**Task 'End of Module Assignment e-Portfolio Submission' - Unit 12**

# Reflective Summary of the Semester – Security and Risk Management and E-Portfolio Submission

## 1. Units 1 and 2: Foundations and Assessment of Security and Risk Management

### WHAT

Units 1 and 2 introduced the foundation of Security and Risk Management (SRM), covering key definitions of risk, uncertainty, the CIA triad, and the structure of formal

risk management processes. Standards frame risk to qualitative and quantitative methods and stakeholder involvement are applied in practice.

(Stoneburner et al., 2002; Aven and Thekdi, 2024; Renn et al., 2021).

**SO, WHAT**

During this time, I have learned that risk is not purely technical rather than shaped by context, values, and judgment. Initially, I viewed standards and numerical outputs as completely reliable, this was challenged through reflection and peer discussion. Strict compliance can sometimes limit ethical judgement; quantitative methods may obscure uncertainty and lead to social impacts if voices are excluded. Additionally, qualitative approaches can introduce bias. Linking theory to human rights investigations showed how tools designed to protect privacy can also create risks related to bias, cultural misunderstanding and fairness, if applied, without oversight.

(Hancock, 2024; Aven and Thekdi, 2024); Abraha, 2025).

**NOW WHAT**

I will critically examine the assumptions behind risk definitions and standards to align with organizational values, ethics and the social context. In practice, I’ll employ qualitative and quantitative techniques, engage stakeholders to reduce gaps, and improve communication for ethical and accountable risk decisions.

2. **Units 3 and 4 – Threat Modelling and Management Techniques**

**WHAT**

These units explored threat modelling methods such as STRIDE, DREAD, Attack Trees, OCTAVE, and PASTA, along with tools like OWASP and MITRE Att&Ck.

(Shostack, 2020; Shevchenko et al., 2018).

**SO, WHAT**

Applying these models showed that no single threat modelling method fits all situations. I initially searched for the ‘best’ model, though, peer discussions revealed the value of using different approaches. Considering more models, reinforced the importance of assessing threat capabilities and vulnerability management. Some tools may create false confidence, results without human judgement that reinforce the idea that digital systems are both opportunities and risks.

(Renn et al., 2021).

**NOW WHAT**

I will use flexible, combined threat modelling approaches and clearly record assumptions, limits, and uncertainty. I will combine methods, prioritize human oversight and inclusive methods to manage socio-technical and ethical threats.

## 3. Units 5 and 6 – Practical Implications of Security and Risk Standards

**WHAT**

Units 5 and 6 examined regulatory and industry standards such as GDPR, and PCI DSS across sectors. Unit 6 required collaborative group work applying standards such as ISO 31000, ISO 27005 and more, into practical scenarios.

(Barafort et al., 2018; Sørensen, 2018)

**SO, WHAT**

Unit 6 marked a turning point. I recognized early in the project that leadership was required and maintaining focus and coordination was necessary, by driving communication and proactively engaging with the team members and ensuring a concept initiation and project structure was being formed. I kept the direction. While the engagement momentum was enhanced quite early, risks related to workload and decision dependency emerged, by inconsistent engagement. Absorbing additional responsibilities ensured delivery. This revealed limitations in delegation. This experience showed that effective risk management depends on governance, accountability, and interpersonal dynamics. The unit forced a re-evaluation of my assumptions. It highlighted the risks of failure at the team level.

**NOW WHAT**

I will address collaboration risks by clarifying roles early. I will escalate challenges very early. I will embed team responsibilities and accountability mechanisms into group governance structures and document such accordingly.

## 4. Units 7 and 8 – Quantitative Risk Modelling, Concepts and Implementation

### WHAT

These units introduced quantitative risk modeling techniques. These techniques include Monte Carlo simulation, Bayesian analysis, and multi-criteria decision-making. In addition, I learned that CVSS scoring is inconsistent, subjective, and often misunderstood as a risk measure.

(Metropolis, 1987; Asadabadi & Saberi, 2019).

### SO, WHAT

Overconfidence in quantitative models can result in decision-makers overlooking key uncertainties or failing to question assumptions. Sensitivity to input assumptions emerged as a critical limitation. This reinforces the critique of misplaced numerical certainty. Qualitative models, for instance vulnerability prioritization, could be undermined. This could limit decision reliability even when staff members are skilled.

(Hubbard, 2020).

### NOW WHAT

I will use quantitative output as decision-support tools. I will not use them as definitive answers. I will triangulate them with qualitative insight. Furthermore,

organizations should treat vulnerability results as preliminary. They should integrate different hybrid frameworks and contextual data; this will help improve decisions.

## 5. Units 9 and 10 – Risk, Business Continuity and Disaster Recovery

**WHAT**

These units focus on business continuity and disaster recovery, addressing RTO, RPO, and cloud-based resilience, threat and risk handling strategies.

(Andrade et al., 2017; Kumar, 2024).

**SO, WHAT**

Recognizing that resilience planning reflects an organization's mission and risk appetite, vendor lock-in and trade-offs challenge assumptions about the superiority of cloud solutions.

**NOW WHAT**

I will ensure that resilience planning aligns with organizational goals and risk governance by implementing continuous testing and scenario analysis tailored to the specific business use cases.

## 6. Units 11 and 12 – Projects, Emerging Trends, Module Integration and the Great Debate

**WHAT**

Units 11 and 12 consolidated the module through an executive-level project interconnected to unit 6 scenario focusing on digitalization, automation, and global supply chains. In addition to a reflection assignment.

(Pineiro-Chousa et al., 2017).

**SO, WHAT**

The quantitative evaluation showed that uncertainty is not merely a flaw but an inherent part of the system, as demonstrated by recent findings in supply chain analysis, this demonstrated the necessity of governance, oversight, and human judgment. The project demonstrated that various SRM techniques are more effective when employed as a unified decision-making framework alongside research, strategy, ethics, and risk awareness.

(Pineiro-Chousa et al., 2017).

**NOW WHAT**

I will continue leveraging research to develop evidence-based methods with due diligence and logically grounded security practices that communicate uncertainty, evaluate emerging technologies, and support effective executive due care.

## Conclusion

This semester, my knowledge of security has grown, particularly through Units 6, 11, and 12, which strengthened my understanding of leadership, collaboration, accountability, project management, governance and team dynamics. I developed a

critical understanding of SRM and how to better adapt to; uncertainty, context, and human factors, integrating multiple methods, navigating leadership challenges enhancing communication skills and the ability to resolve complex challenges. I gained much valuable knowledge throughout this seminar. The material, combined with the tutor's guidance, fostered a very positive, clear, and encouraging environment. This has been the most enriching semester for me, and I was consistently motivated to engage, the content was very in-depth and very clear, what greatly enhanced my learning experience. I hope that this high standard will be maintained also in future semesters.

## References


- Aven, T. and Thekdi, S. (2024) Risk Science. Routledge.
- Alhazmi, O.H. and Malaiya, Y.K., 2013, January. Evaluating disaster recovery plans using the cloud. In 2013 *proceedings annual reliability and maintainability symposium* (rams) (pp. 1-6). IEEE.
- Andrade, E., Nogueira, B., Matos, R., Callou, G. and Maciel, P., (2017). Availability modeling and analysis of a disaster-recovery-as-a-service solution. Computing, 99(10), pp.929-954.

- Asadabadi, M.R., Chang, E. and Saberi, M., (2019). Are MCDM methods useful? A critical review of analytic hierarchy process (AHP) and analytic network process (ANP). Cogent Engineering, 6(1), p.1623153.
- Barafort, B., Mesquida, A.L. and Mas, A., 2018. Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards & Interfaces*, 60, pp.57-66.
- Hancock, J., Hui, R., Singh, J. and Mazumder, A., (2024), June. Trouble at Sea: Data and digital technology challenges for maritime human rights concerns. *In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 988-1001).
- Hubbard, Douglas W. The Failure of Risk Management: Why It's Broken and How to Fix It. Second edition. Newark: Wiley, (2020). Web. Available at: https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_askewsholts_vlebooks_9781119522027. [Accessed 30 December 2025]
- Kumar, A. (2024) Cloud Vendor Lock-In: Identify, Strategies and Mitigate.
- Metropolis, N. (1987) The Beginning of the Monte Carlo Method'.
- Pineiro-Chousa, Juan et al. "Managing Reputational Risk through Environmental Management and Reporting: An Options Theory Approach." Sustainability 9.3 (2017): 376. Web. Available at: https://essex.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_proquest_miscellaneous_2327993361 [Accessed 9 January 2026]
- Rolfe, G., Freshwater, D. and Jasper, M., 2001. Critical reflection for nursing and the helping professions: A user's guide.
- Shostack, A. et al. (2020) Threat Modeling Manifesto.

- Shevchenko, N., et al. (2018) Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.
- Stoneburner, G., Goguen, A. and Feringa, A. (2002) SP 800-30: *Risk Management Guide for Information Technology Systems*.