



Business Continuity And Disaster Recovery Project Checklist Template 2026

Business Impact Analysis (BIA) & Risk Assessment

Identify critical business functions, evaluate potential threats (natural disasters, cyberattacks, etc.), and determine the impact of operational downtime on key organizational processes.

Critical Business Process Name

Write something...

Description of Business Impact if Process is Disrupted

Write something...

Target Recovery Time Objective (RTO)

Enter time...

Estimated Financial Loss per Hour of Downtime

Enter a number...

Identified Risk Threats

- ☐ Cyberattack/Ransomware
- ☐ Natural Disaster
- ☐ Power/Utility Failure
- ☐ Human Error/Malice
- ☐ Supply Chain Disruption

Supporting Risk Assessment Documentation

 Upload File

Disaster Recovery (DR) Strategy Development

Define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), and outline technical procedures for restoring IT systems, data, and infrastructure.

Recovery Time Objective (RTO) per Critical System

Write something...

Recovery Point Objective (RPO) per Critical System

Write something...

Primary Recovery Site Type

- ☐ Hot Site (Fully operational)
- ☐ Warm Site (Pre-configured hardware)
- ☐ Cold Site (Infrastructure only)
- ☐ Cloud-Based Recovery (DRaaS)

Critical IT Assets to be Recovered

- ☐ Database Servers
- ☐ Customer-Facing Applications
- ☐ Email and Communication Systems
- ☐ ERP/CRM Systems
- ☐ Network Infrastructure

Draft DR Strategy Document

 Upload File

Next Strategy Review Date

Enter date...

Communication & Crisis Management Planning

Establish emergency communication protocols, identify the crisis management team, and define internal and external stakeholder notification procedures.

Crisis Management Team Lead Name

Write something...

Primary Communication Channels

- ☐ SMS/Text Alert
- ☐ Email Blast
- ☐ Corporate Slack/Teams
- ☐ Emergency Phone Tree
- ☐ Company Intranet/Dashboard

External Stakeholder Notification Script

Write something...

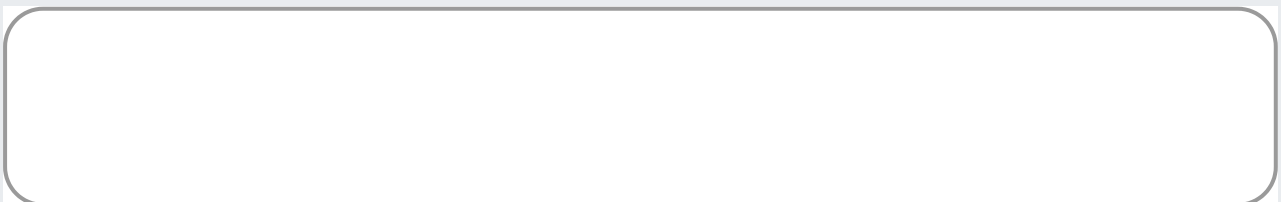
Last Communication Protocol Review Date

Enter date...

Emergency Contact Directory (Master List)

 Upload File

Plan Approval Signature



Data Backup and Redundancy Verification

Audit existing backup schedules, ensure offsite/cloud storage integrity, and verify the immutability of backups against ransomware threats.

Last Backup Completion Date

Backup Storage Location

- ☐ On-Premise Server
- ☐ Cloud Storage (AWS/Azure/GCP)
- ☐ Offsite Physical Media
- ☐ Hybrid Cloud

Data Sets Verified

- ☐ Critical Databases
- ☐ System Configuration Files
- ☐ User Files/Documents
- ☐ Application Logs
- ☐ Financial Records

Recovery Point Objective (RPO) in Minutes

Backup Integrity Test Report

 Upload File

IT Manager Verification

Resource and Infrastructure Readiness

Verify availability of emergency hardware, secondary workspaces, power backups (UPS/Generators), and essential software licenses for recovery scenarios.

Critical Infrastructure Assets Verified

- ☐ Backup Power Generators/UPS
- ☐ Secondary Site/Warm Site Access
- ☐ Redundant Network Connectivity
- ☐ Emergency Hardware Inventory
- ☐ Cloud Disaster Recovery Environment

Secondary Site Location Details

Write something...

Last Hardware Audit Date

Enter date...

Infrastructure Inventory Document

 Upload File

Minimum Required Power Redundancy (Hours)

Enter a number...

IT Infrastructure Manager Approval

Incident Response Plan (IRP) Documentation

Develop step-by-step actionable workflows for different disaster scenarios, including roles, responsibilities, and escalation matrices.

Incident Declaration Procedure

Write something...

Incident Severity Levels

- ☐ Low - Minor disruption
- ☐ Medium - Partial service unavailability
- ☐ High - Critical system failure
- ☐ Critical - Total business shutdown

Escalation Contact Matrix

Write something...

Standard Operating Procedures (SOP) Documents

 Upload File

Last Document Review Date

Enter date...

Plan Approval Authorization

Testing, Training, and Simulation

Schedule and execute tabletop exercises, full-scale disaster simulations, and staff training sessions to validate the effectiveness of the recovery plan.

Last Simulation Date

Enter date...

Simulation Type

- ☐ Tabletop Exercise
- ☐ Full-Scale Disaster Drill
- ☐ IT System Failover Test
- ☐ Communication Drill

Departments Involved in Training

- ☐ IT & Security
- ☐ Operations
- ☐ Human Resources
- ☐ Legal & Compliance
- ☐ Executive Leadership

Simulation Results & Gap Analysis

Write something...

Upload Simulation Post-Mortem Report

 Upload File

Incident Commander Approval

Supply Chain and Third-Party Dependency Audit

Review critical vendor SLAs and ensure that key suppliers have compatible business continuity plans in place to prevent downstream failures.

Critical Vendors Identified

- ☐ Cloud Service Providers (SaaS/IaaS)
- ☐ Logistics & Transportation Partners
- ☐ Software/SaaS Vendors
- ☐ Hardware & Infrastructure Suppliers
- ☐ Managed Service Providers (MSP)

Vendor Risk Rating

Write something...

Vendor Business Continuity Plan (BCP) Evidence

 Upload File

Last Audit Completion Date

Enter date...

Dependency Criticality Level

- ☐ Mission Critical
- ☐ High Impact
- ☐ Moderate Impact
- ☐ Low Impact

Identified Dependency Gaps and Mitigation Strategy

Write something...

Post-Disaster Recovery & Post-Mortem Procedures

Define the process for transitioning back to normal operations (failback) and conducting audits to improve the plan based on lessons learned.

Date of Post-Mortem Meeting

Enter date...

Summary of Incident and Impact

Write something...

Identified Root Causes

- ☐ Cybersecurity Breach
- ☐ Hardware/Infrastructure Failure
- ☐ Human Error
- ☐ Natural Disaster
- ☐ Third-party/Vendor Failure
- ☐ Other

Lessons Learned and Corrective Actions

Write something...

Incident Report Documentation

 Upload File

Crisis Management Lead Approval

Maintenance and Periodic Plan Review

Establish a recurring schedule for updating contact lists, updating technology inventories, and revising the plan to reflect new 2026 organizational changes.

Next Scheduled Review Date

Enter date...

Review Frequency

- ☐ Monthly
- ☐ Quarterly
- ☐ Bi-Annually
- ☐ Annually

Areas Reviewed During This Cycle

- ☐ Contact Information/Call Trees
- ☐ IT Infrastructure/Server Inventory
- ☐ Vendor/Third-Party Contracts
- ☐ Backup and Recovery Procedures
- ☐ Emergency Resource Availability

Review Findings and Required Updates

Write something...

Plan Approver Signature

< Previous

> Next

✓ Finish

✂ Generate Sample Report