Security and Risk Management:

This unit introduced foundational concepts in security and risk management, focusing on definitions of risk, threat, and vulnerability. According to ISO/IEC 27005, risk is modelled as: **Risk = Threat × Vulnerability × Impact**

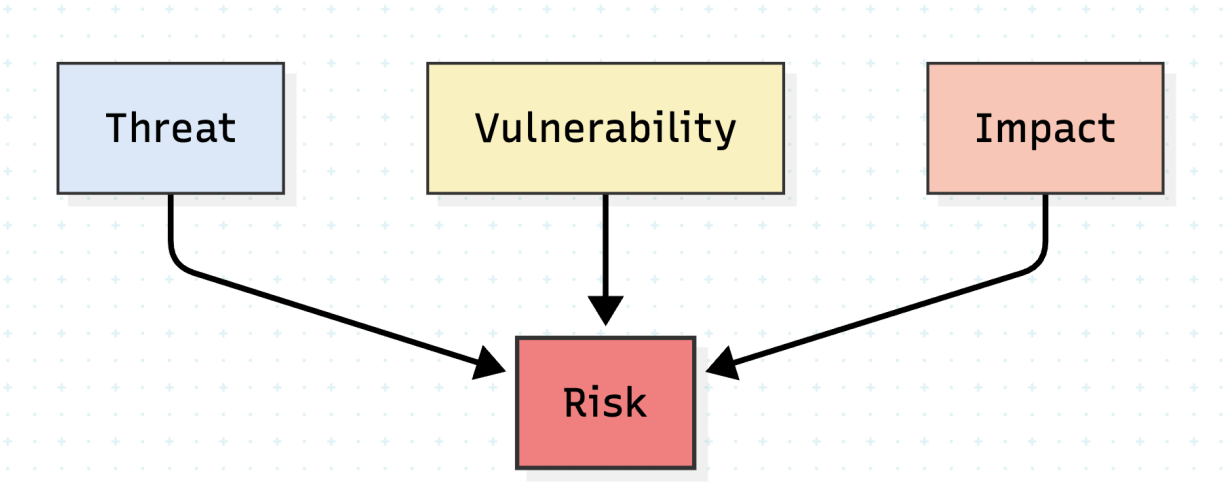

Figure 1: Relationship between Threat, Vulnerability, and Impact contributing to Risk (ISO/IEC 27005:2018)

Tools/Standards Used:

- ISO/IEC 27005:2018 – Information security risk management
- CVSS v3.1 – Vulnerability severity scoring

Learning Outcomes:

I learnt how risk is calculated and managed using ISO 27005 and how CVSS helps prioritise vulnerabilities and how soon they need to be fixed based on criticality. This foundation supports future work in threat modelling, quantitative risk analysis, and business impact evaluations.

References

ISO/IEC (2018) *Information security risk management (ISO/IEC 27005:2018).* Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/80585.html (Accessed: 18 October 2025).

FIRST (2019) *CVSS v3.1 Specification Document.* Forum of Incident Response and Security Teams. Available at: https://www.first.org/cvss/v3-1/specification-document (Accessed: 18 October 2025).