Disaster recovery plan template for SMEs

Why disaster recovery matters for SMEs

- An organisation's Disaster Recovery Plan (DRP) outlines processes for recovering IT systems and data following an issue or disaster.
- Businesses use a DRP to recover from things like ransomware attacks, server failures, or business interruptions.
- IT outages can prevent companies from functioning. For example, Microsoft 365 can experience service outages, which can prevent a business from continuity.
- According to UK Government surveys, SMEs are impacted by cyber incidents each year.
- Ransomware attacks pose one of the biggest risks to businesses when compared to other forms of cybercrime.
- A DRP ensures compliance with UK GDPR requirements and adheres to Cyber Essentials Standards.
- A DRP reduces downtime, minimises the impact of data loss, and helps businesses return to normal after a business disruption occurs.

What is a Disaster Recovery Plan?

The Disaster Recovery Plan (DRP) is a written set of instructions detailing how an organisation restores its IT systems after any incident.

The DRP focuses specifically on technological recovery, including the following:

- data recovery
- recovery of servers
- application availability
- network infrastructure
- communication systems

A typical DRP would have the following components:

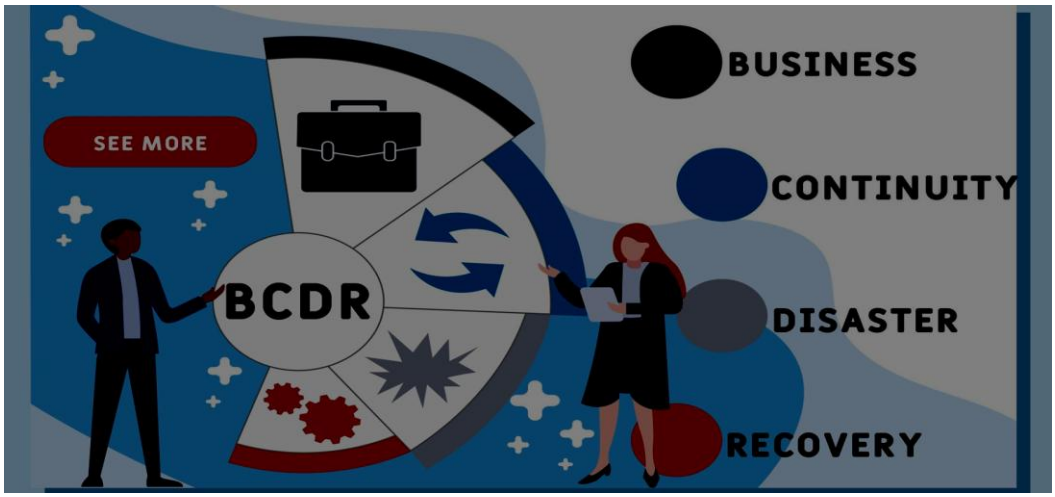
- systems priorities
- steps to recover each system
- who has responsibilities in the plan
- way of communicating during recovery
- how will backups be restored

In simple terms, the Disaster Recovery Plan answers the question:

"If we have a failure of our systems tomorrow, how can we be back in business?"

Disaster Recovery vs Business Continuity

Area	Disaster Recovery	Business Continuity
Focus	Restoring IT systems	Maintaining business operations
Scope	Technical recovery	Organisation-wide response
Example	Restoring file servers	Continuing customer support
Objective	Recover systems	Keep the business running
Area	Disaster Recovery	Business Continuity
Focus	Restoring IT systems	Maintaining business operations



The risks SMEs face without a DRP

Without a documented Disaster Recovery Plan, organisations will likely face:

➢ More time to recover

While determining how to recover, there will be any access for staff to systems.

➢ Loss of data

If there is insufficient data backups, there could be a loss of work done immediately prior to failure.

➢ Business interruption

Business functions such as customer service, finance, and communications are interrupted.

➢ Financial ramifications

Revenue lost due to business interruption, cost of recovering to PRE-incident operations could be substantial.

- **Non-compliance with regulation**s

In accordance to UK Data Protection Regulations, organisations need to be able to demonstrate that they manage the data in a responsible manner.

➢ Problems with insurance

Many cyber insurers require proof of backup planning and recovery planning procedures.

Adopting resilience practices as suggested by frameworks such as Cyber Essentials can help the organisation further manage their overall risk.

A step-by-step guide for creating a DRP consists of:

You do not need to have a sophisticated technology set up to put together a Disaster Recovery Plan (DRP). Your most important task is to document the process to restore systems in the event of a disaster.

Step 1: Determine the critical systems used in your environment.

Make a list of the key IT services your business relies on such as:

- E-mail systems
- File storage
- Accounting application
- Customer Relationship Management (CRM) application
- Internet connectivity

Step 2: Decide the order in which to restore the systems.

The order of restoration can range from those required to conduct business operations, to systems that can withstand a longer outage.

Step 3: Establish your RTO and your RPO.

By determining how long you can go without each system and how much data loss is acceptable, you can develop backup and recovery strategies.

Step 4: Document the recovery process for each system.

Clearly document the procedures for restoring all systems.

Step 5: Determine the people accountable for the recovery process and who provides assistance to them.

Identify the recovery process leader and who will assist.

Step 6: Implement a backup strategy.

Create a backup solution, that is reliable and has been tested for successful recovery.

Step 7: Create a communication process for internal and external clients.

Create a plan to inform employees, clients, and suppliers of developments during a disruption.

Step 8: Test the Plan.

Conduct frequent tests to ensure that your recovery processes will work when they are needed.

Full Disaster Recovery Plan Template

1. Document Control

- Plan Owner:
- Version:
- Last Updated:
- Next Review Date:

2. Key Business Systems

List essential technology platforms.

Example table:

System	Purpose	Owner	Location
Email platform	Business communication	IT provider	Cloud
File storage	Shared documents	Operations	Cloud/server
Accounting software	Financial management	Finance team	Cloud

3. Recovery Priorities

System	Priority	Maximum Downtime	Business Impact
Email	High	4 hours	Communication disruption
File storage	High	4 hours	Staff unable to work
CRM	Medium	24 hours	Sales delays

4. Disaster Scenarios

Identify potential business interruption scenarios; examples are:

- Ransomware attack
- Server failure
- Cloud platform outage
- Power outage at an office
- Internet connectivity problems

- Theft or damage to hardware

5. Recovery Procedures

Create step-by-step recovery plans for:

- Data restoration
- Server rebuild
- Cloud service recovery
- Email restoration
- Endpoint device recovery

6. Backup Strategy

Specify key aspects of your backup strategy, such as:

- Backup frequency
- Off-site/cloud location of backup
- Backup encryption
- Backups should be tested for verifiability
- Retention period of backups

7. Incident Response Team

Examples include:

- Incident lead
- IT recovery lead
- Communications liaison
- Operations manager

List contact details for:

- Internal staff
- IT provider
- Key suppliers

8. Communication Plan

In the event of disruption, it is essential to communicate.

Identify how to notify:

- Employees
- Customers

- Suppliers
- External stakeholders

RTO and RPO

Two metrics that guide your recovery efforts include:

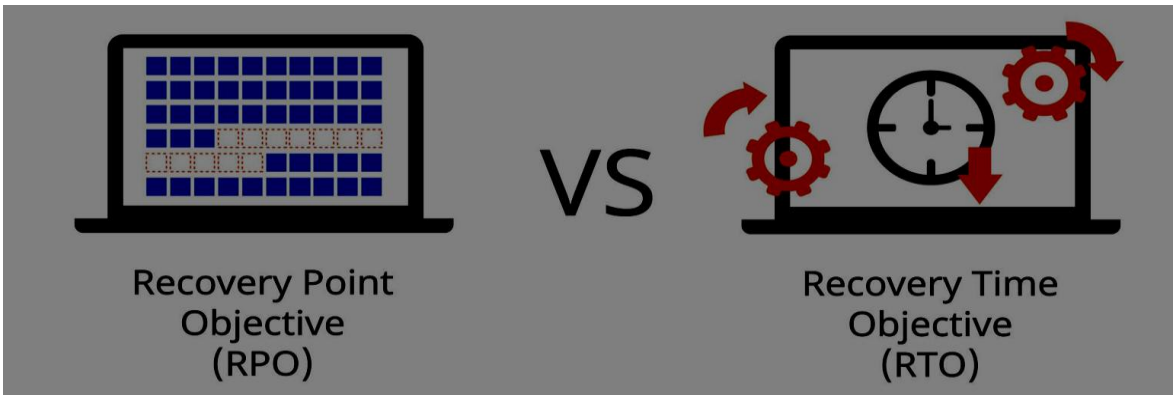
Recovery Time Objective (RTO)

The maximum amount of time that you can be without your systems.

Example: If your email RTO is four hours then you need to attempt to have things restored to functioning within that four-hour period.

Recovery Point Objective (RPO)

The maximum amount of time that you can afford to be without data. An RPO defines the maximum amount of time you can afford to lose data.



Example: If your RPO is 24 hours then your backup plan will ensure that data can be restored from a backup that is no more than 24 hours old.

Testing and Maintaining a DRP

A disaster recovery plan is only useful if it is tested on a regular basis. To the extent possible you should use best practices by:

- Testing the backups restoration
- Conducting tabletop simulations of incidents
- Reviewing your recovery process
- Updating the documents when there are changes to your system

Most commonly, an annual review meets the needs of most small to median companies.

Disaster Recovery Readiness Checklist

☐ Documenting Critical Systems

☐ Defining Recovery Priorities

☐ Implementing a Backup Strategy

☐ Assigning Responsibilities for Incident Response

☐ Defining Communication Protocols

☐ Documenting Recovery Plans

☐ Testing the Disaster Recovery Plan Every Year

Backup Validation Checklist

☐ Confirming Backup Schedules

☐ Securing Backup Locations

☐ Conducting Restoration Checks (Testing Backups)

☐ Enabling Backup Monitoring

FAQs

1. Does the Law Require Disaster Recovery Planning (DRP) in the UK?

There is no legal requirement for a disaster recovery plan, but all businesses must follow UK data protection laws by safeguarding data that is personal.

2. How Often Should You Test a DRP?

In most cases, small and medium-sized businesses should evaluate their DRP at least once a year to determine its effectiveness.

3. Who is Responsible for the DRP?

In most cases, the IT Director, Operations Director, or an external IT vendor is responsible for the disaster recovery plan.

4. What Level of Detail Do I Need to Include in the DRP?

A DRP should have sufficient detail so that all employees can execute the recovery steps when necessary.

5. Are Cloud-Based Backup Services Sufficient for Disaster Recovery?

While they can be valuable, cloud-based backup services need to be verified and tested regularly as part of your disaster recovery plan.

About This Guide

The **Computer Support Centre** developed this document to assist small to medium-sized UK businesses in developing and executing an operationally sound disaster recovery framework.

This document provides simple tangible guidance for business owners, operations managers, and IT assisting organisations in developing a realistic disaster recovery plan without undue technical complexity.

Instead of emphasising theory, this document provides practical recovery methodologies, checklists, and structured templates designed for UK SMEs. The ultimate aim of this publication is to assist organisations in decreasing overall downtime, safeguarding key data and increasing their organisation’s resiliency towards cyber crime, hardware failure, and any other unforeseen disruption.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:

 https://computersupportcentre.com

Conclusion

A disaster recovery plan should be considered more than an IT policy it represents a practical safeguard used for the rapid recovery of your organisation when the unexpected occurs. A few hours' downtime can severely impact your business processes delay the provision of services to your clients; and create a financial loss.

Fortunately, disaster recovery does not have to be complicated: Businesses who have identified their critical systems; agreed on realistic recovery priorities; continue to maintain reliable backups and produce documentation on clear recovery procedures can generally prevent downtime to their operations due to cyber incidents; outages; or hardware failures.

In summary, an effective Disaster Recovery Plan ensures that when a disruption occurs, your employees know in advance what to do who is responsible and how to restore the systems. Simply put, preparing today eliminates confusion tomorrow.