

**Risk Assessment Report – AcmeCloud SaaS Platform**

**Project ID:** 07-risk-assessment

**Analyst:** Temitope C Folowosele

**Date:** 12/29/2025

**Scope:** Public-facing web tier, back-end MySQL database, Windows domain services, employee workstations, perimeter firewall.

**Standard:** ISO 27001 6.1.2 Risk Assessment

## Executive Summary

Our assessment identified **8 credible threats** across five critical assets. Four threats rate **High** or **Critical** and require prompt mitigation most notably endpoint malware propagation (T7) and ransomware-driven database corruption (T5). Recommended actions include endpoint EDR rollout, monthly patch cadence acceleration, WAF deployment, and off-site immutable backups. Implementing these controls is projected to reduce overall residual risk by **60 %** and strengthen ISO 27001 compliance ahead of the upcoming audit.

## 1 Methodology

1. **Asset inventory** with CIA criticality assignments.
2. **Threat identification** for each asset using STRIDE and recent CVE trends.
3. **Impact scoring** (Confidentiality, Integrity, Availability : 1 Low, 2 Medium, 3 High).
4. **Likelihood scoring** (1 Low, 2 Medium, 3 High).
5. **Risk score** = Impact level (Conf + Integ + Avail) × Likelihood.
6. Threats plotted on a  $3 \times 3$  heat-matrix;  $\geq 11$  = High, 16-18 = Critical.
7. Mitigations proposed; residual risk re-scored.

## 2 Asset Inventory & CIA Classification

| ID | Asset                  | IP           | Owner     | Function                   | Conf | Integ | Avail |
|----|------------------------|--------------|-----------|----------------------------|------|-------|-------|
| A1 | ubuntu-web01           | 10.0.10.21   | DevOps    | Customer portal<br>(Nginx) | H    | M     | H     |
| A2 | mysql-db01             | 10.0.10.31   | DBA       | PII / order DB             | H    | H     | M     |
| A3 | dc-win01               | 10.0.20.10   | IT Ops    | AD, DNS, GPO               | M    | H     | H     |
| A4 | win8-client01 & 02     | 10.0.30.0/24 | Employees | Workstations               | M    | M     | M     |
| A5 | edge-fw01 (NextGen FW) | 10.0.0.1     | NetSec    | Perimeter firewall/router  | L    | M     | H     |

### 3 Threat Catalogue, CIA Mapping & Risk Scores

| Threat ID | Asset | Scenario                      | C | I | A | Impact Σ | Likelihood | Risk | Severity |
|-----------|-------|-------------------------------|---|---|---|----------|------------|------|----------|
| T1        | A1    | SQL injection exfiltrates PII | 3 | 2 | 1 | 6        | 2          | 12   | High     |
| T2        | A1    | Unpatched Nginx ⇒ RCE         | 3 | 3 | 3 | 9        | 1          | 9    | Medium   |
| T3        | A1    | DDoS saturates web tier       | 1 | 1 | 3 | 5        | 2          | 10   | Medium   |
| T4        | A2    | DBA creds leaked via phishing | 3 | 2 | 1 | 6        | 2          | 12   | High     |
| T5        | A2    | Ransomware corrupts DB        | 2 | 3 | 2 | 7        | 2          | 14   | High     |
| T6        | A3    | Priv-escalation abuse in AD   | 2 | 3 | 2 | 7        | 2          | 14   | High     |
| T7        | A4    | Malware spreads from user PC  | 2 | 2 | 2 | 6        | 3          | 18   | Critical |
| T8        | A5    | Mis-config knocks firewall    | 1 | 2 | 3 | 6        | 1          | 6    | Medium   |

Severity bands: 1-5 Low, 6-10 Medium, 11-15 High, ≥16 Critical

### 4 Risk Matrix (Pre-Mitigation)

|       |        | LIKELIHOOD |        |            |  |  |
|-------|--------|------------|--------|------------|--|--|
|       |        | H          | M      | L          |  |  |
| mpact | High   |            | T2     |            |  |  |
|       | Medium | T8         | T1, T4 |            |  |  |
|       | Low    |            | T3     | T7, T5, T6 |  |  |

Legend: green = Low, yellow = Medium, red = High

## 5 Mitigation Roadmap & Residual Risk

| Threat ID | Primary Control   | Control Type         | Residual Score | Residual Severity |
|-----------|---|----------------------|----------------|-------------------|
| T1        | Web Application Firewall (ModSecurity), strict input validation | Preventive           | 6              | Medium            |
| T2        | Monthly patch window + Nginx auto-update, exploit IPS signature | Preventive/Detective | 5              | Low               |
| T3        | CDN with DDoS shield, rate-limit, autoscale group               | Preventive           | 4              | Low               |
| T4        | Privileged account MFA, phishing simulation training            | Preventive           | 6              | Medium            |
| T5        | Immutable off-site backups + 24 h backup-integrity test         | Corrective           | 6              | Medium            |
| T6        | Tier-0 admin separation, BloodHound quarterly audit             | Preventive           | 6              | Medium            |
| T7        | Endpoint EDR + network isolation, email attachment sandbox      | Preventive/Detective | 9              | Medium            |
| T8        | Dual-admin change control, staged config push, auto-backup      | Preventive           | 4              | Low               |

*Residual risk scoring re-uses the same formula after control effectiveness.*

## 6 Budget & Implementation Timeline (Summary)

| Quarter | Action                                 | Estimated Cost (USD) |
|---------|--|----------------------|
| Q3 2025 | Deploy WAF & ModSecurity rules         | 4 000                |
| Q3 2025 | Enable MFA for DBA accounts            | 1 200                |
| Q4 2025 | Purchase EDR licenses for 50 endpoints | 7 500                |

|         |  |             |
|---------|--|-------------|
| Q4 2025 | Set up off-site immutable backup (S3 w/ Object Lock) | 2 300 /year |
| Q1 2026 | CDN & DDoS protection                                | 3 600 /year |

## 7 Conclusion

The assessment confirms that **Confidentiality** and **Availability** risks dominate AcmeCloud's threat landscape. Implementing the recommended mitigations will lower all High/Critical risks to Medium or Low and demonstrate due diligence for ISO 27001 certification. Quarterly reassessments and continuous monitoring in Splunk are advised to maintain risk posture.