University of Essex

	Helpful to achieving the objective	Hamper achieving the objective
Internal origin (attributes of the system)	Strengths 1. I combine practical experience as an IT Project Manager in an international organisation with academic knowledge in Enterprise IT Management. 2. I have strong analytical and structured thinking skills, particularly in data-driven and enterprise contexts. 3. I am experienced in cross-functional and stakeholder communication, bridging business and technical perspectives. 4. I manage time and priorities effectively while balancing professional and academic responsibilities.	Weaknesses/Areas for further development 1. My hands-on proficiency in advanced coding languages is limited and requires further development. 2. I tend towards high personal performance standards, which can increase pressure and workload. 3. Limited time availability reduces opportunities for additional technical experimentation.
External origin (attributes of the environment)	Opportunities 1. Growing demand for enterprise IT and digital transformation expertise. 2. Opportunity to strengthen coding skills relevant to enterprise IT and data analytics. 3. Obtaining professional certifications (e.g. cloud platforms, project management, enterprise systems) to formalise expertise. 4. Ability to apply academic concepts directly within my current organisation.	Threats 1. Rapid technological change requires continuous upskilling to remain relevant. 2. Increasing competition for IT management and leadership roles. 3. Risk of workload saturation when combining work, studies, and continuous learning.

University of Essex

Reflection based on Gib's Reflective Cycle

Description

One key aspect of the IT Security Management module that has significantly impacted my professional practice is the application of structured risk and threat modelling frameworks, particularly during Units 3–8. Frameworks such as STRIDE, DREAD, CVSS, and OWASP were applied within a group-based case study, enabling me to conduct a practical risk assessment in an enterprise-like scenario. This experience connected theoretical security concepts with real-world organisational decision-making.

Feelings

At the beginning of the module, I felt confident about conceptual discussions around risk, governance, and compliance, as these align closely with my role as an IT Project Manager. However, I also felt challenged and occasionally frustrated when engaging with technical tools such as GitHub, Yasai, and quantitative risk modelling. These challenges initially caused uncertainty regarding my technical contribution but also motivated me to persist and develop new skills.

Evaluation

A key strength of this learning experience was gaining a structured approach to identifying, analysing, and prioritising security risks. Group work allowed me to contribute through organisation, critical thinking, and stakeholder-oriented analysis, while learning from peers with stronger technical backgrounds. Feedback on the group assignment highlighted that our analysis would have benefited from focusing on fewer models in greater depth, reinforcing the importance of critical selection rather than broad application.

Conversely, technical challenges and unfamiliar tools increased time pressure, particularly close to submission deadlines. This highlighted the gap between conceptual understanding and technical execution.

Analysis

The module demonstrated that IT security management is not purely technical but deeply embedded in enterprise risk management and organisational decision-making. Discussions on CVSS and its limitations illustrated how security metrics can oversimplify complex risks (Spring et al., 2021). Exploring alternatives such as SSVC reinforced the need for contextual, stakeholder-specific risk assessment. This insight is highly relevant to my professional role, where vulnerability scores often influence prioritisation and investment decisions without sufficient critical interpretation.

Additionally, the focus on regulatory frameworks such as GDPR highlighted the importance of compliance and governance in security strategy (Voigt and Von dem Bussche, 2017). These learnings have strengthened my ability to engage confidently in security-related discussions with both technical and non-technical stakeholders.

Conclusion

Overall, the module enhanced my understanding of IT security as a strategic enterprise concern. I recognised my strengths in analytical thinking and communication, while identifying the need to further develop technical and coding skills to better support quantitative risk assessments. The experience increased my confidence in applying structured security frameworks while maintaining a critical perspective.

Action Plan

Going forward, I plan to strengthen my technical skills, particularly in Python and security-related tools, to improve my engagement with quantitative risk modelling. I also aim to pursue relevant professional certifications in IT security or risk management to formalise my knowledge. In professional practice, I will apply a more selective and critical approach to risk frameworks, prioritising suitability and depth over breadth.

References

Spring, J., Hatleback, E., Householder, A., Manion, A. and Shick, D. (2021) ‘Time to Change the CVSS?’, IEEE Security & Privacy, 19(2), pp. 74–78. https://doi.org/10.1109/MSEC.2020.3044475

Voigt, P. and Von dem Bussche, A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer.

Shostack, A. (2014) Threat Modeling: Designing for Security. Hoboken, NJ: John Wiley & Sons.