

# Cloud Storage Threat Analysis Document Example

## 1. Introduction

This document provides an overview of the potential threats associated with cloud storage usage within the organization. It is intended to aid decision-makers and security teams in understanding and mitigating risks.

## 2. Scope

- Cloud storage providers in use (e.g., AWS S3, Google Cloud Storage, Microsoft Azure Blob Storage)
- Data types stored
- User access scenarios

## 3. Threat Analysis Table

ID	Threat	Description	Potential Impact	Mitigation
1	Data Breach	Unauthorized access to sensitive data due to misconfigured permissions or compromised accounts.	Loss of confidentiality, regulatory fines, reputational damage.	Strong access controls, encryption, regular audits.
2	Data Loss	Accidental deletion or loss of data due to software errors or insider threats.	Disruption of business operations, data unavailability.	Versioning, backups, disaster recovery planning.
3	Denial of Service (DoS)	Cloud storage services become unavailable due to attacks or provider outages.	Service downtime, loss of productivity.	Redundancy, multi-region deployment, monitoring.
4	Insecure APIs	Exploitable APIs that expose data or allow unauthorized actions.	Compromise of cloud resources, potential data exposure.	API security best practices, validation, and monitoring.
5	Insider Threats	Malicious or negligent employees accessing or sharing sensitive data.	Data exfiltration, regulatory violations.	Least privilege, monitoring, user training.

## 4. Recommendations

1. Implement strict access controls and review permissions regularly.
2. Ensure all sensitive data is encrypted at rest and in transit.
3. Enable logging and real-time monitoring for suspicious activities.
4. Regularly test disaster recovery and backup procedures.
5. Educate users about secure cloud storage practices.

## 5. Conclusion

Regular threat analysis for cloud storage ensures organizational resilience and compliance. Mitigation strategies should be continuously revised as new threats emerge and organizational usage evolves.