**Reflections: Evaluation of the Final Project (Unit 11) vs. the Status Document (Unit 6)**

**E-Portfolio link:** [**https://kaylie89.github.io/index.html**](https://kaylie89.github.io/index.html)

**Introduction**

The journey from the initial status document in Unit 6 to the final project in Unit 11 has been instrumental in deepening my understanding of risk management and digitalisation. Collaborating with a team initially and transitioning to an individual project provided varied experiences in project management, teamwork, and independent analysis. This reflection critically evaluates the final project against the status document, highlighting key learnings, challenges, and personal growth.

**Project Overview: Initial Status Document (Unit 6)**

In Unit 6, our Cyber Risk Rangers team analysed and presented a comprehensive risk assessment and digitalisation strategy for Pampered Pets. The status document outlined our methodology, goals, and expected outcomes, focusing on enhancing our understanding of risk assessment frameworks and collaborative research. We incorporated ISO 31000, STRIDE, and FAIR models to establish a structured, comprehensive risk management approach. The expected outcomes included developing a digitalisation strategy that addressed business growth, cost reduction, and customer retention risks.

**Transition to the Final Project (Unit 11)**

The final project in Unit 11 required a more in-depth and individual-focused analysis. This project evaluated risks and opportunities in Pampered Pets' digitalisation plan, utilising Monte Carlo simulations to quantify financial impacts (Olson & Wu, 2020). Key recommendations were made to implement advanced monitoring systems, enhance quality assurance, encrypt data, and diversify suppliers to mitigate identified risks. The project provided a comprehensive risk analysis, focusing on quality risks, supply chain disruptions, and financial impacts.

**Security and Risk Management Process**

The methodological depth and application evolved substantially from Unit 6 to Unit 11. Initially, the status document primarily focused on setting the groundwork and understanding the frameworks of ISO 31000, STRIDE, and FAIR models (ISO, 2023; Shostack, 2014; Wang et al. 2019). However, in Unit 11, these methodologies were applied in greater detail, primarily through Monte Carlo simulations, to provide a quantitative risk assessment (Olson & Wu, 2020). This process enhanced my understanding of integrating multiple risk management frameworks to address various aspects of digitalisation. The transition from qualitative to quantitative analysis provided a more robust evaluation of potential financial impacts, demonstrating an advanced understanding and practical application of risk management techniques.

**Individual Contributions to Team Activities**

In Unit 6, my contributions were integral to the team's success. I led several discussions, ensuring productive and goal-oriented meetings. I also conducted thorough research on ISO 31000 and FAIR models, which are critical for our risk assessment framework. My efforts in compiling and editing the final report ensured coherence and clarity. The peer review highlighted effective teamwork but highlighted challenges such as differing work paces and conflicting ideas (Watts, 2024). Managing these dynamics required open communication and compromise, strengthening my collaborative skills. Specifically, I facilitated conflict resolution by mediating between differing viewpoints and enhancing team cohesion.

**Experience as a Member of a Development Team**

Working with the Cyber Risk Rangers in Unit 6 emphasised the importance of teamwork, communication, and collective problem-solving. Each member brought unique strengths, and we learned to integrate diverse perspectives to enhance our overall analysis (Paredes & Watts, 2024). The experience underscored the value of regular meetings, precise role definitions, and mutual support. Despite challenges, such as integrating different parts of the project and aligning on the project's direction, the collaborative effort resulted in a comprehensive and well-structured risk assessment.

**Emotional Response and Analysis**

Working on the project elicited a range of emotions. Initially, the collaborative nature fostered a sense of camaraderie and shared purpose. However, challenges such as conflicting ideas on risk assessment models and differing work paces in data collection and analysis sometimes lead to frustration. These emotions impacted my work by driving me to improve my communication and develop patience and negotiation skills. Reflecting on peer feedback and previous experiences, I realised the importance of adaptability and emotional resilience in collaborative environments. This realisation was supported by literature on team dynamics, emphasising emotional intelligence's role in successful teamwork (Goleman, 1995).

**Learning and Changed Actions**

The transition to an individual project in Unit 11 prompted a significant shift in my approach to learning and problem-solving. The autonomy required for independently managing complex analysis pushed me to develop a more structured and disciplined approach. Specifically, using Monte Carlo simulations necessitated meticulous data validation and critical assessment of assumptions, significantly deepening my analytical skills (Olson & Wu, 2020). This rigorous process highlighted the importance of data integrity and the impact of accurate assumptions on risk assessments. Additionally, I explored alternative risk assessment techniques, such as Bayesian networks, to compare their effectiveness against Monte Carlo simulations. This comparative analysis broadened my understanding of different methodologies. The insights gained from this project have fundamentally changed my approach to risk assessment, making me more thorough and data-driven.

**Skills and Knowledge Developed**

Throughout this journey, I significantly enhanced my ability to apply risk management frameworks and conduct quantitative analysis using Monte Carlo simulations. My analytical thinking improved through the detailed evaluation of potential risks and impacts. Additionally, my project management skills developed significantly as I transitioned from collaborative to individual work settings. The challenges faced provided valuable learning opportunities. Ensuring data accuracy and managing complex projects independently demonstrated personal growth and confidence in my analytical abilities. These skills are directly applicable to real-world scenarios in Cybersecurity and risk management.

**Professional and Personal Development**

The challenges faced during this journey provided valuable learning opportunities. They have profoundly impacted my professional development, as I gained deeper insights into digitalisation and risk management, which are valuable for future professional roles in Cybersecurity and risk analysis. My communication skills improved as I developed the ability to articulate complex analyses and recommendations clearly and effectively in writing and presentations.

**Future Applications and Continuous Learning**

The skills and knowledge developed through this project have equipped me with the tools necessary for continuous learning and professional growth. Adapting to new methodologies, critically evaluating data, and integrating theory with practice will enhance my effectiveness in identifying threats and devising appropriate defences in my future career. This commitment to continuous improvement is essential in the ever-evolving field of Cybersecurity.

**Conclusion**

The journey from the initial status document in Unit 6 to the final project in Unit 11 has been a transformative learning experience. It has significantly enhanced my understanding of risk management, improved my analytical and project management skills, and provided valuable insights into collaborative and independent work environments. This project has contributed to my academic growth and prepared me for future Cybersecurity and risk management professional challenges.

**References List**

Barafort, B., Mesquida, L.-A. & Mas, A. (2018) ISO 31000‐based integrated risk management process assessment model for IT organisations. *Journal of Software: Evolution and Process*. 1-15. DOI: <https://doi.org/10.1002/smr.1984>

Goleman, D. (1995). *Emotional Intelligence*. New York: Bantam Books. Available from: <https://asantelim.wordpress.com/wp-content/uploads/2018/05/daniel-goleman-emotional-intelligence.pdf> [Accessed 19 July 2024].

ISO. (2023) ISO31000:2018 Risk Management Guidelines Second Edition. Available from: <https://www.iso.org/standard/65694.html> [Accessed 14 May 2024].

Olson, L. D., & Wu, D. (2020) *Enterprise risk management models* (3rd ed.). Springer Nature. <https://doi.org/10.1007/978-3-662-60608-7_5>

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P. & Woody, C. (2018) Threat modelling: a summary of available methods. Available from: <https://apps.dtic.mil/sti/pdfs/AD1084024.pdf> [Accessed 25 May 2024].

Shostack, A. (2014) *Threat Modeling: Designing for Security. ProQuest Ebook Central:* John Wiley & Sons, Incorporated.Available from: <https://ebookcentral.proquest.com/lib/universityofessex-ebooks/detail.action?docID=1629177> [Accessed 25 May 2024].

Paredes, B.M. & Watts, K. (2024) Cyber Risk Rangers Team Contract.

Wang, J., Neil, M. & Fenton, N. (2019) A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security.* 89:1-20. DOI: <https://doi.org/10.1016/j.cose.2019.101659>

Watts, K. (2024). Peer evaluation template.