Rick Abraham

My Company  Dallas, TX

Risk Assessment – Backup and Recovery Risks

Contents

[Introduction 2](#_Toc182582686)

[Purpose 2](#_Toc182582687)

[Scope 2](#_Toc182582688)

[Risk Identification 2](#_Toc182582689)

[Risk Analysis 3](#_Toc182582690)

[Mitigation Recommendations 3](#_Toc182582691)

[Sensitive Data 3](#_Toc182582692)

[Network Infrastructure 3](#_Toc182582693)

[Supply Chain Operations 4](#_Toc182582694)

[Compliance Requirements 4](#_Toc182582695)

[Vendor Management Accounts 4](#_Toc182582696)

[Monitoring and Review 4](#_Toc182582697)

[Frequency 4](#_Toc182582698)

[Daily 4](#_Toc182582699)

[Monthly 4](#_Toc182582700)

[Quarterly 5](#_Toc182582701)

[Bi-Annually 5](#_Toc182582702)

[Annually 5](#_Toc182582703)

[Incident Response 5](#_Toc182582704)

[Documentation and Compliance 5](#_Toc182582705)

Risk Assessment – Backup and Recovery Risks

# Introduction

Purpose: This risk assessment identifies and evaluates risks associated with backup systems and disaster recovery processes. It addresses vulnerabilities in data integrity, availability, and protection from malware (e.g., ransomware), and provides actionable recommendations to mitigate these risks.

Scope: Includes all on-premises and cloud-based backup systems, disaster recovery plans (DRPs), and processes for data restoration and continuity.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Backup Files | Corruption or deletion by ransomware | Lack of encryption or immutability | Permanent data loss, inability to recover | High |
| Backup Systems | Failure to restore critical data during an outage | Insufficient testing of backup integrity | Operational downtime, revenue loss | High |
| Cloud Backups | Unauthorized access to cloud-stored backups | Misconfigured access controls and lack of MFA | Data breaches, compliance violations | High |
| Disaster Recovery Plans | Ineffective response to major incidents | Outdated or untested DRPs | Prolonged downtime, reputational damage | Medium |
| Backup Infrastructure | Hardware or software failure | Aging or unpatched infrastructure | Data recovery delays, additional downtime | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Backup Files | High | High | Critical |
| Backup Systems | Medium | High | High |
| Cloud Backups | Medium | High | High |
| Disaster Recovery Plans | Medium | Medium | Moderate |
| Backup Infrastructure | Medium | Medium | Moderate |

# Mitigation Recommendations

## Backup Files

* Enable **immutable storage** for backups to prevent unauthorized deletion or alteration.
* Encrypt all backup data, both in transit and at rest, using strong encryption protocols (e.g., AES-256).
* Regularly replicate backups to secure offsite locations to ensure redundancy.

## Backup Systems

* Test backup integrity and restorability monthly to ensure successful recovery in case of data loss.
* Implement **automated backup monitoring tools** to detect failures or incomplete backups.
* Ensure backup schedules align with critical recovery point objectives (RPOs).

## Cloud Backups

* Enforce **multi-factor authentication (MFA)** and restrict access to authorized personnel only.
* Use **cloud-native security tools** to monitor and secure backup environments.
* Regularly audit cloud storage permissions to prevent misconfigurations.

## Disaster Recovery Plans (DRPs)

* Review and update DRPs bi-annually to address changes in infrastructure, technology, or threat landscape.
* Conduct **tabletop exercises** to simulate disaster scenarios and refine response strategies.
* Ensure DRPs include detailed escalation paths and communication plans.

## Backup Infrastructure

* Replace aging backup hardware and software with modern, reliable solutions.
* Regularly patch backup software to protect against vulnerabilities.
* Monitor hardware performance to identify and address potential failures proactively.

# Monitoring and Review

Frequency

### Daily

* Monitor backup logs for errors, incomplete backups, or storage capacity issues.
* Validate alerts from backup monitoring tools for potential ransomware threats.

### Monthly

* Test backup restorations for critical systems to ensure data integrity and availability.
* Audit backup schedules and configurations to confirm alignment with business continuity requirements.
* Review cloud backup storage activity logs for unauthorized access or unusual patterns.

### Quarterly

* Conduct comprehensive backup audits, including file integrity checks and version history reviews.
* Evaluate the performance of backup infrastructure, identifying bottlenecks or outdated systems.
* Test DRP processes, focusing on recovery time objectives (RTOs) and identifying areas for improvement.

### Bi-Annually

* Perform ransomware resilience tests, including attempts to simulate attacks targeting backups.
* Run disaster recovery simulations, testing the organization’s ability to recover from large-scale incidents.
* Review vendor SLAs for cloud backup services to ensure compliance with uptime and security standards.

### Annually

* Reassess backup and recovery risks based on evolving threats and updates to the organization’s infrastructure.
* Update backup policies and disaster recovery procedures based on lessons learned from simulations and incidents.
* Conduct an organization-wide backup awareness campaign to educate staff on the importance of proper data storage practices.

Incident Response

* Maintain a dedicated Backup and Recovery Response Team (BRRT) to address backup failures or ransomware incidents.
* Conduct bi-annual incident response drills for scenarios involving data loss or delayed recovery.
* Document all backup-related incidents, including causes, impacts, and remediation steps, to improve future resilience.

Documentation and Compliance

* Maintain logs of backup processes, including successful restorations, errors, and anomalies.
* Document backup policies, schedules, and vendor agreements to demonstrate adherence to best practices.
* Ensure compliance with applicable regulations and standards, including:
  + NIST SP 800-53: CP-9 (Backup), CP-10 (System Recovery), and SI-12 (Data Integrity).
  + ISO 27001 and GDPR for data protection and recovery obligations.