SOFTTECO

Disaster recovery plan checklist

Use this checklist to confirm your organization has covered the key elements of a practical disaster recovery plan. Adapt the detail to your organization's size, complexity, and risk profile.

01 Scope, governance and ownership

- [ ] Define the purpose and scope of the DR plan
- [ ] Define what constitutes a disaster or major disruption for your organization
- [ ] Identify who owns the DR program and who can activate the plan
- [ ] Define recovery roles, responsibilities and decision-making authority
- [ ] Assign owners to critical recovery activities and systems
- [ ] Identify key internal and external stakeholders involved in recovery
- [ ] Ensure the plan is accessible to authorized personnel during an outage

02 Risks and threats

- [ ] Identify threats that could disrupt critical business operations or IT services
- [ ] Assess the likelihood and potential business impact of each relevant threat
- [ ] Consider operational, financial, contractual, regulatory, and reputational consequences
- [ ] Identify significant single points of failure and existing mitigating controls
- [ ] Prioritize the risks that require prevention, mitigation or recovery measures

03 Business impact and recovery priorities

- [ ] Identify critical business functions and their IT services, data, and providers
- [ ] Assess the operational, customer, financial and compliance impact of disruption
- [ ] Establish recovery priorities based on business impact
- [ ] Identify which systems must be recovered first and which can tolerate longer outages
- [ ] Document dependencies that affect the recovery order

04 RTO, RPO, and recovery metrics

- [ ] Define an RTO for each critical service or system
- [ ] Define an RPO where data loss is relevant
- [ ] Ensure RTO and RPO values reflect actual business requirements
- [ ] Define how recovery performance will be measured during tests and real incidents
- [ ] Compare actual recovery performance with targets and address significant gaps

05 IT assets, infrastructure, and dependencies

- [ ] Maintain an inventory of the technology supporting critical business functions
- [ ] Map key apps, databases, infrastructure, networks, cloud services, and providers
- [ ] Document critical technical dependencies and single points of failure
- [ ] Record business and technical owners, hosting locations, and vendor information
- [ ] Keep architecture and dependency information aligned with production environment

06 Recovery strategy design

- [ ] Define how each critical system or service will be recovered
- [ ] Select appropriate recovery methods
- [ ] Define backup, replication, and data protection requirements
- [ ] Ensure the strategy can meet the defined RTO and RPO
- [ ] Address critical third-party dependencies and identify alternatives where necessary
- [ ] Incorporate cybersecurity requirements into the recovery strategy
- [ ] Balance the resilience provided by the strategy against its cost and complexity

07 Recovery procedures development

- [ ] Create executable recovery procedures for critical systems and services
- [ ] Define the recovery sequence, prerequisites, responsible teams, and verification steps
- [ ] Ensure recovery teams have the required access, tools, documentation, and information
- [ ] Document failover and failback procedures where applicable
- [ ] Keep procedures specific, current, and accessible during an outage
- [ ] Automate recovery activities where appropriate and safely test the automation

08 Communication and coordination plan

- [ ] Define the communication and escalation chain for a disaster
- [ ] Identify primary and backup communication channels and keep contact information current
- [ ] Define how IT, management, business teams, customers and critical vendors will be informed
- [ ] Establish who is authorized to communicate externally
- [ ] Prepare predefined messages for common disruption scenarios where useful
- [ ] Ensure recovery team members understand their roles and communication responsibilities

09 Testing, measurement, and continuous improvement

- [ ] Establish a regular DR testing schedule
- [ ] Test critical recovery procedures, backups, failover, communications, and dependencies
- [ ] Include realistic cyber incident scenarios where relevant
- [ ] Measure actual recovery performance against RTO and RPO targets
- [ ] Document test results, failures and lessons learned
- [ ] Assign owners and deadlines to corrective actions and track them to completion
- [ ] Review and update the plan after significant technology, personnel, or vendor changes

Final readiness check

- [ ] Critical business functions and IT services are identified and prioritized
- [ ] RTOs and RPOs reflect business requirements
- [ ] Critical dependencies and single points of failure are documented
- [ ] Recovery strategies and procedures have been tested
- [ ] Roles, decision-making authority and communication responsibilities are clear
- [ ] Third-party and cybersecurity risks are addressed
- [ ] Test findings and real incidents result in documented improvements
- [ ] The DR plan is maintained as a living document

Contact us

softteco.com

info@softteco.com