the importance of preparedness and response – a key factor for any turbulent time. Organizations with high involvement from third-party security providers reported fewer incidents and higher confidence in handling security issues. This suggests that leveraging external expertise is critical to an effective security strategy.

Download a full copy of Allied Universal's *World Security Report* aus.com/world-security-report and see what else chief security officers are saying.

Download now

Part One: What do You Need to Protect?

In any organization, the foundation of effective emergency planning begins with a clear understanding of what you're trying to protect.

This involves identifying the critical assets and functions that are essential to the organization's operations and success. These include people, physical assets like buildings and equipment, digital assets such as data and IT systems, and intangible assets like reputation and intellectual property. Recognizing these priorities allows for the development of targeted strategies to safeguard them in the event of an emergency.

An organization's resilience planning isn't a one-time effort. As the business environment evolves, new threats emerge and the use and value of certain assets can change, and new types of assets and functions might be introduced. As such, it is crucial for teams to regularly review and update their plans based on changing priorities and risk factors. Continuous monitoring and reassessment ensure that emergency plans remain relevant and effective. Engaging stakeholders from various departments in this process helps capture a broad perspective, ensuring that all potential impacts are considered and that the plan reflects those threats in a way that makes sense for the business.

By staying proactive and adaptive, organizations can enhance their resilience and better protect their vital interests against unforeseen emergencies. For these efforts to succeed, you'll need to get buy-in at the highest level to create a culture of preparedness within your organization. Operational assets are critical to the ongoing mission of the organization, and that is a key responsibility for executives. If you don't have an executive sponsor who recognizes the importance of resilience to the business, you are setting yourself up to have a document that sits on a shelf and gathers dust.

Furthermore, it is critical that your planning considers the operational impact of crisis.

Look at the types of events that could impact your different types of assets and start prioritizing from the most vulnerable and impactful to the least. Consider natural disasters such as earthquakes or floods and human-made emergencies such as active shooter and power outages. Then, take a look at the potential impact on your operations, employees and stakeholders.

The next two sections dive into what to consider in your resilience plan and how to get started.

Part Two: What Does it Need Protection From?

Now that you have alignment and understanding on what you are trying to protect, we will focus on the question, “What does it need protection from?”

Risk factors are the various threats and vulnerabilities that could potentially impact the organization's assets. These threats can range from natural disasters like hurricanes and earthquakes to human-made incidents such as cyber-attacks, terrorism or even internal threats like employee misconduct. By conducting a comprehensive risk assessment, organizations can identify which threats are most likely to occur and which assets are most at risk, enabling them to allocate resources and develop plans that mitigate these risks effectively.

In this section we will look at:

Categories of Risk

Typically, events fall into one of two categories - events with warning and events without warning. Protecting from the latter requires advanced planning and agility to respond in the moment.

Probable vs. Potential Threats

With competing priorities and budgets, you may need to prioritize your planning for probable rather than possible threats. Often, creating mitigation strategies for the probable will also create a template of action for the more far-reaching threats. When you understand how to respond in the face of a crisis, the crisis itself is often secondary.

Events With Warning

Events with warning are those where there's typically a lead time due to intelligence, policy, weather forecasts and geological monitoring. These risks are known to an organization and should give you time to put mitigation strategies into play. The true benefit to an event with warning is that it allows time to prepare stakeholders and possibly practice your response, leading to a greater feeling of preparedness while reducing anxiety.

The following is a list of common events that would traditionally come with advance warning. We have supplied a few considerations and strategies. However, it is important to note that these are not exhaustive lists, just a few thought starters.

Natural Disasters

Natural disasters such as hurricanes, floods and earthquakes typically come with some degree of warning, allowing organizations time to enact pre-planned responses. Weather forecasts and geological monitoring provide critical data to predict when and where these events might occur.

Considerations

- Continuous monitoring of weather and geological reports.
- Maintaining updated and easily accessible emergency response plans.
- Training employees on evacuation procedures and emergency roles.

Strategies

- Implementing robust communication channels to inform all stakeholders of impending threats.
- Preparing physical barriers and other mitigation tools to protect facilities and critical infrastructure.
- Securing supplies and backup power sources to ensure continuity during disruptions.

Planned Large-scale Public Events

Events such as major sporting events, concerts or political rallies can turn into crises if crowd control, infrastructure and security are not adequately managed. These events are typically known in advance, giving organizations time to prepare. The closer you are to the site, the greater the likelihood of risk.

Considerations

- Assessing the expected crowd size and demographic to tailor security measures.
- Coordinating with local law enforcement and emergency services.
- Reviewing and reinforcing contingency plans specific to scenarios of unrest or emergency.

Strategies

- Establishing clear perimeter security and access controls.
- Deploying sufficient security personnel to monitor and manage the crowd.
- Implementing emergency communication systems to address the public and coordinate with staff.

Industrial Actions

Strikes or planned protests represent a type of industrial action that can disrupt operations and pose security risks, particularly if they lead to picketing or sit-ins at business facilities.

Considerations

- Understanding the grievances leading to industrial actions to better manage negotiations.
- Planning for potential disruptions to supply chains and daily operations.
- Ensuring safety measures are in place to protect non-participating employees and assets.

Strategies

- Engaging in preemptive dialogue with union representatives and workers to address issues before they escalate.
- Preparing for alternative operational arrangements, such as remote work or temporary relocation of critical functions.
- Maintaining neutrality and ensuring all communication is respectful and constructive to minimize animosity.

Public Health Warnings

Epidemic outbreaks, such as influenza or the more recent global occurrence of COVID-19, often come with health advisories and warnings, allowing organizations to implement safety protocols ahead of time.

Considerations

- Monitoring health advisories from local and international health organizations.
- Understanding the potential impact on employee health and business operations.
- Implementing policies for hygiene, remote work and social distancing.

Strategies

- Stockpiling necessary health and safety supplies like masks, sanitizers and disinfectants.
- Developing and testing business continuity plans that include scenarios for significant absenteeism.
- Offering training and resources to employees on disease prevention and maintaining hygiene in the workplace.

Each of the scenarios outlined in the preceding pages represent a real threat to organizational resilience and require a tailored and nuanced response. By addressing these considerations and implementing these outlined strategies, along with others as required, organizations can enhance their resilience against events with warnings and mitigate potential impacts effectively.

Events Without Warning

Terrorist Attacks

Terrorist attacks are deliberate, violent acts that can occur with little to no warning. They aim to create fear, cause harm and disrupt operations. The unpredictable nature of these attacks requires a high level of preparedness and resilience.

Considerations

- Identifying potential targets within the organization's assets and personnel.
- Understanding the general threat level in the area or industry.
- Regularly updating and practicing an incident response plan.

Strategies

- Establishing robust surveillance and security measures, including access controls and monitoring systems.
- Training staff on recognition of suspicious behavior and proper reporting protocols.
- Developing quick-response teams that are well equipped and trained to handle emergencies.

Sudden Industrial Accidents or Failures

These can include machinery failures, chemical spills, or power outages that occur without any preceding signs. These incidents can pose immediate risks to safety and disrupt operations.

Considerations

- Regular maintenance and inspection of equipment to reduce the risk of failures.
- Training employees on emergency procedures related to industrial accidents.
- Evaluating the sufficiency of safety measures in place to handle unexpected incidents.

Strategies

- Implementing emergency shut-off systems and other safety controls to minimize damage.
- Keeping spill containment kits and first aid readily available.
- Designing redundancy into critical systems to ensure continuity of operations during power outages.

These are typically sudden and leave little to no time for specific preparation. These events can often cause chaos and panic. The successful navigation of these events comes down to the work done to prepare for the "what if" in advance. Sharing the preparedness plan, ensuring a thorough review, running tabletop exercises and infusing preparedness into your culture will help your team know what to do in times of crisis – with or without warning.

Earthquakes or Tsunamis

Seismic events like earthquakes and tsunamis come with very little warning and can cause harm to people and property, leading to devasting business disruption and sometimes loss of life. While you can't prevent the damaging impact of a natural disaster of this magnitude, you can prepare your facility and people to react in ways that will make recovery easier.

Considerations

- Assessing the seismic risk based on geographical location.
- Ensuring that buildings and facilities comply with earthquake-resistant construction standards.
- Preparing evacuation plans and emergency kits that are easily accessible.

Strategies

- Conducting regular drills to ensure everyone knows how to act during and after seismic events.
- Securing heavy furniture and equipment to prevent movement and potential injuries.
- Establishing communication plans that can operate without standard telecommunication lines, which may be disrupted.

Sudden Acts of Violence in the Workplace

Workplace violence can stem from internal conflicts or external threats and can occur without warning, significantly affecting employee safety and morale.

Considerations

- Create a zero-tolerance policy toward violence within the organization.
- Encourage a culture where employees feel safe to report grievances and suspicious activities.
- Regularly assess employee morale and mental health.

Strategies

- Offer training on conflict resolution and stress management to all employees.
- Implement strict access controls and visitor management systems to monitor and control who enters the premises.
- Empower a crisis management team specifically trained to respond to violent incidents, providing immediate support and intervention.

Internal Theft – Property or Intelligence

If you are a company with valuable physical or intellectual assets, you are at risk for employee theft.

Considerations

- Create strong access control parameters.
- Conduct regular system testing.
- Prepare for back-up security when and if technology fails (i.e. power outage).
- Encourage a culture where employees feel safe to report grievances and suspicious activities.

Strategies

- Implement strict access controls and visitor management systems to monitor and control who enters the premises.
- Avoid crime of circumstance – create a culture that is diligent about security.

Conclusion

For sudden events, it's essential to have a proactive, well-thought-out emergency response plan that includes training, technology and tools designed to reduce risks and manage the situation effectively. While these events are challenging to predict, thorough preparation can significantly mitigate their impact.

Recognizing a Probable Threat

As part of the strategic planning process, develop a comprehensive guide or checklist to help identify, assess, and escalate potential threats or crisis situations. Ensure they are categorized accurately into "probable" versus "possible" scenarios. Implementing this systematic approach, ensures a proactive approach to addressing risks, enhancing overall preparedness and resilience.

Such a checklist ensures that early signs of disruption are identified and categorized, and those deemed a "true risk" are prioritized, minimizing the possible negative impact on business operations.

Implementing this proactive measure enhances organizational resilience, ensures a coordinated response, and helps safeguard the company's physical and intellectual assets, reputation and stakeholders.

Probable vs Possible

Understanding the distinction between probable and possible risk is crucial in effective risk management and emergency preparedness.

Probable risk refers to threats that have a high likelihood of occurring based on historical data, trends and current conditions. These risks are often foreseeable and can be planned for with specific, targeted measures. For example, a city located on the coast might consider hurricanes a probable risk due to its geographical location and past experiences.

On the other hand, possible risk encompasses a broader range of potential threats that, while they might not be highly likely, still represent a possible danger. These risks are less predictable and often require flexible planning and response strategies. An example might be a terrorist attack in a rural area, which, while less likely, remains within the realm of possibility.

By distinguishing between probable and possible risks, organizations can prioritize resources and develop more nuanced emergency preparedness plans that address both the most likely threats and a wider array of potential hazards.

Checklist: Recognizing a Threat or Crisis Situation

This checklist provides key indicators to recognize potential threats or crises that require escalation:

Unusual Activity Detection ☑

- Have there been any unusual activities or anomalies in IT systems, such as unauthorized access attempts or data breaches?
- Are there unexpected fluctuations in financial transactions or discrepancies in accounting records?
- Have there been any reports of suspicious behavior or activities on the premises?

Identified External Activity ☑

- Are there any external activities that could impact your business (i.e. protest, strike, parade)?
- Are there any weather activities suspected to impact your area?

Operational Disruptions ☑

- Are there any significant disruptions to core business operations, such as supply chain interruptions, facility damage or key personnel absences?
- Have there been unexpected outages of critical infrastructure (e.g., power, water, telecommunications)?
- Is there a sudden increase in customer complaints or product/service delivery issues?

Reputational Risks ☑

- Is there negative media coverage or social media activity that could harm the organization's reputation?
- Have there been any incidents involving legal or regulatory non-compliance?
- Are there whistleblower reports or internal complaints indicating potential misconduct or unethical behavior?

Health and Safety Concerns ☑

- Are there reports of widespread illness or a health epidemic among employees or in the community?
- Have there been workplace accidents or incidents resulting in serious injury or fatalities?
- Are there hazardous material spills or environmental contamination events?

Stakeholder Feedback ☑

- Have customers, partners or suppliers expressed concerns about potential risks or issues?
- Is there feedback from employees indicating stress, fear or confusion regarding specific incidents?
- Are there warnings or advisories from industry bodies, government agencies or regulatory authorities?

25 Questions to Ask When Identifying Potential Threats

Asking the right questions and taking a critical look at your company and the environment in which you operate is crucial. Here are 25 targeted questions to help you recognize and evaluate potential risks:

General High-Level Questions

1. Is our organization part of a high-risk industry for workplace violence or accidents?
2. What key landmarks or high-profile sites may be near our company? (Think tourist attractions, government buildings and transportation hubs)
3. Are there frequent large public gatherings near our location? (Concerts, protests, sports events)
4. What is the crime rate in our area? Is the vicinity known for higher incidents of crime?
5. Are we located in a region prone to natural disasters such as floods, earthquakes, hurricanes or tornados?
6. What are the economic trends of the region where we operate?
7. What is the risk of internal threat to our business?

External Partnerships and Factors

8. How reliant are we on external partners and service providers, and what risks do they pose to our business continuity?
9. What are the vulnerabilities in our supply chain that could disrupt our operations?
10. Do we have alternate suppliers for critical goods and services?
11. How reliant are we on specific utilities (water, power, internet)?
12. How will we handle communication with external emergency services (i.e. fire, police, medical)?
13. Do we have a communications strategy to share critical information with clients and external partners?

Internally Focused Questions

14. Do our operations depend heavily on digital infrastructure? (Vulnerability to cyber-attacks)
15. Do we store or handle hazardous materials?
16. What level of access control do I currently have? (Physical and digital)
17. How robust are my current emergency and evacuation procedures?
18. Are we compliant with all relevant health and safety regulations?
19. Do we have an emergency communication tree in place?
20. Do we have visitors to account for in our emergency preparedness planning?

Externally Focused Questions

21. Are there any construction projects nearby that might increase risk (i.e. excavation, demolition)?
22. How good is the local infrastructure in supporting emergency response? (Roads, hospitals, emergency services)
23. How well trained is staff in emergency preparedness and response?
24. What backup systems are in place for critical operations?
25. What is the impact and possibility of media exposure?

Vertical-Specific Questions

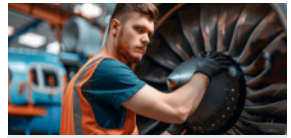
We know that you may require industry-specific questions. We've created this set of bonus questions. Please note that this list is not exhaustive. If your industry is not represented and you would like more information, we invite you to call your local Allied Universal representative, who can help you get started. We have expertise across many industries and can work with you to ensure you ask the right questions for your threats.

Chemical / Petrochemical

Commercial Real Estate

Condominium and High-rise

Construction



Defence and Aerospace

Aviation

Maritime and Ports

Healthcare

High Tech and Telecom

Hotel and Hospitality

Distribution and Logistics

K-12 Education

Higher Education

Financial Institutions

Government Institutions

Manufacturing and Industrial

Residential

Retail

Transit

Utilities

Data Centres

Healthcare

- Does the facility rely on a single source for critical supplies such as pharmaceuticals, which could be disrupted?
- Is the healthcare provider part of a network in a region with high digital infrastructure risks (i.e. frequent outages, cyber threats)?
- Are significant demographic shifts occurring in the area (aging population, influx of non-native speakers) that could impact service demands?
- Is the facility dependent on technology that could become obsolete or unsupported shortly?
- Is there a risk of reduced funding or changes in healthcare policy that could significantly affect operations?

Manufacturing

- Is the manufacturing sector experiencing a workforce shortage or skill gap that could impact production?
- Are there local or regional regulations that could impose new compliance costs or operational restrictions?
- Is the sector vulnerable to global economic fluctuations affecting the demand for manufactured goods?
- Does the location expose the company to fluctuations in energy costs or availability that could affect production costs?
- Is there a risk of intellectual property theft or technological espionage that could undermine competitive advantages?

Education

- Is the institution subject to fluctuations in enrollment or funding due to local economic conditions?
- Are there changes in educational policy or accreditation standards that could affect operational viability?
- Is the campus's technological infrastructure adequate for modern educational demands, such as online learning platforms?
- Does the institution face challenges related to diversity and inclusion that could affect its reputation and operational stability?
- Is there a potential for significant staff turnover that could impact educational quality or continuity?

Finance

- Is the financial institution exposed to significant fluctuations in the real estate market, affecting its mortgage portfolio?
- Are there impending regulatory changes that could alter operational practices or require substantial compliance investments?
- Does the institution's technological infrastructure adequately protect against increasingly sophisticated cyber threats?
- Is there a high reliance on automated processes that software failures or malfunctions could disrupt?
- Are geopolitical tensions affecting currency stability or international transactions?

Retail

- Is the retail environment susceptible to shifts in consumer behavior, such as a move toward online shopping?
- Does the retailer face significant competition from e-commerce platforms that could erode market share?
- Are there local economic factors that could affect consumer spending power and retail sales?
- Is the retailer dependent on seasonal sales that could be impacted by external factors such as weather or economic downturns?
- Are there risks associated with data breaches or other cyber threats due to high volumes of personal customer data being processed?

Worksheet: Assessing Organizational Risk

Please use the following worksheet to identify your unique risk landscape.

Possible Hazards and Emergencies	Risk Level (None, Low, Moderate or High)	Mitigation Strategies
Internal Threats		
IT System Failure		
Breach of Information		
Active Shooter		
Strike and Unrest		

Source: FEMA: https://www.fema.gov/pdf/areyouready/basic_preparedness.pdf

Possible Hazards and Emergencies	Risk Level (None, Low, Moderate or High)	Mitigation Strategies
External Threats		
Floods		
Hurricanes and Tornadoes		
Earthquakes		
Power Outages		
Winter Storms		
Fire and Wildfire		
Hazardous Materials Incident		
Explosions		
Chemical Threats		
Active Shooter		
Civil Unrest		
Health Pandemic		

Part Three: How do You Most Effectively Protect it?

When planning for the "What If," where do you start? There are seemingly infinite possibilities of threats to your business, and you can't possibly prepare for them all. Can you? The answer is simple… you don't need to exhaust the possibilities, but you need to start somewhere.

You have set the stage for creating and implementing a successful emergency preparedness strategy within your organization. It's time to move from planning to the development and implementation stages. Here are the four things to consider:

Detailed Response Plan

Your emergency planning team is responsible for creating a detailed response plan tailored to your organization's unique risks and vulnerabilities. This is where you dive into the details, including:

- Defining roles and responsibilities for key personnel.
- Outlining communication procedures.
- Establishing evacuation routes.
- Determining protocols for continuity of operations during emergencies.

Emergency Preparedness Team

Create a team responsible for developing, socializing, testing and implementing your emergency preparedness plan. This team should include representatives from different departments or functions to ensure comprehensive coverage and diverse perspectives.

Communication and Coordination

Establish clear internal and external communication channels for disseminating information during emergencies. Develop protocols for coordinating with emergency responders, local authorities and relevant stakeholders. Ensure all employees know how to access emergency information and who to contact.

Operationalizing the Plan

A plan is just paper until socialized, practiced and adopted. Provide training and education to employees to ensure they understand their roles and responsibilities in emergencies. Conduct drills and exercises regularly to test the effectiveness of the emergency response plan and familiarize staff with emergency procedures.

Detailed Response Plan

Emergency planning encompasses five critical areas: prevention, protection, response, recovery and mitigation. A well-crafted plan must be comprehensive enough to equip all stakeholders with the knowledge and actions required to handle any threat or hazard effectively. At the same time, it should be clear and straightforward, avoiding excessive complexity that might discourage engagement or understanding. Striking the right balance ensures the plan is actionable and accessible, empowering everyone involved to respond swiftly and effectively in an emergency.

Your preparedness plan could include some or all of the following elements:

Introduction 1

- Purpose of the Plan
- Scope
- Objectives
- Plan Development and Maintenance

Emergency Preparedness Policy 2

- Statement of Commitment
- Roles and Responsibilities
- Legal and Regulatory Requirements

Risk Assessment and Hazard Analysis 3

- Identifying Potential Hazards
- Risk Assessment Methodology
- Hazard Analysis Summary

Emergency Response Procedures 4

- Incident Identification and Notification
- Evacuation Procedures
- Shelter-in-Place Procedures
- Lockdown Procedures
- Medical Emergencies
- Fire Emergencies
- Natural Disasters
  (i.e. earthquakes, floods, hurricanes)
- Technological Emergencies
  (i.e. power outages, IT failures)

Emergency Communication Plan 5

- Internal Communication
- External Communication
- Communication Tools and Channels
- Media Relations

Emergency Roles and Responsibilities 6

- Emergency Response Team
- Incident Commander
- Floor Wardens
- First Aid Responders
- Security Personnel
- Crisis Management Team

Emergency Supplies and Equipment 7

- Emergency Kits and Supplies
- First Aid Kits
- Emergency Equipment Maintenance

Training and Drills 8

- Training Programs
- Drill Schedule and Procedures
- Evaluation and Improvement

Business Continuity Plan 9

- Continuity of Operations
- Critical Functions and Resources
- IT and Data Recovery
- Alternate Work Locations

Evacuation Plan 10

- Evacuation Routes and Exits
- Accounting for All Employees

Shelter-in-Place Plan 11

- Designated Shelter Areas
- Procedures and Supplies

Lockdown Procedures 12

- Initiating a Lockdown
- Communication During Lockdown
- Lockdown Termination

Post-Incident Procedures 13

- Incident Reporting
- Debriefing and Review
- Psychological Support for Employees

Plan Maintenance and Review 14

- Plan Review Schedule
- Plan Updates and Revisions
- Document Control

Appendices 15

- Contact Information (Internal and External)
- Maps and Floor Plans
- Emergency Response Checklists

Testing and Challenging Assumptions of the Plan

Assumptions are the foundation of any business continuity and disaster plan, but they can also be its weakest link if not adequately scrutinized. Challenging the assumptions that underpin your plan is essential to ensure its robustness in the face of unexpected events. Identifying, questioning and testing these assumptions can uncover vulnerabilities and strengthen a plan's resilience.

Identify Key Assumptions

List the assumptions underpinning your plan. Question their validity and consider scenarios where these assumptions might fail. 1

Review Each Section

Go through each section of the plan and highlight statements or procedures that depend on certain conditions being true.

Questions to Ask Yourself and Stakeholders:

- What specific conditions must be true for this section of the plan to be effective?
- Are there any dependencies or interconnections with other sections of the plan?
- Which parts of this section rely on external factors, such as supply chains or third-party services?
- How would this section of the plan perform if those conditions change or fail?
- Are there any areas in this section that are overly complex or unclear?

Brainstorm Scenarios

Think about various scenarios that might disrupt these conditions. For example, if your plan assumes that key personnel will be available, consider what happens if they are not.

Questions to Ask Yourself and Stakeholders:

- What are the most likely scenarios that could disrupt key assumptions?
- Have we considered a wide range of scenarios, including both common and rare events?
- What are the potential impacts of each scenario on operations?
- How would our response change if a key assumption failed during a crisis?
- Are there any historical events or industry-specific risks that we have overlooked?

Identify Key Assumptions 1

Consult Stakeholders

Engage with team members and other stakeholders to uncover implicit assumptions they may have made while contributing to the plan.

Questions to Ask Yourself and Stakeholders:

- What are the most likely scenarios that could disrupt our key assumptions?
- Have we considered a wide range of scenarios, including both common and rare events?
- What are the potential impacts of each scenario on our operations?
- How would our response change if a key assumption failed during a crisis?
- Are there any historical events or industry-specific risks we have overlooked?

Test Your Assumptions 2

Conduct Scenario Analysis

Develop alternative scenarios to test your plan's resilience. Consider events like prolonged power outages, cyber-attacks or natural disasters that were not initially considered.

- What alternative scenarios could challenge the fundamental assumptions of the plan?
- Have we considered both common and rare events in our scenario analysis?
- What would the impact be on our operations if these scenarios occurred?
- How would our response differ in each scenario?
- Are there any scenarios that we overlooked or not fully explored?

Compare Against Data 3

Use historical data and industry reports to validate assumptions. This helps determine if they are realistic based on past occurrences.

- What historical events can provide insights into the validity of our assumptions?
- Are there industry reports or case studies that highlight similar situations we might face?
- How do our assumptions compare with historical data and industry benchmarks?
- Have we identified any trends or patterns that could inform our planning?
- What adjustments can we make based on the data gathered?

By systematically testing your assumptions through these methods, you can ensure that your business continuity and disaster plan is robust, comprehensive and capable of handling a wide range of potential disruptions.

Emergency Preparedness Team

Emergency management and communications should be handled by an Emergency Preparedness Team (EPT), which is comprised of key stakeholders throughout the organization who can provide input into how to mitigate business disruption and recover in the face of disruption. Let's face it, sometimes our best planning isn't enough to stop an emergency, but it can dictate how we respond and recover.

The role of the EPT is threefold:

1. Foster a culture of preparedness within the organization
2. Create, test and train on mitigation strategies to protect against the "probable" risks
3. Manage the response to and recovery from any disaster or crisis that impacts the business

Start by completing the grid below to identify key members of your EPT. Remember, signing up isn't enough. Your EPT should be engaged and active in the workplace. They are the ambassadors who help create a security-conscious culture.

Worksheet: Emergency Preparedness Team

Team Role	Name	Work and alternate email	Work and alternate phone
Lead			
Crisis support			
Operations			
Human Resources			
Security			
Health and Safety			
Legal			
IT			
Communications			
Disaster Recovery Manager			

Effective Communication

Effective communication is a cornerstone of emergency preparedness plans. In times of crisis, clear, timely and accurate information can make the difference between safety and disaster. Well-established communication protocols ensure that all stakeholders—employees, emergency responders, and the public—receive crucial updates and instructions. This facilitates coordinated responses, reduces confusion and helps manage the spread of misinformation. Moreover, robust communication strategies enhance preparedness by informing everyone about roles, responsibilities and procedures before an emergency occurs, fostering a culture of readiness and resilience.

The EPT should consider the information channels their employees and stakeholders use:

- Main web page
- Online and Intranet message boards
- Social media (such as Facebook, Instagram and LinkedIn)
- Text updates
- Phone calls
- Email
- Banners and billboards

Emergency communications should incorporate a strategic mix of information channels to make communications as accessible and widely transmitted as possible. Other considerations are the location of your employees and stakeholders. Are they hybrid? Do they work across multiple campuses? Do you need to communicate across borders?

Questions to ask:

- Do we have a chain of command for approving strategy and action?
- Are we using a variety of channels to communicate the plan?
- Do we know how to reach all employees and stakeholders?
- Do employees and stakeholders update their contact information regularly?
- Is our messaging clear and easily understood by all employees?
- Are employees encouraged and able to provide feedback effectively?

Socializing the Plan

Ensuring that your business continuity and disaster plan is understood and ingrained in your organization's culture is crucial for its success. An emergency plan that is not shared is just a hope. This section provides best practices for socializing the plan, creating awareness and fostering a culture of preparedness.

A well-socialized plan means that employees and appropriate stakeholders understand the plan, have trained and practiced against the plan and have an open line of communication. Asking these simple yes / no questions will ensure that your rollout has been successful:

Do you know where to find the business continuity and disaster plan?	Yes / No	Are you receiving regular updates about the plan?	Yes / No
Are you aware of the critical components of the plan?	Yes / No	Do you know how to provide feedback or ask questions about the plan?	Yes / No
Do you understand your role in the plan?	Yes / No	Are you aware of the communication channels used for emergency information?	Yes / No
Have you participated in recent training sessions?	Yes / No	Do you feel prepared and confident in your ability to respond to an emergency?	Yes / No
Are you familiar with the emergency procedures through practical drills?	Yes / No	Are you aware of the support systems available during and after an emergency?	Yes / No
Do you know who to contact in case of an emergency?	Yes / No	Do you know the safety protocols and how to execute them?	Yes / No

Socializing the Plan: Best Practices and Tips

Effective socialization of a plan involves clear communication, continuous training, and active engagement with all employees. It's about making the plan a living document that is integral to daily operations.

Top-Down Communication

Ensure leadership communicates the importance of the plan and leads by example.

Interactive Workshops

Conduct interactive workshops to engage employees and address their concerns.

Regular Updates

Keep the plan visible through regular communications.

Questions to Ask Yourself and Stakeholders:

- How effectively is leadership communicating the importance of the plan?
- Are employees actively engaged in workshops and training sessions?
- How frequently are employees updated on changes to the plan?

Training Strategies

Training on an emergency preparedness plan is crucial for ensuring the safety and well-being of everyone in your organization. Training fosters a culture of safety and preparedness within the organization. Regular drills and simulations reinforce procedures, allowing staff to practice and internalize their responses. This hands-on approach ensures that employees can execute the plan under pressure and helps identify gaps or weaknesses, making it more robust.

In emergencies, such as natural disasters, fires, or other security threats, you want a team that can respond swiftly and effectively, minimizing harm and disruption. When employees are familiar with the organizational emergency procedures, they can act confidently and cohesively, reducing panic and confusion. Creating a high level of readiness protects lives, safeguards property and maintains business continuity.

Effective Training: Best Practices and Tips

Continuous training ensures that employees are prepared to implement the plan effectively.

- Schedule regular training sessions to keep skills fresh.
- Incorporate practical drills that simulate real-life scenarios.
- Establish a feedback loop to improve training based on employee input.

Questions to Ask Yourself and Stakeholders:

- Are our training sessions comprehensive and engaging?
- How often are we conducting practical drills?
- Are we gathering and incorporating feedback from training sessions?

Continuous Review and Testing

A plan with gaps has a higher chance of failing at a key moment in a crisis—like a lifeboat without paddles. Testing the plan helps find and close potential gaps. An emergency readiness plan needs to be tested and updated regularly—we recommend annually at a minimum.

How do you go about reviewing and updating your plan? Start with the team that created the initial plan and review the initial testing process. This helps to quickly identify and share any organizational changes that could negatively or positively impact the plan. Next, share with your frontline team that understands the workplace best and can provide valuable insights. Lastly, make the necessary updates, such as revising your call chain or updating the evacuation routes, to name a few. Remember, you don't need to wait until the annual review to make changes. Any significant changes should be captured immediately.

Updating the Plan: Best Practices and Tips

Utilizing a variety of training exercises and communication tools ensures a broad reach and increased understanding.

Continuous training ensures employees are prepared to implement the plan effectively.

- Conduct frequent emergency drills and simulations to familiarize employees with the crisis plan.
- Ensure the emergency preparedness plan is accessible to all employees.
- Tailor training sessions to address different employees' specific roles and responsibilities during a crisis. Provide detailed instructions and guidance for each role and offer additional training for team leaders and key personnel.

Questions to Ask:

- Do we have a set schedule for updating the emergency plan?
- When was the last time we updated the emergency plan?
- Do we have new employees who may have something unique to bring to the emergency plan?

Conclusion

Thank you for reviewing our resilience planning guide. We hope it proved useful in improving your emergency preparedness.

A comprehensive and well-practiced emergency preparedness plan is vital for the safety and resilience of an organization. By prioritizing regular training, clear communication and role-specific preparation, companies can ensure their employees are ready to respond effectively in any crisis – saving lives and protecting against business disruption.
A robust emergency plan beyond protecting the business, reinforces a culture of safety and preparedness, providing stakeholders with the peace of mind that their security is a priority.
Investing in preparedness today is the key to navigating tomorrow's uncertainties with confidence and competence.

In addition to collaborating with Allied Universal, for more information and training on creating a comprehensive preparedness plan, consider reaching out to these experienced organizations:

- Federal Emergency Management Agency (FEMA)
- Ready.gov
- Centers for Disease Control and Prevention (CDC)
- Occupational Safety and Health Administration (OSHA)
- American Red Cross
- National Fire Protection Association (NFPA)
- World Health Organization (WHO)

Contact our sales team at: www.aus.com/contact-us

ALLIED UNIVERSAL®
There for you.

Resilience Planning Guide

Thank you for taking time to read our eBook. If you'd like to delve deeper into the topics covered, explore our website - aus.com - for additional resources, tools and insights.

There's security in our solutions®