**Individual Reflection**

**What?**

Before starting this module, I had already studied Network Security, where the focus was mainly on standards, protocols, and controls. At that time, I believed that robust frameworks such as the Common Vulnerability Scoring System (CVSS) were sufficient to address most information-security concerns. However, through the Information Security Management module, I realised that although such standards are robust, they are not universally applicable or context sensitive. This understanding marked a key turning point in how I now perceive security management, less as a checklist of standards and more as a holistic, adaptive process.

Throughout the module, I learned how Security Risk Management (SRM) is conducted from the ground up, including identifying, assessing, and mitigating risks across organisational contexts. I explored how risks are defined differently depending on business objectives, and how both quantitative and qualitative approaches can be applied to measure and prioritise them. The learning materials and activities clearly connected theoretical frameworks to real-world applications, which deepened my conceptual clarity.

A major highlight was the Pampered Pets case study, which offered a practical SME-based context. It provided a strong foundation for understanding the transition challenges a traditional business face when adopting digitalisation. By analysing its vulnerabilities, I was able to apply risk identification, assessment, and treatment concepts meaningfully to a real-world-like scenario.

Another significant learning experience came from the final assessment: developing a Python-based application to model and visualise attack trees. This task demonstrated how software tools can transform complex security data into interactive, decision-support visualisations. It reinforced the importance of usability and clarity when communicating technical risk information to non-technical stakeholders. The process also introduced me to the formal structure of attack trees described by Mauw and Oostdijk (2005) and later extended into attack–defence trees by Kordy et al. (2014), which helped me understand how logical nodes, probabilities, and expected losses can be combined to evaluate risk quantitatively.

I also contributed a discussion post on the risks of digitalisation, which helped me critically explore the balance between innovation and exposure, consolidating theoretical knowledge with reflective analysis.

**So What?**

This module changed my perspective on information security from being technology-centric to risk-centric. Previously, I focused mainly on defensive technologies, firewalls, IDS, and encryption. Now, I appreciate that understanding risk context, likelihood, and impact is equally essential. Through the practical activities, I learned how to connect assessment frameworks with strategic decision-making, and how SRM outcomes directly inform governance and compliance.

Developing the attack-tree application particularly strengthened my problem-solving, critical-thinking, and digital skills. Applying the mathematical concepts outlined by Mauw and Oostdijk (2005) on probability aggregation and Kordy et al. (2014) on incorporating defensive strategies gave the project a theoretical foundation. Designing and testing the Python interface helped me understand how even small, purpose-built tools can support decision-makers. Translating risk models into interactive visuals made the learning process more engaging and highlighted how digital transformation can be leveraged responsibly to enhance security analysis. It also improved my ability to manage my own time, structure development tasks, and deliver within defined constraints.

Another area of growth was critical reflection itself. Interpreting risk definitions, comparing frameworks, and evaluating their applicability in different environments required deep analytical thinking. This process helped me refine my ability to distinguish between what is technically correct and what is contextually appropriate. I also became more aware of the role of ethical and professional judgment in applying security principles, particularly when balancing protection, usability, and resource constraints.

In terms of the professional skills matrix and personal development plan (PDP), I observed improvements in several domains:

* Developing the application and interpreting case-study data required continuous evaluation of options and trade-offs.
* Reviewing different definitions of risk and communicating findings in concise written form strengthened my academic and professional writing.
* Analysing digitalisation risks from the SME perspective emphasised accountability and data-protection ethics.

**Now What?**

Looking ahead, the knowledge and skills gained from this module will guide how I evaluate and design security systems in both academic and professional contexts. I now understand that effective information-security management begins with contextual awareness, structured assessment, and continuous monitoring rather than isolated technical fixes.

I plan to apply this structured SRM mindset in my future work by:

* **Integrating Risk Thinking into Design:** During system or process design, I will explicitly map risks, impacts, and mitigation plans before implementation.
* **Applying Quantitative and Qualitative Balance:** I intend to use a mixed-method approach, aligning numerical metrics with qualitative insights from users and stakeholders.
* **Developing Practical Security Tools:** Inspired by the attack-tree project, I aim to continue building small, functional tools that assist in visualising and prioritising security decisions for teams and clients.
* **Maintaining Ethical Awareness:** I will ensure that every security decision also considers privacy, fairness, and transparency—especially when automation or AI is involved.
* **Continuous Professional Development:** I plan to expand my expertise in frameworks such as ISO 27005 and NIST SP 800-30, integrating them with what I have learned about risk quantification and contextual adaptability.

Overall, this module has been both intellectually and professionally rewarding. It transformed my understanding of security management from a purely technical pursuit into a dynamic discipline requiring judgment, adaptability, and critical reflection. By connecting theoretical standards with practical tools, I now feel more confident to evaluate security risks comprehensively and to design solutions that balance robustness, usability, and organisational context.

**References**

Forum of Incident Response and Security Teams (FIRST) (2019) *Common Vulnerability Scoring System v3.1: Specification Document.* Available at: [https://www.first.org/cvss/v3-1/specification-document](https://www.first.org/cvss/v3-1/specification-document?utm_source=chatgpt.com) (Accessed: 13 October 2025).

Kordy, B., Mauw, S., Radomirović, S. and Schweitzer, P. (2014) ‘Attack–defence trees’, Journal of Logic and Computation, 24(1), pp. 55–87. <https://doi.org/10.1093/logcom/exs029> (Accessed: 19 October 2025).

Mauw, S. and Oostdijk, M. (2005) ‘Foundations of attack trees’. In: Won, D. and Kim, S. (eds.) Information Security and Cryptology: ICISC 2005. Lecture Notes in Computer Science, 3935. Berlin and Heidelberg: Springer, pp. 186–198. Available at: <https://link.springer.com/chapter/10.1007/11734727_17> (Accessed: 19 October 2025).

Rolfe, G., Freshwater, D. and Jasper, M. (2001) Critical reflection in nursing and the helping professions: A user’s guide. Basingstoke: Palgrave Macmillan.