Security and Risk Standards – Practical Application:

This unit focused on applying international security and risk-management standards ISO/IEC 27005, NIST CSF v2.0, PCI-DSS, GDPR, and HIPAA

Tools & Frameworks Used:

• ISO/IEC 27005 (2022)

• NIST CSF (2024)

• PCI-DSS, GDPR, HIPAA

• STRIDE

• Risk Matrix (likelihood × impact evaluation)

Group Risk Report – Pampered Pets Case Study (SME):

Our group applied a dual framework approach, using ISO 27005 for current manual operations and NIST CSF for digitalisation planning.

Mitigation Recommendations:

• MFA and phishing training

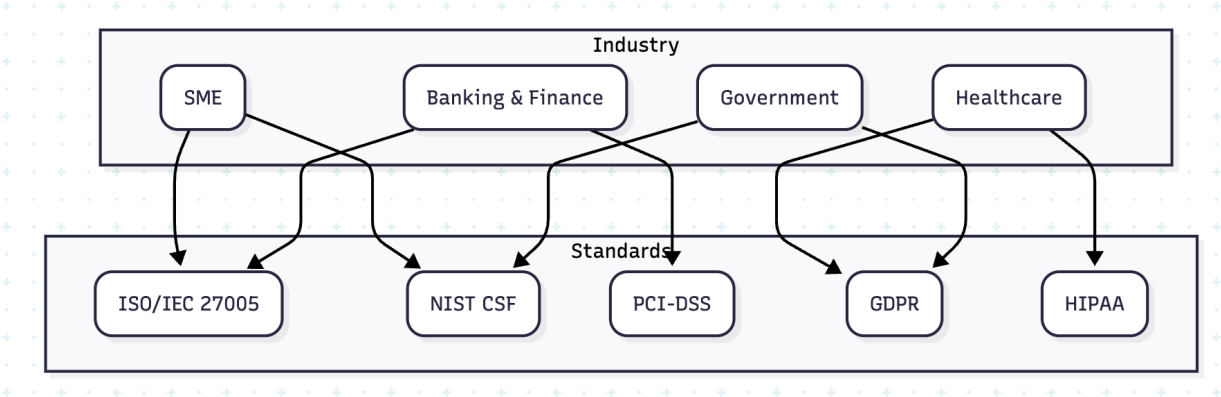
• Role-based access with audit logging

• GDPR compliant cloud storage

• PCI-DSS controls for online payments

• Regular backup testing and BCP validation

Figure 1: **Security standards mapped to different industries.**



Peer Reflection:

I led formatting and task coordination, drafted mitigation strategies, and helped to align our report with submission criteria and peer feedback.

Learning Outcomes:

I learned to apply industry standards to practical risk scenarios and understood how frameworks like ISO 27005 and NIST CSF complement each other for SMEs. The project improved my skills in risk modelling, compliance alignment, and team collaboration.

References:

European Union (2016) *General Data Protection Regulation (EU) 2016/679.* Available at: https://gdpr.eu (Accessed: 19 October 2025).

ISO/IEC (2022) *Information Security Risk Management (ISO/IEC 27005:2022).* Geneva: International Organization for Standardization.

NIST (2024) *Cybersecurity Framework 2.0.* Available at: https://www.nist.gov/cyberframework (Accessed: 18 October 2025).

PCI Security Standards Council (2020) *PCI-DSS Overview.* Available at: https://www.pcisecuritystandards.org (Accessed: 18 October 2025).

U.S. Department of Health & Human Services (2020) *HIPAA for Professionals.* Available at: https://www.hhs.gov/hipaa (Accessed: 18 October 2025).