# DR PLAN CHECKLIST

A disaster recovery plan checklist & planning guide for small to medium businesses.

# IS YOUR BUSINESS PREPARED?

Ponemon Institute: 43% of businesses that experience a disaster without a DRP never recover. Don’t be one of them.

Get started with your DR plan today. We can help.

**WWW.ASI-NETWORKS.COM**

# Disaster Recovery Plan Checklist and Planning Guide

For: Business Managers and IT Directors | August 15, 2023

**Table of Contents**

## Introduction and Purpose

In the ever-changing landscape of business and technology, preparedness for unforeseen events is paramount. This checklist aims to provide a foundational framework for creating your organization's disaster recovery plan. It's important to note that while this checklist covers a wide range of considerations, it is not an exhaustive list.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

Every business environment is unique, and each organization has distinct requirements. Therefore, this checklist should be viewed as a starting point, a guide to be customized and expanded upon based on your specific needs. Your company's size, industry, technology infrastructure, and risk profile will influence the shape and scope of your disaster recovery plan.

This checklist covers key areas including risk assessment, data backup, recovery strategies, communication plans, testing procedures, resource allocation, legal compliance, employee education, and much more. It's designed to help IT Administrators systematically address essential aspects of disaster preparedness.

Remember, disaster recovery planning is an ongoing endeavor. Regularly review, adapt, and improve your plan to stay aligned with evolving business dynamics and technological advancements. With careful planning, you can safeguard your organization's critical operations, data, and reputation.

Use this checklist as a tool to guide your disaster recovery planning process, ensuring that your organization is well-prepared to face unforeseen challenges and emerge stronger from adversity.

Kay, so let's get into it!

# Risk Assessment and Business Impact Analysis

These are processes that help organizations identify potential threats and vulnerabilities and their potential consequences for business operations.

**Risk Assessment:** This involves identifying and evaluating various risks that can affect the organization, such as natural disasters, cyberattacks, or supply chain disruptions. It helps prioritize which risks are most critical.

**Business Impact Analysis:** This delves into understanding how each risk, if realized, would impact different aspects of the business, including operations, finances, and reputation. It helps determine the severity and potential losses associated with each risk.

Together, these processes provide insights for organizations to make informed decisions about how to prepare for and mitigate the impact of potential disruptions. They form the foundation of a solid disaster recovery plan.

- □ Identify potential threats and disasters that could affect the business.
- □ Assess vulnerabilities in infrastructure, systems, and operations.
- □ Conduct a business impact analysis to determine the consequences of disruptions on critical functions.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

# Critical Data Identification and Backup

This refers to the process of identifying and prioritizing the most important data within your organization and establishing a systematic approach to ensure its protection and availability.

## Critical Data Identification:

Identify data that is essential for your organization's day-to-day operations, compliance requirements, or strategic decision-making.

It includes data such as customer records, financial information, intellectual property, and any other information that, if lost, could significantly impact your business.

## About Backing up Your Data

Once critical data is identified, a backup strategy is put in place. This strategy includes regular and secure copies of critical data, typically stored in different locations. It ensures that even in the event of data loss due to hardware failure, cyberattacks, or other disasters, you can quickly restore your critical data to minimize downtime and prevent data loss.

These are crucial components of disaster recovery planning. Make sure that your most vital information is safeguarded and can be recovered when needed.

- □ Identify critical data and prioritize its backup and restoration.
- □ Establish a regular data backup schedule for all critical systems.
- □ Explore both on-site and off-site backup storage options.
- □ Test data restoration procedures to ensure backups are valid.

# Recovery Time Objective (RTO)

RTO is a critical metric in disaster recovery planning. It defines the maximum allowable downtime for a business process or system after a disruption.

In simpler terms, RTO represents the time a business can afford to be without a particular function or system before it significantly impacts operations.

Achieving a shorter RTO means quicker recovery and less disruption to business continuity, but it often requires higher investments in redundancy and recovery solutions.

Businesses should set RTOs based on the criticality of each function or system to balance operational needs and costs.

- □ Define the acceptable maximum downtime for each critical business function (RTO).

# Recovery Point Objective (RPO)

RPO is another vital metric in disaster recovery planning. It defines the maximum acceptable data loss in time.

In short, RPO represents the point in time to which data must be recovered after a disruption. For instance, if your RPO is set at one hour, it means that you can tolerate data loss up to one hour before the incident.

RPO is closely tied to data backup and recovery strategies. A shorter RPO means minimal data loss, but it often requires more frequent data backups and sophisticated recovery solutions.

Businesses must carefully set RPOs based on the criticality of data and systems, balancing data protection needs with cost-effectiveness.

- □ Determine the maximum amount of data loss tolerable during recovery (RPO).
- □ Align RTO and RPO with business needs and resources.

# Disaster Recovery Team and Communication Plan

You’ll designate a group of individuals responsible for managing and coordinating actions during and after a disaster, as well as outlining how communication will be handled.

Here’s why this is important:

**Rapid Response:** Having a dedicated team ensures a swift and organized response to disasters, minimizing downtime and damage.

**Clear Communication:** The plan outlines how communication will be managed, ensuring that information reaches the right people at the right time, both internally and externally.

**Minimizing Confusion:** In a crisis, clear roles and responsibilities reduce confusion and empower team members to take decisive actions.

**Stakeholder Updates:** Effective communication keeps stakeholders, including employees, clients, and the public, informed about the situation, maintaining trust and confidence.

**Legal and Regulatory Compliance:** In some cases, regulatory compliance mandates the establishment of a designated disaster recovery team and communication plan.

This is vital to safeguarding the organization and its stakeholders.

- ☐ Appoint a Disaster Recovery Team with defined roles and responsibilities.
- ☐ Establish communication protocols during a disaster, both internal and external.
- ☐ Maintain up-to-date contact lists for employees, vendors, and stakeholders.

# Alternate Worksite and Workspace Recovery

An "Alternate Worksite and Workspace Recovery" plan is crucial in a disaster recovery (DR) plan because it provides a strategy for maintaining business operations when the primary location or workspace becomes unavailable due to a disaster or disruption.

Okay, so why’s this so important? It must cost a lot to set this up, no? Let's look at it in detail from these key points:

**Business Continuity:** It ensures business operations continue even if the primary location is inaccessible. This minimizes downtime, revenue loss, and customer impact.

**Data and Resource Accessibility:** Alternate worksite locations allow employees to access essential data, systems, and resources, ensuring uninterrupted service to clients and customers.

**Disaster Preparedness:** It demonstrates proactive disaster preparedness and a commitment to maintaining service levels, which can boost customer and stakeholder confidence.

**Risk Mitigation:** Having a backup workspace reduces the risk associated with single points of failure, such as a single office location.

**Employee Safety:** In cases of physical threats like natural disasters, providing a safe alternate workspace ensures employee well-being.

- ☐ Identify alternate worksite locations for employees to continue operations if the primary location is unavailable.
- ☐ Develop plans for remote work and establish secure remote access to business systems.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

# Power and Utility Continuity

- □ Evaluate power sources and backup power options.
- □ Establish protocols for utility continuity (e.g., water supply) during disasters.

Power and utility continuity planning involves strategies and measures to ensure that essential services such as electricity, water, and other utilities remain available during a disaster or disruption.

Here are some key considerations:

## Redundancy and Backup Power

**Backup Generators:** Installing backup generators can provide a reliable source of power during electrical outages. Generators should be regularly tested and well-maintained.

Uninterruptible Power Supplies (UPS): UPS systems can bridge the gap between a power outage and a generator startup. They are crucial for sensitive electronic equipment.

## Diverse Power Sources

**Alternative Energy Sources:** Consider alternative and renewable energy sources like solar panels and wind turbines to reduce reliance on the grid. These sources can provide sustainable power during disruptions.

## Monitoring and Alerts

**Real-time Monitoring:** Implement monitoring systems to track power quality and utility services. These systems can provide early warnings of disruptions.

**Automated Alerts:** Configure automated alerts to notify key personnel when power or utility issues are detected, allowing for a rapid response.

## Energy Efficiency

**Energy Audits:** Conduct energy audits to identify opportunities for energy efficiency improvements. This can help reduce energy consumption and lower costs.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

## Infrastructure Protection

**Physical Security:** Protect critical infrastructure, such as power generators and distribution systems, from physical threats like vandalism or sabotage.
Water and Utilities:

**Water Supply:** Ensure access to clean water during disruptions. Consider on-site water storage and filtration systems.

**Gas and Fuel:** Plan for continuity of fuel supplies if your operations rely on gas or other fuels. Ensure safe storage and backup options.

## Regulatory Compliance

**Compliance Assessment:** Understand and comply with local, state, and federal regulations related to power and utility continuity, particularly in highly regulated industries.
Communication and Reporting:

**Internal Communication:** Establish clear communication channels within your organization for reporting power or utility issues and coordinating responses.

**External Communication:** Maintain communication with utility providers and local authorities to stay informed about restoration efforts and timelines.

# Equipment and Inventory Protection

This one's an obvious one, but we assume nothing and explain everything!

You can't argue that power and utility continuity are critical aspects of a disaster recovery (DR) plan. Having a plan for continuous power ensures that essential services like electricity, water, and other utilities remain available during and after a disaster or disruption.

How's this going to help your operation specifically?

**Sustaining Operations:** Many business operations are highly dependent on a continuous power supply. Ensuring power continuity keeps these operations running, reducing downtime and revenue loss.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

**Data Center and IT Infrastructure:** Data centers and IT infrastructure rely heavily on electricity. Power continuity prevents data loss, maintains online services, and safeguards critical IT systems.

**Communication:** Uninterrupted power is essential for communication tools, such as phones, email, and collaboration platforms. It ensures employees can stay connected during a crisis.

**Security:** Adequate power is vital for security systems, including surveillance cameras, access control, and alarm systems. Maintaining security helps protect assets and personnel.

**Customer Service:** Continuous power enables businesses to maintain customer service operations, preventing service disruptions and preserving customer satisfaction.

**Emergency Response:** During a disaster, power is crucial for emergency response efforts, including lighting, communication, and medical equipment.

**Data Center Cooling:** Data centers require stable cooling to prevent overheating of servers and data loss. Power continuity ensures data center cooling systems remain operational.

- ☐ Implement measures to safeguard critical equipment and inventory from physical damage.
- ☐ Consider redundant hardware and spare parts for essential systems.
- ☐ Cybersecurity and Data Protection
- ☐ Implement robust cybersecurity measures to prevent cyberattacks.
- ☐ Establish protocols for incident response and data breach management.

# Vendor and Supplier Continuity

You may not think this is a key element of a DR plan, but hopefully, these points will make you consider including them in your plans.

Vendor and supplier continuity planning is an essential component of a disaster recovery (DR) plan because it ensures that the goods and services provided by external partners remain available, even during and after a disaster or disruption.

**Here’s how this is going to help:**

**Supply Chain Resilience:** Vendor and supplier continuity planning strengthens your supply chain's resilience. It reduces the risk of disruptions in the availability of essential materials, products, or services.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

**Business Operations:** Many organizations rely on external vendors and suppliers for critical components. Ensuring their continuity prevents production halts and service disruptions.

**Customer Commitments:** Maintaining relationships with reliable vendors and suppliers helps you meet customer commitments and maintain trust, even during challenging times.

**Resource Availability:** Vendors and suppliers may provide resources necessary for your disaster recovery efforts, such as backup hardware, alternative workspaces, or emergency services.

**Risk Mitigation:** By assessing and planning for vendor and supplier continuity, you mitigate the risks associated with third-party dependencies.

**Legal and Regulatory Compliance:** In some industries, regulatory compliance requires businesses to have contingency plans for vendor and supplier continuity.

- □ Assess the business continuity plans of key vendors and suppliers.
- □ Establish alternative suppliers to ensure the continuity of essential supplies and services.

# DR Plan Testing and Training

If you can’t be sure your plan will work and that everyone knows what to do in a DR scenario, then what good is the plan?

Testing and training your Disaster Recovery (DR) plan with employees and staff is of paramount importance. Here's why:

**Validation of Preparedness:** Testing allows you to validate the effectiveness of your DR plan. It helps identify gaps, weaknesses, and areas that require improvement. Without testing, assumptions about the plan's effectiveness remain unverified.

**Familiarization:** Training ensures that employees and staff are familiar with the DR plan's procedures and their roles during a disaster. This familiarity reduces confusion and hesitation in a real crisis, enabling a quicker and more effective response.

**Response Efficiency:** Regular drills and exercises enhance the efficiency of your team's response. Well-trained staff can perform tasks more swiftly and accurately, minimizing downtime and potential losses.

**Awareness and Accountability:** Training raises awareness about the importance of disaster preparedness. It instills a sense of accountability among employees, making them proactive in ensuring the plan's success.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

**Adaptation to Change:** As your organization evolves, so should your DR plan. Regular training allows employees to adapt to new technologies, processes, and organizational changes, ensuring that the plan remains relevant.

**Legal and Regulatory Compliance:** In some industries, demonstrating that employees are trained and that the DR plan is regularly tested is a legal or regulatory requirement.

**Stakeholder Confidence:** Stakeholders, including customers, partners, and investors, gain confidence in your organization when they know that you have a tested and well-trained DR plan in place. It demonstrates a commitment to business continuity and risk mitigation.

**Reduced Stress:** Familiarity with the DR plan reduces stress levels during an actual disaster. Employees are more likely to remain calm and follow established procedures.

Testing and training sessions provide valuable feedback that can be used to refine and enhance the DR plan over time.

- □ Train employees on their roles and responsibilities during a disaster.
- □ Periodically test the disaster recovery plan to ensure its effectiveness.
- □ Document and review test results to identify areas for improvement.
- □ Educate employees about the importance of disaster preparedness.
- □ Conduct training sessions and workshops.

# Crisis Communication and Public Relations

Crisis communication and public relations are critically important components of a comprehensive disaster recovery (DR) plan. Here's why:

**Maintaining Reputation:** Effective crisis communication and public relations help protect and maintain your organization's reputation during and after a disaster. How you communicate can greatly influence how stakeholders perceive your response.

**Transparency and Trust:** Open and honest communication fosters trust among employees, customers, partners, and the public. It demonstrates your commitment to transparency, even in challenging times.

**Timely Updates:** Providing timely updates on the situation keeps stakeholders informed and reduces uncertainty, preventing the spread of rumors and misinformation.

**Legal and Regulatory Compliance:** In some industries, regulatory compliance mandates specific communication protocols during disasters. Failing to comply can lead to legal and financial consequences.

**Customer and Employee Reassurance:** Effective communication assures customers and employees that their well-being and interests are a priority, even in a crisis.

**Media Relations:** Managing media inquiries and relations during a disaster is crucial. Well-prepared communication can help control the narrative and ensure accurate reporting.

**Coordination:** Coordination with government agencies, emergency services, and other organizations often requires effective communication to ensure a seamless response.

**Social Media Management:** In the age of social media, managing the online narrative is crucial. Social media channels can disseminate information rapidly, making it important to have a social media strategy in place.

**Recovery Image:** Beyond the immediate response, crisis communication plays a role in how your organization is perceived during the recovery phase. It can impact the speed and success of your recovery efforts.

- ☐ Develop a crisis communication plan for external stakeholders, including customers and the media.
- ☐ Establish protocols for communicating the status of operations during a disaster.

# Emergency Response and Evacuation Procedures

Emergency response and evacuation procedures are vital elements of a disaster recovery plan. In a nutshell:

**Safety First:** Prioritize the safety of employees and occupants during a disaster. Include clear guidelines on how to respond to different types of emergencies, such as fires, natural disasters, or security threats.

**Evacuation Plans:** Outline evacuation routes, assembly points, and procedures for safely leaving the premises. Well-practiced evacuation plans can save lives in critical situations.

**Emergency Contacts:** Provide contact information for local authorities, medical services, and other relevant parties who need to be informed or involved in the response.

**Training and Drills:** Ensure that employees are familiar with these procedures, know what to do in an emergency, and can respond quickly and effectively.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*

- □ Establish emergency response procedures, including evacuation plans.
- □ Conduct drills to ensure employees are familiar with evacuation routes and assembly points.

# Continuous Improvement

Regularly review and update the disaster recovery plan based on changes in the business environment, technology, or risks.

A yearly review is a good starting point for this.

# Additional Resources

**Guidance on Power and Utility Continuity Planning:**

1. U.S. Small Business Administration (SBA)
2. Federal Emergency Management Agency (FEMA)
3. Occupational Safety and Health Administration (OSHA)
4. National Institute of Standards and Technology (NIST)

**Emergency Response and Evacuation Procedures:**

1. OSHA's eTool: Access the eTool
2. FEMA's toolkit: Download the toolkit
3. NFPA-Emergency evacuation planning guide

**DATTO - RTO and RPO Calculator:**
Access the calculator

# Contact ASi Networks

Ready to safeguard your business against unforeseen disasters? Contact ASi Networks today for a free consultation and assessment of your disaster recovery needs. **800-251-1336**

Our experienced team is here to help you create a tailored disaster recovery plan that ensures the resilience and continuity of your operations.

Be proactive, and don't wait for a disaster to hit before you begin planning for it.

*This checklist provides general guidance and should not be considered as a replacement for professional advice. Consult with experts in relevant fields when developing your organization's disaster recovery plan.*

*Please note that the checklist is for informational purposes only. Your organization's specific environment and requirements will necessitate modifications to this checklist to ensure its applicability to your situation.*