Unit 6: Security Standards

Which standards apply to the organization in the assessment?

(i) GDPR — applies if the organization processes personal data of EU/EEA residents or is EU-based. (ICO Guide to GDPR).
(ii) PCI-DSS — applies if the organization accepts, processes, stores or transmits cardholder data (online payments). (PCI Security Standards Council).
(iii) HIPAA — applies if the organization is a UAE. covered entity or business associate handling protected health information (PHI).
(iv) ISO/IEC 27001 / 27701 — widely applicable standards for information security management and privacy information management; useful as an overarching control framework.

How to evaluate the company against the appropriate

(i) **Scoping & Documentation:** Confirm data types, data flows, processing locations and third-party relationships (DPIAs, data flow diagrams).
(ii) Review policies: Data protection, information security, incident response, acceptable use, encryption, retention.
(iii) **Governance & Roles**: Verify presence of a DPO (if required), senior information risk owner, and defined responsibilities. Review training records and awareness programmes.
(iv) **Standard-Specific Checks**
- **GDPR**: DPIAs for high-risk processing, lawful basis records (Article 6), records of processing activities (RoPA), subject access request handling, lawful international data transfer mechanisms (Sakamoto et al.,2022).
- **PCI-DSS**: cardholder data environment (CDE) segmentation evidence, compliance with relevant SAQ or ROC, quarterly external scans by ASV, penetration testing and logging requirements.
- **HIPAA**: documented risk analysis, BAAs with vendors, administrative/physical/technical safeguard implementation, breach notification procedures.

(v) **Third-party & Supply Chain**: Review vendor security questionnaires, SOC 2 / ISO 27001 certificates or equivalent, contractual security clauses and SLAs.

Recommendations to meet those standards

(i) **Establish & maintain governance:** Appoint a DPO (if required) and define accountabilities. Maintain RoPA and DPIAs for risky processing.
(ii) **Classify & minimize data**: Map and classify data; minimize storage of personal, PHI and cardholder data; remove unnecessary retention.
(iii) **Apply strong technical controls**: Enforce encryption in transit and at rest for sensitive data; deploy MFA; implement robust key management.
(iv) **Segment sensitive environments**: Segregate CDE (cardholder) and systems holding PHI from general networks to reduce scope and risk.

(v) **Continuous vulnerability & patch management**: Implement automated scanning, timely patching, and prioritized remediation workflow.
(vi) **Adopt an ISMS / PIMS**:Implement ISO/IEC 27001 and privacy extension ISO/IEC 27701 to institutionalize controls and support audits(Lyons and Fitzgerald,2023).

Assumptions made

(i) The organization processes personal data of EU/EEA residents or is EU-based (hence GDPR relevant).
(ii) The company may handle card payments online (so PCI-DSS likely relevant). If not, PCI controls are unnecessary.
(iii) The organization may not be a U.S. covered entity for HIPAA unless explicitly in healthcare; HIPAA only applies if PHI is handled.
(iv) The environment has a mix of cloud and on-prem systems; third-party services are used (thus supply-chain controls needed).
(v) No current full ISMS or formal certification exists unless stated otherwise; recommendations assume remedial work is required.

References

Sakamoto, L.S., Abe, J.M., de Souza, J.S., de Souza, N.A., Duarte, A.C., Tarkiainem, E. and de Lima, L.P., 2022, September. Professional Guidance of the DPOs-BR in Corporate Governance in Logistics Chains. In *IFIP International Conference on Advances in Production Management Systems* (pp. 57-65). Cham: Springer Nature Switzerland.

Lyons, V. and Fitzgerald, T., 2023. *The Privacy Leader Compass: A Comprehensive Business-Oriented Roadmap for Building and Leading Practical Privacy Programs*. CRC Press.