E-Portfolio - Individual Reflective Piece

My Github Link: https://nas-25.github.io/E-Portfolio/

Course: MSc in Cybersecurity \ Security and Risk Management

Date: 20/10/2025

Table of Contents

Description

Throughout this module on Security and Risk Management, I explored the fundamental principles of protecting information, assets, and systems within organisations. The project involved examining real-world security incidents, developing risk assessment strategies, and applying theoretical frameworks to practical contexts. I participated in group discussions, analysed case studies, and contributed to collaborative tasks that deepened my understanding of security, governance, compliance, and risk mitigation. One key project focused on evaluating organisational resilience and developing a risk management plan (Kure et al.,2022). Initially, I found the technical aspects of security controls challenging, but ongoing engagement and peer feedback enhanced my confidence and comprehension.

Analysis and Interpretation

Engaging with this module reshaped my perspective on how security is integrated into business processes. I realised that effective security management is not solely about technology but also about human behaviour, communication, and policy (Metin et al.,2024). Working on the project evoked mixed emotions; excitement when identifying potential solutions but also frustration when facing complex analytical tasks or conflicting group opinions. These experiences taught me patience, critical thinking, and the importance of collaboration.

ISO 31000 (2018) and NIST frameworks, helped me understand structured risk assessment and governance principles. Reflecting on my behaviour, I noticed that I initially hesitated to take leadership in group discussions, preferring to focus on technical documentation. However, as the project evolved, I became more proactive in coordinating tasks, ensuring that deadlines were met, and contributing to report synthesis. Feedback from peers highlighted my analytical strength and reliability, which reinforced my motivation to take on greater responsibility (Ksibi et al.,2022).

This phase of learning also encouraged me to consider ethical dimensions in security management. Jyoti & Hutcherson (2021) made me appreciate the moral obligations professionals hold in safeguarding personal and organisational data. My emotional engagement especially the anxiety of potential data breaches made theoretical learning feel authentic and directly relevant to real-world contexts.

My Role in Team Tasks

During the Security and Risk Management module, my role in team tasks was both collaborative and analytical. I contributed primarily by coordinating our group's research and documentation process. For instance, I led a discussion on various risks and their organisational impacts, which initially felt challenging because I was uncertain about presenting technical details to peers. However, after receiving encouraging feedback from them, my confidence improved, and I learned to articulate security concepts more clearly. The collaborative exercises were equally transformative, and the Team Risk Identification Project was one of them.

Another contribution involved reviewing and editing the group report to ensure it met academic and professional standards. This required attention to referencing styles, content flow, and risk analysis accuracy. My analytical approach helped the team identify gaps in our evaluation, particularly when comparing qualitative and quantitative risk models. Although I initially found it difficult to balance leadership with equal participation, I learned that effective teamwork depends on trust, communication, and shared accountability (Kosmowski et al.,2022). When some members faced time constraints, I took the initiative to redistribute tasks and maintain progress. These experiences developed my organisational and leadership skills, reinforcing my ability to coordinate tasks in structured, time-sensitive environments.

Overall, this role helped me grow from a hesitant participant to a confident contributor. The process enhanced my problem-solving and interpersonal communication skills. I discovered that successful collaboration in cybersecurity projects is not about individual expertise but the collective ability to integrate technical, ethical, and strategic insights for practical solutions (Huda et al.,2024).

Teamwork Experience

Working within a diverse team was both stimulating and challenging. At the start, I felt overwhelmed by the variety of opinions and working styles. Clashing views on task prioritisation occasionally caused tension, especially when deadlines were tight. However, these moments taught me to compromise, listen actively, and recognise that disagreement can lead to more comprehensive and balanced outcomes. Over time, our discussions became more respectful and solution-focused, and we learned to appreciate each member’s unique perspective.

I noticed that teamwork fostered a deeper understanding of how communication and emotional intelligence influence project success. For instance, when I took time to acknowledge others’ suggestions, team morale improved, and collaboration became smoother. Sharing knowledge about data protection strategies and security governance frameworks helped us combine our strengths effectively (Onuh Matthew Ijiga et al., 2024). The process also highlighted the importance of empathy and adaptability—essential qualities in cybersecurity teams where roles and priorities often shift rapidly.

Reflecting on this experience, I realised that teamwork in security management mirrors real-world professional environments. Challenges such as time pressure, differing expertise, and conflicting opinions are inevitable, but they also provide opportunities to refine interpersonal and leadership skills. I learned to balance assertiveness with openness, ensuring that decisions were both informed and inclusive. By the end of the project, I felt more capable of working in multidisciplinary teams, confident that mutual respect and shared goals can transform obstacles into growth opportunities.

Application and Future Learning

This experience has significantly enhanced both my technical and soft skills. I gained proficiency in conducting risk assessments, identifying vulnerabilities, and applying mitigation strategies systematically. More importantly, I developed transferable skills such as teamwork, reflective thinking, and adaptability. In future professional settings, I intend to apply the ISO 27005 framework to evaluate organisational risks, particularly in the context of cybersecurity and information systems management.

Through this reflective process, I have learned the importance of continuous professional development and documentation. The e-Portfolio served as a valuable tool for tracking my growth, showcasing my analytical work, and linking theoretical understanding to practical outcomes. It helped me visualise my progress and provide evidence of the competencies I developed.

Moving forward, I plan to integrate reflective practices into my career to ensure ongoing learning. I also aim to strengthen my leadership and communication abilities in multidisciplinary teams, recognising that security management often requires coordination across departments. Ultimately, this module has inspired a mindset of responsibility, curiosity, and ethical awareness (Babu et al., 2022). Therefore, applying the insights gained, I am better prepared to contribute to secure and resilient organisational environments.

Conclusion

Finally, the Security and Risk Management module has been a very valuable learning experience that has enhanced my insight into the intricate interplay between security, risk, and organisational resilience. The theoretical study and practical application allowed me to have a holistic sense of how effective risk management enables strategic decision-making and safeguards both digital and physical assets (Bendler & Felderer,2023). The course also sharpened my analytical, problem solving, and collaborative abilities so that I can more confidently analyse threats and suggest suitable control measures.

Looking back on my experience, I can say that I have grown a lot, both personally and professionally. Moreover, I was taught to take issues systematically, communicate efficiently in a team, and consider ethical and governance aspects in planning security. The interaction with frameworks, such as ISO 31000 and NIST reinforced my ability to translate theoretical frameworks into practice (Magnusson et al., 2025). The reflective process and especially keeping an e-Portfolio promoted self-assessment and constant improvement.

References

Babu, G. N., Anbu, S., Kapilavani, R. K., Balakumar, P., & Senthilkumar, S. R. (2022). Development of cyber security and privacy by precision decentralized actionable threat and risk management for mobile communication using Internet of things (IOT). AIP Conference Proceedings, 2393, 020130. https://doi.org/10.1063/5.0074634

Bendler, D., & Felderer, M. (2023). Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model. ACM Transactions on Computing Education, 23(2), 1–33. https://doi.org/10.1145/3573205

Huda, S., Islam, M. R., Abawajy, J., Kottala, V. N., & Ahmad, S. (2024). A cyber risk assessment approach to federated identity management framework-based digital healthcare system. Sensors, 24(16), 5282. https://doi.org/10.3390/s24165282

Jyoti, D., & Hutcherson, J. A. (2021). Salesforce security architecture. In Salesforce Architect's Handbook (pp. 147–184). https://doi.org/10.1007/978-1-4842-6631-1_5

Kosmowski, K. T., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated functional safety and cybersecurity evaluation in a framework for business continuity management. Energies, 15(10), 3610. https://doi.org/10.3390/en15103610

Ksibi, S., Jaidi, F., & Bouhoula, A. (2022). A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach. Mobile Networks and Applications, 28(1), 107–127. https://doi.org/10.1007/s11036-022-02042-1

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection.

Neural Computing and Applications, 34(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. International Journal of Information Security, 24(4). https://doi.org/10.1007/s10207-025-01097-x

Metin, B., Duran, S., Telli, E., Mutlutürk, M., & Wynn, M. (2024). IT risk management: Towards a system for enhancing objectivity in asset valuation that engenders a security culture. Information, 15(1), 55. https://doi.org/10.3390/info15010055

Onuh, M. I., Idoko, P. I., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. Open Access Research Journal of Science and Technology, 11(1), 001–004. https://doi.org/10.53022/oarjst.2024.11.1.0060