Cloud Data Security Risk Assessment

General Information

Project Name	_____
Assessment Date	_____
Assessed By	_____
Cloud Service Provider	_____
Environment	Production / Development / Test

Asset Identification

Asset	Description	Sensitivity
Customer Data	Personal and financial information stored in the cloud platform.	High
Application Source Code	Proprietary codebase deployed in the cloud.	Medium
System Backups	Periodic snapshots of production systems.	High

Threats & Vulnerabilities

- Unauthorized access to cloud accounts
- Data leakage via misconfigured storage
- Insecure APIs
- Insufficient access controls
- Compromised credentials
- Data loss due to lack of backup strategy

Risk Assessment Matrix

Risk	Likelihood	Impact	Risk Level	Mitigation
Account compromise via weak password policy	Medium	High	High	Enforce MFA, strong password policies
Data breach from public storage buckets	Low	High	Medium	Regular configuration audits, restrict access
Loss of data due to accidental deletion	Low	Medium	Low	Implement regular, automated backups

Recommendations

- Implement identity and access management (IAM) best practices
- Enable multi-factor authentication (MFA) for all accounts
- Encrypt data at rest and in transit
- Regularly review cloud configurations and permissions

- Maintain up-to-date backups in separate regions

Approval

Name	_____
Date	_____
Signature	_____