Title: ZenFinTech Ltd – AWS S3 Security Advisory Report
Date: June 2025
Prepared By: Lambert Agbeehia – Cybersecurity & GRC Consultant

---

📌 Executive Summary

This report provides a focused assessment of Amazon S3 usage at ZenFinTech Ltd. It identifies high-priority risks associated with insecure storage configurations and outlines specific security mitigations aligned with ISO 27001:2022 and the NIST Cybersecurity Framework (CSF). These mitigations are designed to prevent data breaches, improve audit readiness, and harden our cloud posture.

🔍 Key Risks Identified

Risk	Description	Likelihood	Impact	Rating
R1	Public access to S3 buckets	High	Severe	**High**
R2	Lack of encryption on sensitive files	Medium	High	**High**
R3	Misconfigured permissions (ACLs & IAM)	Medium	Medium	**Medium**
R4	Inadequate monitoring or alerting	Medium	Medium	**Medium**

✅ Recommended Mitigations

1. Enforce Bucket Privacy and Access Policies

- Enable **Block Public Access** for all S3 buckets
- Use **IAM policies with least privilege**; avoid use of wildcards (*)
- Deny public uploads via SCPs or bucket policies
- Review bucket access via AWS Config rules

🔗 **ISO 27001 Mapping**: A.5.15, A.5.23
🔗 **NIST Mapping**: PR.AC-4, PR.AC-6

---

2. Enforce Default Encryption (SSE-KMS)

- Enable **Server-Side Encryption with AWS KMS (SSE-KMS)** by default
- Use bucket policies to reject unencrypted uploads
- Rotate encryption keys on a 12-month schedule

🔗 **ISO 27001 Mapping**: A.8.10
🔗 **NIST Mapping**: PR.DS-1, PR.DS-2

📊 *3. Implement Logging, Alerts, and Monitoring*

- Enable **CloudTrail + S3 access logs** for all buckets
- Use **AWS Config + Security Hub** for real-time misconfiguration alerts
- Set up SNS alerts for policy changes, failed access attempts, or uploads to public buckets

📎 **ISO 27001 Mapping**: A.8.16
📎 **NIST Mapping**: DE.CM-7, DE.CM-8

🔄 *4. Define Lifecycle and Versioning Policies*

- Enable **versioning** to prevent loss from overwrite/deletion
- Apply **lifecycle policies** to transition old data to Glacier or auto-delete logs
- Enforce minimum retention periods for logs and backups

📎 **ISO 27001 Mapping**: A.5.10, A.8.14
📎 **NIST Mapping**: PR.IP-6, PR.DS-5

📝 *5. Conduct Quarterly Cloud Risk Reviews*

- Create an automated review checklist (bucket policy, encryption, logs)
- Include S3 posture in internal audit scope
- Maintain records of changes for ISO 27001 audit trail

📎 **ISO 27001 Mapping**: A.9.2 (ISMS audit), A.5.31
📎 **NIST Mapping**: ID.RA-1, ID.RA-3

🧩 Implementation Priority

Mitigation	Impact	Effort	Priority
Enforce bucket privacy	High	Low	✅ Now
Enable SSE-KMS	High	Medium	✅ Now
Add monitoring/alerts	Medium	Medium	🔜 Next
Define lifecycle policies	Medium	Low	🔜 Next
Schedule cloud risk reviews	Medium	Low	🔄 Ongoing

📎 Final Notes

Failure to enforce these mitigations can result in:

- Regulatory non-compliance (GDPR, ISO 27001 clause 5.23)

- Financial and reputational damage
- Failed audits or vendor due diligence reviews

📌 **Prepared by**:
Lambert Agbeehia
Cybersecurity & GRC Consultant
lambmeister7@gmail.com
