

Preparing for the Unexpected: A Business Disaster Preparedness Checklist

Practical steps to prepare your organization for disruption and recovery in the face of a disaster

A crisis can take many forms, from natural disasters and cyber incidents to fraud, employee absences, or supply chain interruptions. While we can't control when a crisis occurs, we can control how we respond and how well prepared we are to recover. A clear continuity plan can help protect critical resources, reduce confusion, and keep essential operations moving.

Use this checklist as a starting point to identify gaps, assign next steps, and develop a more detailed continuity plan tailored to your organization's operations and risks.

1. Assess Business Risks

Identify the disruptions most likely to affect your organization and the critical operations, systems, employees, facilities, and vendors they could interrupt.

Rank identified risks based on their potential impact and determine which critical functions would need to resume first.

Map the people, systems, facilities, data, vendors, and other dependencies required to restore those critical functions.

Document practical steps to reduce each major risk and assign responsibility for follow-up.

2. Review Insurance Coverage

Review business interruption (also known as business income and extra expense), property, cyber, liability, and other relevant coverage at least annually.

Confirm policy limits, exclusions, waiting periods, and claim requirements.

Maintain current insurer and broker contact information.

Update coverage as your organization's operations and exposure change.

3. Maintain Financial Reserves

Estimate the cost of maintaining essential operations during a disruption.

Maintain sufficient cash reserves and available credit to support short-term continuity and recovery needs.

Establish backup access to banking, payroll, and accounting systems.

4. Protect Employees and Assign Responsibilities

Create a crisis management team and clearly define individual responsibilities.

Identify backup decision-makers for critical roles.

Document evacuation, shelter, employee accountability, and remote-work procedures.

Maintain appropriate emergency supplies, including first aid materials, protective equipment, emergency radios, and backup power.

5. Establish a Communication Plan

Maintain current emergency contact lists for employees, customers, vendors, advisors, and other key stakeholders.

Establish primary and backup communication methods in case normal systems are unavailable.

Identify critical suppliers, alternate sources, and contract dependencies that could affect operations during a disruption.

Identify customers or other stakeholders who should receive priority communication.

Assign responsibility for internal updates and public or customer-facing communication.

6. Safeguard Important Records

Back up tax, financial, payroll, insurance, legal, ownership, and operational records using secure cloud-based or off-site storage.

Confirm that authorized personnel can remotely access critical records when needed.

Periodically review access permissions and remove access that is no longer required.

7. Prepare for Technology and Cyber Recovery

Use multifactor authentication and other appropriate access controls for critical systems and accounts.

Maintain backups that are appropriately separated from primary systems or networks to reduce the risk of simultaneous loss or compromise.

Periodically test backups and confirm that critical systems and data can be restored.

Document manual workarounds or alternate processes for critical operations if technology systems become unavailable.

Identify internal personnel and outside technology or cybersecurity providers responsible for responding to and recovering from an incident.

8. Document Equipment and Valuables

Maintain an inventory of equipment and other valuable assets, including model and serial numbers, photographs, receipts, and current valuations when available.

Store an updated copy of the inventory away from the primary business location.

9. Identify Disaster Relief Resources

Maintain a list of federal, state, and local assistance resources, including FEMA and the U.S. Small Business Administration.

Identify documentation that may be required when applying for disaster assistance or filing claims.

Establish a process for tracking losses, recovery expenses, insurance proceeds, and relief funds.

10. Involve Your Trusted Advisors

Include your advisors as you assess risks, review insurance coverage, and develop continuity procedures.

Know whom to contact for help with internal controls, financial reporting, insurance claims, relief applications, and recovery decisions.

11. Review and Test the Plan

Assign an owner and target date for unresolved preparedness items.

Share the completed plan with employees and others who have response responsibilities.

Test emergency communication methods, backup access, system recovery, and other critical procedures.

Update the plan based on what you learn from testing.

Review the plan at least annually and whenever significant changes occur in your staff, systems, facilities, vendors, or service providers.

Partnering for a Stronger Future

A practical crisis plan can help your organization protect its people and resources, maintain critical operations, and recover more effectively.

Contact your CRI advisor to discuss your organization's risks and strengthen your business continuity strategy.



criadv.com/contact



†This is not a CPA firm.

*Assurance, attest, and audit services provided by Carr, Riggs & Ingram, L.L.C.

"Carr, Riggs & Ingram" and "CRI" are the brand names under which Carr, Riggs & Ingram, L.L.C.* ("CRI CPA*"), CRI Advisors, LLC† ("CRI Advisors†" or "Advisors†"), and Capin Crouse, LLC* ("Capin Crouse CPA*"), and CRI Capin Crouse Advisors, LLC† ("Capin Crouse Advisors†") provide professional services. CRI CPA*, Capin Crouse CPA*, CRI Advisors†, Capin Crouse Advisors†, Carr, Riggs & Ingram Capital, LLC and their respective subsidiaries operate as an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations and professional standards. CRI CPA* and Capin Crouse CPA* are licensed independent certified public accounting ("CPA") firms that separately provide attest services, as well as additional ancillary services, to their clients. CRI CPA* and Capin Crouse CPA* are independently-owned CPA firms that provide attestation services separate from one another. CRI Advisors† and Capin Crouse Advisors† provide tax and business consulting services to its clients. CRI Advisors† and its subsidiaries, including Capin Crouse Advisors†, are not licensed CPA firms and will not provide any attest services. The entities falling under the Carr, Riggs & Ingram or CRI brand are independently owned and are not responsible or liable for the services and/or products provided, or engaged to be provided, by any other entity under the Carr, Riggs & Ingram or CRI brand. Our use of the terms "CRI," "we," "our," "us," and terms of similar import, denote the alternative practice structure conducted by CRI CPA*, Capin Crouse CPA*, Capin Crouse Advisors†, and CRI Advisors†, as appropriate.