BUSINESS CONTINUITY &
EMERGENCY RESPONSE PLANNING

Disaster Readiness Checklist

SHADOWHQ

The definiton of ‘disaster’ is changing

A multitude of scenarios represent disasters that create IT and business disruption. But did you know that only 5% of disruptions are caused by natural disasters like wind, fires or floods?

Most are the result of human error, IT related issues like hardware of software failures, and of course, cyber-attacks. The Cost of a Data Breach Report 2023 revealed that 83% of surveyed organizations had experienced more than one data breach in 2022, making it far more likely that your business will face IT and security-related disruptions.

Traditional business continuity and emergency response planning tends to focus on natural disaster scenarios, leaving many teams unprepared — and uncoordinated — when an IT or cybersecurity event strikes.

Have confidence in disaster recovery and resiliency planning

When an emergency happens, every minute counts. Achieving business and IT resilience takes coordinated cross-team collaboration, real-time communication, and effective response. While incident response, crisis management and business continuity plans serve different purposes at different points in time, they should be integrated and complementary. Here's why:

Seamless Transition

An incident that begins as a hardware or software failure, or cybersecurity breach, for example, can escalate into a broader crisis, especially if critical systems and customer services are thrown offline. Effective coordination between incident response and business continuity ensures a seamless transition from addressing the immediate threat to maintaining essential business functions.

Holistic Resilience

Integration allows for a more holistic approach to IT and business resilience. Organizations can consider not only the technical aspects of incident response but also the business impact and how to sustain operations during disruptions.

Resource Management

Resources, both human and technological, can be shared between response efforts more efficiently and effectively when plans are integrated.

Consistent Communication

Integrated plans ensure consistent communication with stakeholders (both internally and externally) during a crisis, which is critical for managing the event effectively.

Faster Path to Recovery

Ensuring cross-function teams are aligned throughout the event helps to mitigate impact, get systems back online sooner and quickly return to business as normal, limiting your business's overall financial and reputational risk.

Digitization and rising cyber risk are transforming traditional response planning processes and what disaster readiness looks like. Incident response, disaster recovery, crisis management and business continuity are all essential components of your business's risk management strategy; cohesion is key to rapid event response and disaster recovery.

How to use this checklist

This checklist offers best practices that you can apply across business and IT functions to prepare, activate, execute and audit disaster readiness in a more holistic and cohesive way. By addressing each item on the checklist, you and your team will be better prepared to manage and mitigate risks, safeguard critical business functions, and maintain operational resilience in the face of any crisis.

Use the interactive checklist to keep track of your intiatives, and highlight any gaps.

Step 1: Prepare

Incident response, business continuity, emergency and crisis management plans are all critically important for crisis resolution and the overall resilience of an organization. They play distinct but interconnected roles in ensuring that an organization can effectively manage and recover from crises, incidents, and disasters.

- [ ] Identify critical business functions and their dependencies.
- [ ] Identify different scenarios that are unique to your business and could cause business interruption, service outages, emergency or disaster response, and financial and reputational risk. This list could include things like human error (accidental service interruption), natural disasters, power outages, lockdowns, hardware or software failure, and perhaps most likely, a data breach. Appoint key stakeholders according to the nature of the event.
- [ ] Appoint your organization's response coordinator. This individual will be responsible for activating response team members, facilitating communications, providing regular communications and guiding post-audit activities.
- [ ] Establish a clear communication and escalation plan for each scenario.
- [ ] Identify notification and monitoring channels and processes.
- [ ] Define roles and responsibilities for disaster response team members, by event type.

Pro Tip:

The last thing you want to do in a crisis situation is search desks or shelves for dusty, outdated binders or lost USB keys. Digitize your process and planning documents like key contacts and store those documents in a single location that's accessible even if systems are offline.threat to maintaining essential business functions.

- [ ] Maintain documentation for disaster recovery and business continuity plans.
- [ ] Train general staff on disaster recovery best practices and procedures, educate employees on your organization's approach to disaster response and inform all employees of what their individual responsibilities are in the event of a disaster.
- [ ] Review and update disaster recovery and business continuity plans periodically, incorporating lessons learned from incidents and exercises.
- [ ] Develop a plan to manage public relations and communication with stakeholders during event response, including key message development and spokesperson assignment. Identify key contacts at external partners like a crisis management communications firm.
- [ ] Identify key audiences and appropriate communications channels. Also note who needs to vet and approve key messages before they're shared externally.
- [ ] Appoint key spokespeople. This is usually the CEO, a similar executive designate and/or individuals closely linked to key audiences. This may include a media spokesperson, customer spokesperson or partner spokesperson. Ensure these individuals are media trained and comfortable speaking with media.
- [ ] Maintain an up-to-date list of emergency contacts and resources across all business continuity, incident response, crisis communications and emergency response plans. Remember to note alternate contact information as any event can take business systems and communication channels offline.
- [ ] Outline procedures for preserving digital evidence, which may be crucial for legal and regulatory purposes, as well as for identifying the root cause of the event.
- [ ] Test your plan through regular drills, exercises and simulations like table tops to test and improve response capabilities and workflows.
- [ ] Establish, monitor and track key performance indicators (KPIs) and benchmarks related to event response and recovery.

Step 2: Activate

When an event happens, every minute counts. Activate your response plans and get all hands on deck quickly. The following steps are key to minimize damage, contain the event and restore normal operations as quickly as possible.

Identify, verify and log that an event has occurred, the nature of the event, its severity and its business impacts (e.g. services are offline, internal systems are down or inaccessible, whether the event is ongoing and needs further remediation).

- [ ] Immediately notify response team members and relevant stakeholders about the event. This typically includes the incident response team, senior management, legal, and communication/public relations teams.
- [ ] Assign response tasks, including tasks designated to partners.
- [ ] Prepare and communicate key messaging to response team members.
- [ ] Maintain detailed records of all actions taken during the incident response process. This documentation will be essential for post-event analysis, compliance, and reporting purposes.

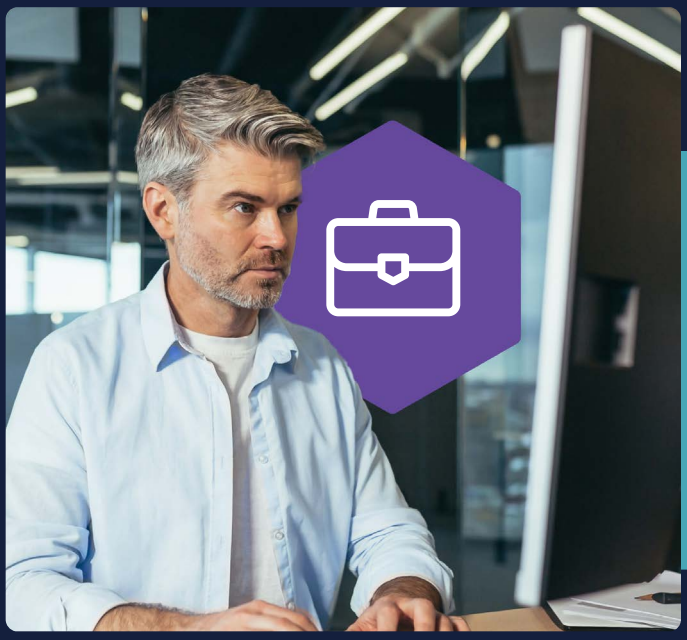
Pro Tip:

Identify alternate and secure voice and video channels in your response plans so you're not scrambling to connect team members when your file sharing and collaboration systems are off offline.

Step 3: Execute

When executing your response plan, alignment across IT, security, and business teams is critical to mitigate the impact and facilitate a swift recovery.

- [ ] Contain the event as fast as possible. For example, if the event in question is a cyber incident, the immediate goal is to prevent further damage and limit the incident's scope. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious network traffic.
- [ ] Disseminate prepared messaging to appropriate external channels and audiences as documented in your business's crisis and emergency response plans.
- [ ] Log all communications through event containment and remediation.
- [ ] Ensure the primary response coordinator provides frequent updates to all responding team members, as well as key stakeholders (as previously defined).



Pro Tip:

Ensuring a virtual 'command center' is already established makes it easier for your team to collaborate and coordinate. Ensure you command center is secure and isolated from core systems to prevent exposure or vulnerability to additional damage.

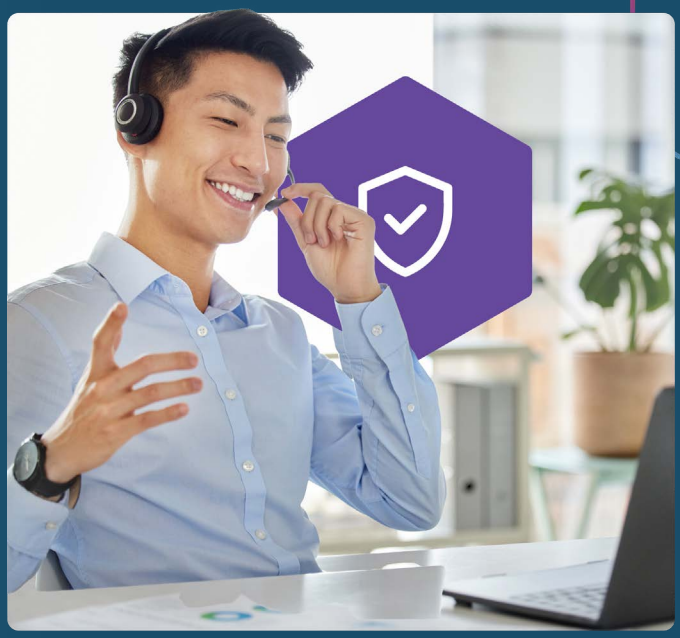
Step 4: Audit & Improve

A post-event response audit is a vital step in the overall response — and learning — lifecycle. It helps organizations learn from their experiences, identify areas for improvement, enhance risk management efforts, and demonstrate their commitment to security, resiliency and disaster recovery. By continually refining response processes, organizations can better protect themselves from future risk and minimize the impact of critical events.

- [ ] Collect feedback from internal team members and other business stakeholders to understand the effectiveness of your response plans, gauge your business's time to recovery and normal operations, and calculate event impact.

- [ ] Generate a comprehensive post-event report for sharing with relevant parties like board members, law enforcement, insurers or regulators. Ensure your plan captures the event's timeline, impact, response workflows and actions taken (with timestamps), key communications, damages and resolution details.

- [ ] Immediately conduct a post-incident review to identify lessons learned and areas for improvement across your response and management plans. Update the plans accordingly to enhance future readiness.

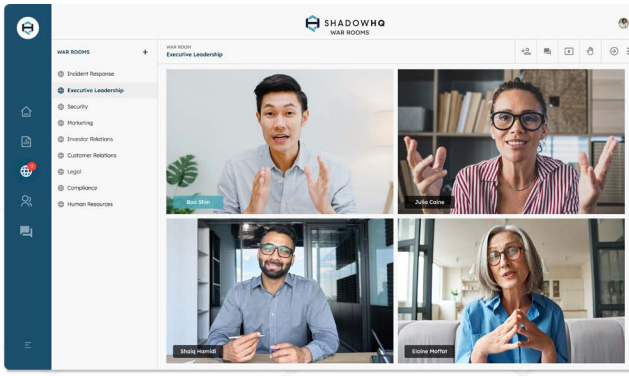


Pro Tip:

Maintain up-to-date activity logs to make make the auditing process effective, easier and more accurate.

Take control, collaborate, and manage any disaster scenario with ShadowHQ

Cover your bases and arm your business continuity and disaster response teams with everything they need to plan for, document, activate and respond to any disaster scenario. ShadowHQ is an all-in-one platform that proactively helps you plan for critical events, and securely manage them. It helps your team collaborate with key stakeholders across the business, assign tasks, access response documents and share real-time information as you navigate a crisis event.



Prepare

No more dusty, outdated binders or lost USB keys. Create your cybersecurity incident response plan with ShadowHQ so you're ready and armed with key contacts, documents and processes.

Execute

Contain any event by executing your mitigation strategy through your own secure and isolated command center. With ShadowHQ, teams can engage in voice, video and group chats, share updates and prioritize tasks safely, without further compromising IT or business stability.

Activate

Quickly coordinate your response efforts with ShadowHQ – log on to the ShadowHQ mobile app or desktop portal to instantly access secure communications channels, business continuity and cyber response plans, collaborative war rooms and real-time status updates.

Audit & Improve

Once an event has been contained and critical systems are restored, the learning can begin. Use ShadowHQ's activity logs and reporting dashboards to audit your response and ensure you're prepared for any future event that might come your way. Rest easy knowing your organization has an on-demand critical event response solution whenever critical events occur.

See how ShadowHQ can support your business's disaster readiness planning. Book your custom demo today.

LET'S TALK

> "
>
> **Finally, a product made for me.**
>
> ~ CISO at a global financial services firm

SHADOWHQ

ShadowHQ unites business continuity, incident response and crisis management—because an organized response supports a faster recovery.

See it in action and schedule your personalized demo today.

GET A DEMO

SHADOWHQ.IO