Internal Security Audit Report

TechConsult S.A.

Prepared by: Wael Rezgui
Date: August 4, 2025

1. Purpose of the Audit

This audit evaluates the effectiveness of TechConsult S.A.'s information security controls and determines compliance with ISO/IEC 27001:2022. It is a simulated internal audit for portfolio demonstration purposes.

2. Audit Objectives

- Assess compliance with selected ISO/IEC 27001:2022 controls
- Identify non-compliant or weak areas
- Recommend improvements
- Simulate real-world audit reporting

3. Audit Scope

Area	Description
Access Control	Review of user accounts, passwords, and role-based permissions
Network Security	Firewall configurations, VPN access, Wi-Fi protection
Asset Management	Inventory of laptops, servers, and data classification
Physical Security	Badge access, surveillance, device locking
Backup & Recovery	Backup frequency, restoration procedures
Security Awareness	Training sessions, phishing simulations
Incident Response	Processes to handle breaches, attack simulation

4. Audit Criteria

- ISO/IEC 27001:2022 – Annex A controls
- CIS Controls v8 (as support reference)

5. Methodology

- Document review: policies, simulated logs, procedures
- Simulated interviews with IT/security (fictional data)
- Compliance checklist (Yes/Partial/No)

- Risk scoring for each domain

6. Tools Used

- Microsoft Excel: Compliance checklist and scoring
- Microsoft Word: Report documentation

7. Audit Team

Name	Role
Wael Rezgui	Lead Auditor (Simulated)

8. Timeline

Phase	Dates
Planning	August 4, 2025
Checklist Evaluation	August 5–6, 2025
Report Drafting	August 7–8, 2025
Portfolio Finalization	August 9, 2025

9. Simulated Checklist Summary

Control Area	Status	Comments
Access Control	Partial	Some admin accounts lack MFA
Network Security	Yes	Firewall rules up-to-date
Asset Management	Yes	Inventory tool in use
Physical Security	Yes	Access logs reviewed regularly
Backup & Recovery	Partial	Backup tested quarterly, not monthly
Security Awareness	No	No simulated phishing in last year
Incident Response	Partial	Process documented, not tested recently

Table 1: Compliance Checklist Result Summary

10. Risk Summary Table

Domain	Risk Level	Key Issue
Access Control	Medium	Incomplete MFA coverage
Security Awareness	High	No recent phishing simulations
Backup & Recovery	Medium	Lack of frequent testing
Incident Response	Medium	Plan not recently validated

11. Recommendations

- Enforce MFA for all privileged accounts
- Launch mandatory phishing awareness campaign
- Increase backup test frequency to monthly
- Conduct an incident response tabletop exercise

12. Conclusion

Based on the simulated audit, TechConsult S.A. demonstrates moderate compliance with ISO 27001. Key technical safeguards are in place, but human-centric areas like awareness and readiness need improvement. With action on these recommendations, overall posture would shift to "Low Risk."