# Risk Scoring Method and Appetite

## 1. Risk Scoring Model

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Likelihood (1–5) | Description | Impact (1–5) | Description | Risk Score (L×I) | Risk Level | Treatment Strategy |
| 1 | Rare | 1 | Negligible | 1–5 | Low | Accept / Monitor |
| 2 | Unlikely | 2 | Minor | 6–10 | Medium | Mitigate |
| 3 | Possible | 3 | Moderate | 11–15 | High | Mitigate / Escalate |
| 4 | Likely | 4 | Major | 16–20 | High | Escalate / Prioritize |
| 5 | Almost Certain | 5 | Severe | 21–25 | Critical | Immediate Action / Report |

## 2. Risk Appetite Statement

ShopNimbus maintains a low risk appetite for confidentiality and integrity breaches, a medium appetite for controlled operational disruptions (availability), and a zero-tolerance policy for non-compliance with PCI DSS, GDPR, or NIST CSF control failures.

## 3. Evaluation Cadence

|  |  |  |  |
| --- | --- | --- | --- |
| Review Type | Frequency | Responsible Role | Notes |
| Risk Register Update | Monthly | Security Lead | Reflects new SCC findings and mitigations |
| Control Effectiveness Test | Quarterly | IAM / Network Engineer | Logs reviewed and tested against thresholds |
| Executive Risk Review | Biannually | Project Sponsor | Summarizes key risks and residual exposure |