1. Executive Summary

This risk assessment report evaluates the cybersecurity risks associated with PiggyCo's cloud infrastructure. The assessment identifies key risks, their potential impact, and recommends mitigation strategies to enhance PiggyCo's cybersecurity posture.

2. Scope

The scope of this risk assessment includes PiggyCo's web and mobile applications, cloud environment and cloud data storage systems. The assessment covers potential risks related to data breaches, unauthorized access, system vulnerabilities, and compliance with regulatory requirements.

3. Methodology

The risk assessment was conducted using a combination of qualitative and quantitative methods, including:

- Interviews with key stakeholders and IT personnel.
- Review of existing documentation and cybersecurity policies.
- Vulnerability scanning and penetration testing.
- Risk analysis based on likelihood and impact.
- Framework used: NIST RMF

4. Risk Findings

Table 1: Key Risk Findings and Mitigations

Risk ID	Description	Likelihood	Impact	Mitigation
AR-001	Outdated virtual machines and applications may introduce security vulnerabilities.	High	Moderate	Automate patch management with Azure Update Management and perform monthly security reviews.
AR-002	Web and mobile applications rely on APIs that may be vulnerable to attacks like API abuse or injection attacks.	Medium	High	Implement OAuth 2.0 and OpenID Connect for secure API authentication.

Risk ID	Description	Likelihood	Impact	Mitigation
AR-003	Misconfigured cloud storage, databases, or identity settings may expose customer data to the public.	High	Severe	Enable encryption at rest and in transit for all data storage systems.
AR-004	Failure to comply with GDPR, PCI-DSS, or NIST CSF could result in legal penalties and reputational damage.	Medium	High	Maintain audit logs and compliance reports in Azure Compliance Manager.
AR-005	Employees or third-party contractors may unintentionally or maliciously expose sensitive data.	Medium	Moderate	Enable logging and monitoring in Azure Sentinel for suspicious activity. Conduct security awareness training for all employees
AR-006	Azure-hosted services may be disrupted due to Distributed Denial-of-Service (DDoS) attacks.	Medium	High	Deploy Azure DDoS Protection Standard, and implement Web Application Firewall

5. Conclusion & Recommendations

Based on this assessment, PiggyCo should prioritize the following actions:

- Strengthening Identity and Access Management (IAM) by enforcing MFA and RBAC.
- Implement encryption and private endpoints for all cloud storage.
- Deploy Azure DDoS Protection Standard to safeguard against service disruptions.
- Conduct regular security awareness training to mitigate insider threats.
- Maintain compliance with GDPR, PCI-DSS, and NIST through continuous monitoring.

- Ensure high availability by using multi-region deployments and failover strategies.
- Automate patch management to address security vulnerabilities.

6. Action Items

- Assign risk owners for each identified risk.
- Develop an implementation timeline for mitigation strategies.
- Conduct periodic security assessments and update risk findings accordingly.
- Monitor compliance and security metrics using Azure Security Center and Azure Sentinel.

By implementing these mitigations, PiggyCo can enhance its cloud security posture and reduce risks associated with its Azure environment.

Prepared by: Abi Adeniji

Date: January 25, 2025