**📑 Risk Treatment Report (RTR)**

**Organization:** ABC Bank Ltd.  
**Project Title:** ISO/IEC 27001:2022 Certification Program  
**Version:** 1.0  
**Date:** [Insert Date]  
**Owner:** CISO

**1. Purpose**

This document defines the treatment approach for risks identified in the Risk Assessment Report, including treatment options, control selection, owners, and timelines.

**2. Treatment Options (per ISO 27001:2022)**

* **Mitigate:** Implement controls to reduce risk.
* **Avoid:** Stop the activity causing risk.
* **Transfer:** Outsource/share risk (e.g., insurance, vendor SLA).
* **Accept:** Formally acknowledge risk if within tolerance.

**3. Risk Treatment Table**

| **Risk ID** | **Risk Description** | **Risk Score** | **Treatment Option** | **Control (Annex A Ref)** | **Risk Owner** | **Timeline** | **Residual Risk** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R1 | Unpatched legacy CBS modules vulnerable to ransomware | 20 (Critical) | Mitigate | A.8.9 Configuration Mgmt, A.8.15 Vulnerability Mgmt | CIO | 3 months | Medium |
| R2 | Phishing risk on Internet Banking | 20 (Critical) | Mitigate | A.5.10 Identity Mgmt, A.6.3 Awareness Training | CISO | 2 months | Low |
| R3 | Vendor cloud data breach due to weak SLA | 15 (High) | Transfer & Mitigate | A.5.20 Supplier Security, A.5.23 Supplier Agreements | Head of Compliance | 4 months | Medium |
| R4 | Weak API security in Mobile App | 15 (High) | Mitigate | A.8.25 Secure Coding, A.8.27 Security Testing | Head of IT Apps | 3 months | Low |
| R5 | ATM fraud from weak monitoring | 12 (Medium) | Mitigate | A.8.16 Monitoring, A.5.30 Fraud Detection | ATM Ops Manager | 6 months | Low |
| R6 | Insider threat from excess HR access | 12 (Medium) | Mitigate | A.5.18 Access Mgmt, A.6.7 Disciplinary Process | HR Head | 2 months | Low |
| R7 | SOC over-reliance on manual logs | 10 (Medium) | Mitigate | A.8.16 Monitoring, A.8.23 SIEM Use Cases | SOC Lead | 5 months | Low |
| R8 | DC outage due to poor UPS redundancy | 8 (Medium) | Mitigate | A.7.11 Power Supply, A.7.12 Equipment Redundancy | Facilities Manager | 6 months | Low |

**4. Approval**

Approved by: CIO, CISO, COO  
Date: [Insert Date]