Risk Assessment Report – AcmeCloud SaaS Platform

Project: Risk Assessment

Analyst: Dayo Sonibare

Date: 6 August 2025

Scope: Public-Facing Web Tier, Back-End MySQL Database, Windows Domain Services, Employee Workstations.

Standard: ISO 27001 6.1.2 Risk Assessment

Executive Summary

Our assessment identified **13 credible threats** across six critical assets. Five threats rate **High** or **Critical** and require prompt mitigation most notably endpoint malware propagation (T1 A4) and unsupported Windows OS (T1 A5). Recommended actions include endpoint EDR rollout, monthly patch cadence acceleration, WAF deployment, and upgrade to a supported service pack or operating system. Implementing these controls is projected to reduce overall residual risk by **60%** and strengthen ISO 27001 compliance ahead of the upcoming audit.

1. Methodology

I. **Asset Inventory** with CIA criticality assignments.
II. **Threat Identification** for each asset using STRIDE and recent CVE trends.
III. **Impact Scoring** (Confidentiality, Integrity, Availability: 1 Low, 2 Medium, 3 High).
IV. **Likelihood Scoring** (1 Low, 2 Medium, 3 High).
V. **Risk Score** = Impact level (C+I+A) x Likelihood.
VI. **Threat plotted on a 3 x 3 heat-matrix**: ≥11 = High, ≥16 = Critical.
VII. **Mitigation proposed:** Residual risk re-scored

2. Asset Inventory & CIA Classification

ID	Asset	IP Address	Owner	Function	Conf	Int	Avail
A1	ubuntu-web server 01	10.0.5.13	DevOps	Host Customer portal	H	M	H
A2	mysql-dc01 (kali Linux)	10.0.5.9	DBA	PII storage, Order DB	H	H	M
A3	DC-Win Server 01	10.0.5.10	IT Ops	AD, DNS, GPO	M	H	H
A4	Windows 10	10.0.5.12	Employee	Workstation	M	M	M
A5	Windows 8	10.0.5.8	Employee	Workstation	M	M	M
A6	Web App	Halisans.com	CI	Customer Interface	H	H	H

3. Threat Catalogue, CIA Mapping & Risk Scores

Asset: Ubuntu-Server

Threat ID	Asset	Scenario	C	I	A	Impact	Likelihood	Risk Level	Severity
T1	A1	SQL injection exfiltrate 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	A1	ICMP Timestamp Request Remote Date Disclosure	1	0	0	1	3	3	Low

Asset: Kali Linux

Threat ID	Asset	Scenario	C	I	A	Impact	Likelihood	Risk Level	Severity
T5	A2	SQLite 3.44.0 < 3.49.1 Multiple Vulnerabilities	1	1	1	3	2	6	Medium
T6	A2	SQLite < 3.50.2 Memory Corruption	1	3	1	5	1	5	Low
T7	A2	SSL Certificate Cannot Be Trusted	1	1	0	2	3	6	Medium

Asset: DC - Windows Server

Threat ID	Asset	Scenario	C	I	A	Impact	Likelihood	Risk Level	Severity
T8	A3	Priv-escalation abuse in AD	2	3	2	7	2	14	High

Asset: Windows 10

Threat ID	Asset	Scenario	C	I	A	Impact	Likelihood	Risk Level	Severity
T9	A4	Malware spreads from user PC	2	2	2	6	3	18	Critical

Asset: Windows 8

Threat ID	Asset	Scenario	C	I	A	Impact	Likelihood	Risk Level	Severity
T10	A5	Unsupported Windows OS (Remote)	3	3	3	9	3	27	Critical
T11	A5	MS17-010: Security Update for Microsoft Windows SMB Server	3	3	3	9	2	18	Critical
T12	A5	SMB Signing not required	0	1	0	1	2	2	Low

Asset: Web Application

Threat ID	Asset	Scenario	C	I	A	Impact	Likelihood	Risk Level	Severity
T13	A6	HSTS Missing from HTTPS Server (RFC 6796)	1	1	0	2	3	6	Medium

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

4. Risk Matrix (Pre-Mitigation)

LIKELIHOOD				
		High	Medium	Low
IMPACT	High	T10	T8, T11	T2
	Medium	T9	T1, T3	T6
	Low	T4, T13, T7	T5, T12	

Legend: Green = Low, Yellow = Medium, Red = High

Note: Low risk = 1 to 3, Medium risk = 4 to 6, High risk = 7 to 10

5. Mitigation Roadmap & Residual Risk

Threat ID	Primary Control	Control Type
T1	Web Application Firewall (ModSecurity), strict input validation	Preventive
T2	Monthly patch window + Nginx auto-update, exploit IPS signature	Preventive/Detective
T3	CDN with DDoS shield, rate-limit, autoscale group	Preventive
T4	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14)	Preventive
T5	Upgrade to SQLite 3.49.1 or later	Preventive
T6	Upgrade to SQLite 3.50.2 or later	Preventive
T7	Purchase or generate a proper SSL certificate for this service	Corrective

T8	Tier-0 admin separation, BloodHound quarterly audit	Preventive
T9	Endpoint EDR + network isolation, email attachment sandbox	Preventive/Detective
T10	Upgrade to a supported service pack or operating system.	Preventive
T11	Microsoft has released a set of patches for Windows 8. Microsoft has also released emergency patches for Windows operating systems that are no longer supported.	Preventive
T12	Enforce message signing in the host's configuration.	Preventive
T13	Configure the remote web server to use HSTS	Preventive

Residual risk scoring uses the same formula after control effectiveness.

6. 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.