BeelzTech ISO 27001 Risk Assessment – Risk-Matrix Report

Prepared by: Biliaminu Biola Salawu (Cybersecurity Analyst)
Scope/Context: BeelzTech, a mid-size SaaS company that processes customer PII via a web portal hosted on an Ubuntu web server with a back-end MySQL database. An upcoming ISO 27001 audit requires a formal risk assessment.

---

1. Define Scope

The scope of this risk assessment covers all assets directly supporting the PII-processing SaaS platform:

- The public web portal used by customers
- The Ubuntu web server hosting the portal
- The back-end MySQL database storing customer PII
- Supporting infrastructure components directly involved in processing, transmitting, or storing PII (OS, web server software, DBMS)

Out of scope: Corporate endpoints, HR systems, marketing sites, and any systems that do not process or store customer PII.

The assessment objective is to identify, analyse, and prioritize information-security risks to Confidentiality, Integrity, and Availability (CIA) of customer PII and to provide input to ISO 27001 risk treatment.

---

2. Asset Inventory & Classification

Using Excel, the following logical asset inventory was created and classified according to information criticality.

Asset ID	Asset Name	Description	Owner	Data Type Processed	Classification
A1	Customer Web Portal	Public SaaS web application	IT / Product	Customer PII (in transit)	High
A2	Ubuntu Web Server	OS + web server (e.g., Apache/Nginx, PHP)	IT Operations	App code, session data	High
A3	MySQL Database Server	Relational DB storing customer PII at rest	DBA / IT	Customer PII (at rest)	Very High
A4	Network Interfaces / Firewall Rules	Inbound/outbound connectivity to portal & DB	Network Team	Traffic to A1–A3	High

Classification is aligned to ISO 27001 information-classification guidance (e.g., Public, Internal, Confidential, Restricted).
Customer PII is treated as **Restricted/Very High**.

---

3. Vulnerability Assessment (Tools: Nessus + CVSS Calculator)

A Nessus vulnerability scan was performed on all in-scope hosts (A1–A3). Key illustrative results:

Asset	Example Vulnerability	Nessus Severity	CVSS (Base)
A2	Outdated OpenSSL library (remote code execution)	Critical	9.8
A2	Missing security headers on web server	Medium	5.6
A3	MySQL misconfiguration (weak default settings)	High	8.0
A3	Unencrypted database backups	High	7.5

Asset	Example Vulnerability	Nessus Severity	CVSS (Base)
A1	Reflected XSS in search parameter	Medium	6.1

All findings were validated and consolidated into an Excel tracking sheet, with CVSS scores imported or calculated via the CVSS calculator.

---

4. Threat Identification & CIA Impact Mapping

For each significant vulnerability, plausible threat scenarios and CIA impact on PII were mapped.

Examples:

1. **Threat Scenario T1: External attacker exploits outdated OpenSSL on Ubuntu web server (A2) to gain remote code execution.**
   - **Confidentiality**: Very High impact – attacker could access MySQL credentials and PII.
   - **Integrity**: High impact – attacker could alter application logic or database data.
   - **Availability**: High impact – system compromise could result in outage.
2. **Threat Scenario T2: Exploitation of MySQL misconfiguration (A3) leading to unauthorized DB access.**
   - **Confidentiality**: Very High – mass disclosure of PII.
   - **Integrity**: High – unauthorized modification of records.
   - **Availability**: Medium – possible service degradation.
3. **Threat Scenario T3: Reflected XSS in web portal (A1) used to steal customer sessions.**
   - **Confidentiality**: Medium – limited to affected user sessions, not full DB.
   - **Integrity**: Medium – attacker may perform actions as user.
   - **Availability**: Low – platform remains online.
4. **Threat Scenario T4: Unencrypted database backups exfiltrated from storage.**
   - **Confidentiality**: Very High – full historical PII leak.
   - **Integrity**: Low – backup copies, not live DB.
   - **Availability**: Medium – possible ransom / deletion of backups.

---

5. Likelihood and Impact Estimation

A 5-point qualitative scale was adopted in Excel:

- **Likelihood**: 1 (Rare), 2 (Unlikely), 3 (Possible), 4 (Likely), 5 (Almost Certain)
- **Impact** (on CIA for overall business): 1 (Negligible) – 5 (Severe)

Estimated ratings (informed by CVSS score, exposure, and existing controls):

Threat Scenario	Likelihood	Impact	Justification (summary)
T1 – OpenSSL RCE on A2	4	5	Internet-facing, known exploits, critical CVSS, high data value.
T2 – MySQL misconfiguration	3	5	Requires some access but exposes full PII if compromised.
T3 – Reflected XSS	3	3	Common attack, but scope limited to user sessions.
T4 – Unencrypted backups	3	5	Access path less exposed than live DB, but full data if breached.

6. Risk Score Calculation (L × I – RA)

Using the standard multiplicative method:

Risk Score = Likelihood × Impact

Threat Scenario	Likelihood (L)	Impact (I)	Inherent Risk Score (L×I)
T1	4	5	20
T2	3	5	15
T3	3	3	9
T4	3	5	15

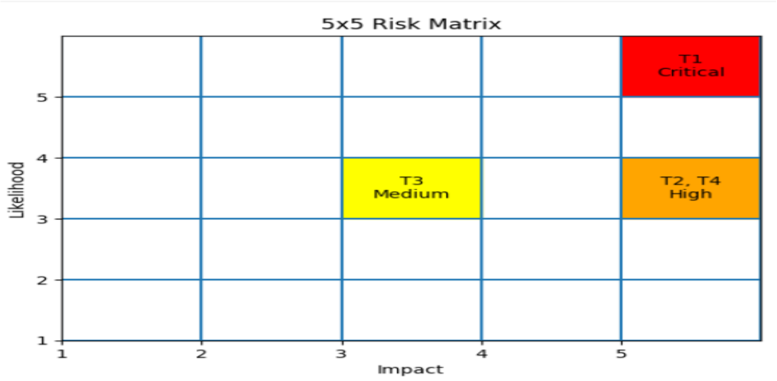
Example scale:

- 20–25: Critical
- 12–19: High
- 6–11: Medium
- 1–5: Low

Using this, T1 is **Critical**, T2 and T4 are **High**, T3 is **Medium**.

(“RA” – risk after treatment – is calculated again in Step 8.)

7. Build the Risk Matrix



A 5×5 likelihood/impact matrix was built in Excel; key risks are plotted as follows:

Rows: Likelihood (1–5)
Columns: Impact (1–5)

- Cell (4,5) – Critical (red): **T1 – OpenSSL RCE on Ubuntu web server**
- Cell (3,5) – High (orange): **T2 – MySQL misconfig**, **T4 – Unencrypted backups**
- Cell (3,3) – Medium (yellow): **T3 – Reflected XSS**

This graphical matrix provides leadership with a clear visual of where risk is concentrated: primarily around the web server stack and database/backup configuration.

8. Mitigation & Residual Risk

For each major risk, specific treatment actions were defined, and residual risk was re-scored assuming completion of controls.

Threat	**Key Mitigation Measures**	**Likelihood**	**Impact**	**Score**	**Risk Level**
T1 – OpenSSL RCE on A2	Patch/upgrade OpenSSL; enable automatic security updates; restrict admin access; implement Web Application Firewall (WAF); harden SSH.	2	5	10	Medium
T2 – MySQL Misconfiguration	Apply secure configuration baseline; enforce strong authentication; restrict DB network access to web server only; enable encryption in transit; regular config reviews.	2	5	10	Medium
T3 – Reflected XSS on A1	Fix vulnerable code; apply input validation and output encoding; add security headers (CSP, X-XSS-Protection where applicable); integrate SAST/DAST into SDLC.	2	3	6	Medium
T4 – Unencrypted Backups	Encrypt backups at rest and in transit; limit backup access; implement key management; test restore to confirm integrity; apply off-site secure storage.	2	5	10	Medium

After treatment, all previously Critical/High risks are reduced to **Medium** or lower. Management acceptance is required for any remaining medium risks, consistent with BeelzTech and ISO 27001's risk-acceptance criteria.

Conclusion and Recommendations

- The most significant inherent risk was the exposure of the Ubuntu web server and MySQL database, which could lead to large-scale PII compromise.
- Implementing the outlined patching, hardening, encryption, and secure-development controls substantially reduces these risks.
- It is recommended that leadership:
    1. Approve the proposed remediation plan and allocate necessary resources.
    2. Formally accept the residual medium risks or request further treatment.
    3. Require ongoing vulnerability scanning (Nessus), annual risk reviews, and integration of risk results into the ISO 27001 ISMS.

This report, along with the detailed Excel risk register, Nessus scan outputs, and CVSS calculations, provides the evidence base needed for the upcoming ISO 27001 audit.