FinBank Ltd — Risk Assessment Report

Scope & Scenario

Industry: Financial Services (UK-based fintech handling payment data)  
Size: ~200 employees, cloud-first (AWS/Azure), customer portal + mobile app  
Regulatory Scope: GDPR + PCI DSS + ISO/IEC 27001  
Assessment Date: 2025-09-09

# 1. Executive Summary

This assessment identified key risks to FinBank Ltd's customer data, cloud infrastructure, user endpoints, and third-party dependencies. High risks primarily relate to credential theft (MFA coverage), web application security, and vendor risk management.

# 2. Methodology

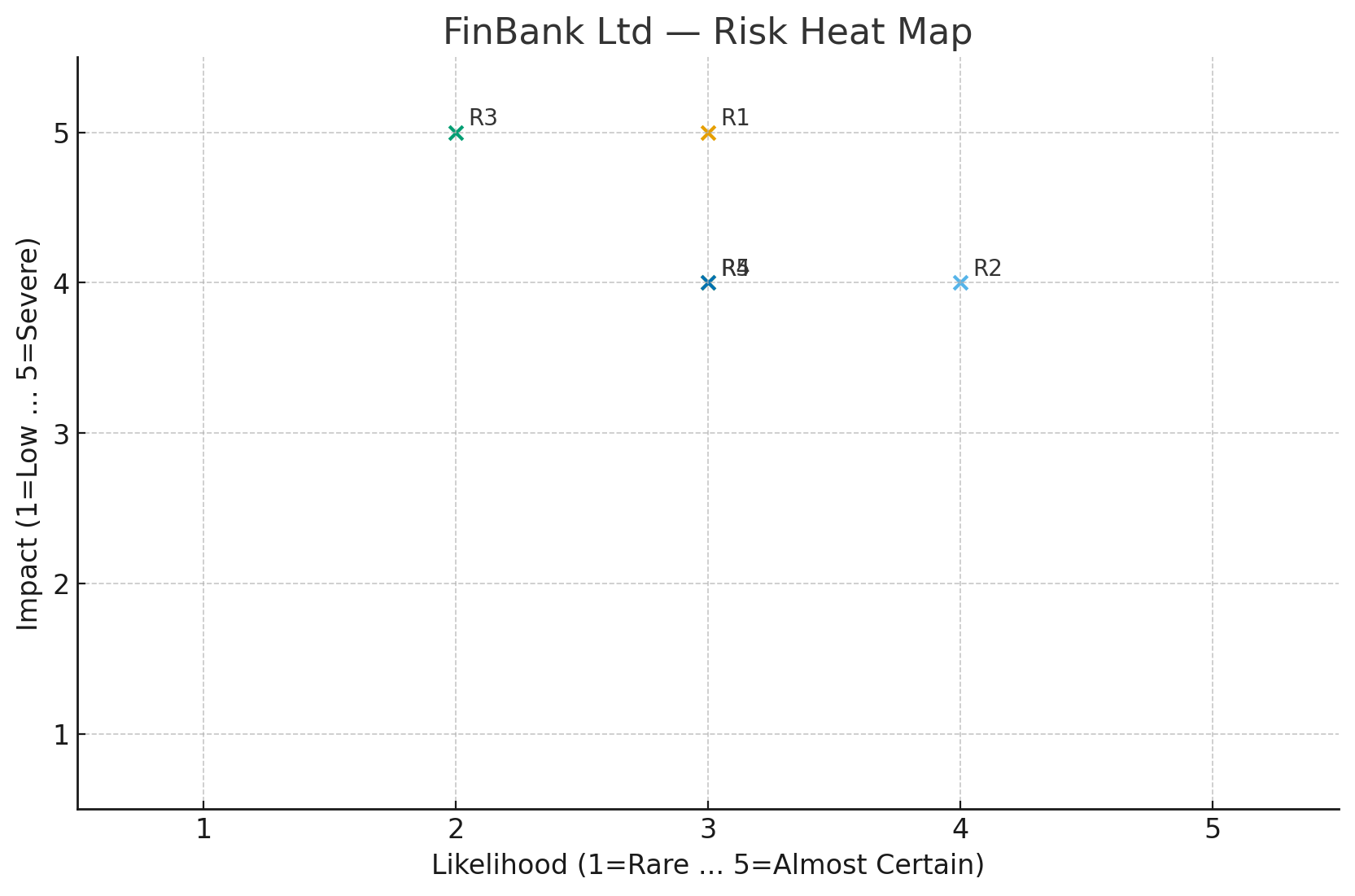
Assessment aligned with ISO/IEC 27005 and NIST RMF principles. Risks were identified via workshops, document review, and limited technical validation. Impact and likelihood were rated on a 1–5 scale; **risk score = impact × likelihood**. Risk categories: Low (≤5), Medium (6–11), High (≥12).

# 3. Risk Register (Summary)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk ID | Asset/Process | Threat | Vulnerability | Risk Score | Inherent Risk |
| R1 | Customer Payment Data (Web App DB) | SQL Injection | Insufficient input validation / parameterization | 15 | High |
| R2 | Employee Laptops (Workstations) | Credential Theft / Phishing | Weak password policy; limited MFA coverage | 16 | High |
| R3 | Cloud Storage (S3/Blob) | Data Leakage / Misconfiguration | Public access not blocked by default; missing encryption-at-rest tag | 10 | Medium |
| R4 | Third-Party Payment Processor | Vendor Breach / Outage | Limited due diligence; no formal SLA review cadence | 12 | High |
| R5 | Privacy / Data Subject Requests (DSAR) | Regulatory Non-Compliance (GDPR) | No formal DSAR workflow or tracking SLA | 12 | High |

# 4. Risk Treatment Plan

* Implement organization-wide MFA for all users and admins; complete rollout by 2025-10-15.
* Deploy WAF with tuned rules and enforce parameterized queries; schedule quarterly web app pentests.
* Enforce cloud guardrails: block public access on storage, encryption-at-rest mandatory.
* Formalize vendor risk management program; define annual due diligence cadence and SLAs.
* Implement GDPR DSAR workflow with SLAs and evidence tracking.



# 5. Conclusion

Applying the above treatments is expected to reduce high risks to medium/low within the next two quarters. Residual risks should be monitored via KPIs/KRIs and reviewed quarterly by the risk committee.