**Part 1: Reflective Piece**

**What?**

During the whole Security and Risk Management module I was on a journey of learning - structured and with both theoretical frameworks and practical applications. The module included a range of activities including unit exercises on risk identification and assessment, discussion groups, group projects and artefacts such as risk matrices, mitigation plans and threat modelling outputs. Each activity enabled me to reflect on the concepts covered in the lectures and put them into practice, so as to give a greater insight into the process of risk management.

One of the first challenges that I encountered was to learn the extent of the Risk Management Process (RMP). At first, I was not able to distinguish between qualitative and quantitative assessment methods. Unit 2 discussions made clear that qualitative assessments (e.g. interviews, expert opinion) are useful for understanding context-specific threats, while quantitative assessments (e.g. Monte Carlo simulations, probabilistic models) provide numbers that can be used for decision making (Unit 7 & 8). Theoretical understanding of the exercises allowed me to systematically assess risks for each exercise, taking both quantitative probability and business impact into account.

Another major learning experience for me was working in a project group with Julian and Peter. From Collaborative Learning Discussion 1, Mohammad Ali Okleh post on Industry 4.0 highlighted the convergence of AI, IoT and cloud computing and the security implications involved (Shevyakova, 2021). Thinking about this, I noticed that the emerging technologies created complex and interdependent risk management challenges, further establishing the necessity to have an ever-evolving threat model. Also in Collaborative Learning Discussion 2, the critique of CVSS by Femi Olowe focused on how generic scoring systems cannot be a good reflection of the context of an organisation. These conversations helped me to develop the following principle: an effective risk management programme needs to be both formally structured and critically objective in its application of tools.

My individual contribution to the team project consisted of the preparation of the project outline, as well as the integration of artefacts from each unit and checking my teammates' work for consistency and clarity. For instance, I wrote the mitigation plan section, which uses what I learned in Units 4 and 6 (the threat modelling and industry standards sections). I also organized our group meetings and kept participation levels high and on track to meeting deadlines. I have had difficulties sometimes in getting everyone's involvement equally (Julian was sometimes quiet in discussions), I learnt how to be effective in communication and make sure that each member's contribution is valued. Peer assessment verified my proactive engagement and contribution to the integration of ideas and support for other team members.

**So what?**

Reflecting on my learning experience, I can say that the module has provided a lot of learning opportunities in terms of both my technical and professional skills. Technically speaking, I gained expertise in identifying, analysing and mitigating security risks. For example, the risk register exercise was useful to systematically group threats based on likelihood, impact and severity and relate this to the right mitigation measures. This skill is transferable to real-world situations in which accurate documentation and prioritisation of risks can have an impact on organisational security decisions.

The teamwork aspect of the module also enhanced my teamwork skills and interpersonal skills. I learned how important communication is in addition to technical knowledge in order to successfully complete a project. Our project was enriched by including the opinions of more reserved members, by incorporating varied information, and by having a productive atmosphere that allowed me to effectively deal with issues of group dynamics. The constructive peer discussions re-emphasized that reflective learning is the order of the day; indeed, by examining the contributions of Mohammad Ali Okleh and Femi Olowe, I learnt to critically examine the quality of academic content and contextual relevance.

The feelings that I have experienced emotionally with this module have been mainly the difficulty of dealing with ambiguity and uncertainty when there is uncertainty, particularly in exercises where the risk scenario is a bit vague or incomplete. My first reaction was one of doubt, in terms of finding ways to measure risks or assessing effective mitigation strategies. However, I was able to become confident in my judgements through iterative practice, peer feedback and studying industry standards such as ISO/IEC 27001. This emotional growth translates to professional resilience as an ability to deal with an ambiguous or high-stakes situation is a key skill for security and risk professionals.

From an individual perspective, the module enhanced my organisational and analytical skills. By breaking down project milestones, task assignments and incorporating feedback, I mastered the art of time management and prioritization. Critical analysis of CVSS limitations, threat modelling, including STRIDE and PASTA, and the implementation of quantitative risk models increased my problem-solving and decision-making skills (Spring et al. 2021).

**Now What?**

In the future, I will take the knowledge and the skills I acquired from this module directly into my learning and into my practice. First of all, I am going to deepen my knowledge in the field of quantitative risk modelling techniques. The practical application of Monte Carlo simulations and Bayesian analysis brought up the value of decision making under uncertainty. I want to develop competence in the relevant software tools and programming applications for transferring these models into practice.

And lastly, the collaborative experiences have highlighted the need for good team management. In future projects, I will pay more attention to the inclusion of participation, the quiet members and the idea contribution, and maintain a structured communication channel. This will foster better team spirit and the quality of project deliverables, especially where multidisciplinary teams are the norm in cybersecurity and risk management roles.

Third, my reflective practice will grow and develop over time. By regularly evaluating my strengths, weaknesses, and emotional reactions in complex situations, I can find aspects of improvement while incorporating learnings into my continual professional development. For instance, I would like to keep a professional development plan (PDP) for acquiring knowledge on advanced penetration testing techniques, understanding the emerging threats in systems enabled by AI, and staying up to date on the global security standards such as GDPR and PCI-DSS (Aggrey et al. 2024).

Finally, this module has strengthened my ethical and professional integrity towards risk management. In the future, I will pay more attention to the technical correctness of my work, as well as adherence to legal, social and organisational standards. As part of the reflection process, an adaptable threat approach will also be developed to maintain accountability to ensure that both the performance of the individual and the security posture of the organisation is improved, thus making the organisation more resilient to change.

**Reference**

Aggrey, R., Osei Afoduo, K. Y., & Abrefi Ababio, M., Ansah Adjei, B. (2024). Understanding and Mitigating AI-Powered Cyber-Attacks. *International Journal for Multidisciplinary Research*, 6(6), 11. [DOI:10.36948/ijfmr.2024.v06i06.33563](https://www.researchgate.net/publication/387298527_Understanding_and_Mitigating_AI-Powered_Cyber-Attacks)Shevyakova, A. (2021). Competence development for Industry 4.0: Qualification requirements and solutions. *Journal of Security and Sustainability Issues*, 10(3), 63–74. <https://jssidoi.org/ird/article/download/63>

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

**Part 2: Evidence Portfolio**

The Security and risk management module has helped me to learn extensively about how to identify, analyse and reduce security hazards and vulnerabilities in the information systems of the contemporary world. I embraced various activities across different units of the module that enforced my comprehensiveness of the cyber risk frameworks, team based project work, and professional practices in fundamental risk management. The artefacts, group discussions, and peer reviews that are contained within this portfolio are all the embodiment of my academic and professional development.

During the first units, I learnt the basics of information security, such as threat modelling, vulnerability analysis and risk identification concepts. I also acquired skills in the process of studying the dynamics of risks in the context of the organisations and how the systematic evaluation may inform prioritisation and mitigation. Applied practice at the early stages involved the use of risk assessment models on simulated business cases, which further helped me relate theoretical risk paradigms in practical situations. The tasks are the search and integration of security data on various different sources, such as cybersecurity alert systems, vulnerability databases on the Internet, and industry reports. The process helped me to test the reliability and applicability of information in risk analysis, which directly promotes the learning outcome of critically analysis of security risks and threats.

The focus changed further into more intricate materials, including governance, compliance, and other ethical considerations of risk management later on in the module. I got involved in the group discussions with professional responsibilities and ethical decision-making analysing in relation to cybersecurity situations. These talks highlighted the importance of compliance frameworks like the ISO/IEC 27001-2022 in handling security risks in organisations. I also helped in coming up with written artefacts, which documented solutions to hypothetical incidences, the use of risk identification criteria as well as mitigation strategies towards risk reduction in line with best practice principles. These assignments allowed me to show that I can apply security concepts to well-structured writings and also convey research results in a professional manner.

The cooperative elements of the module came in handy in the course. By working in the team I was able to use theoretical knowledge in collaborative project work. My group which comprised of myself, Julian and Peter worked well to accomplish the project tasks. The members each added a different voice with Julian providing technical knowledge, Peter giving strategy and me coordinating the outlines of tasks and integration of all the deliverables. Based on the peer evaluation feedback, the team was highly effective, skillful in communication, on-timely and cooperative attitudes. I have contributed to preparing an outline of the project, checking the submissions of the teammates, and assisting them in joining all the parts together so that it would be consistent and high-quality. This process contributed to the relevance of teamwork in risk management where cooperation on the technical level, as well as the organisational level, defines the effectiveness of mitigation processes.

The theme of the Industry 4.0 and the role it will have in transforming businesses and increasing risk was the focus of the Collaborative Learning Discussion 1. My chosen peer, Mohammad Ali Okleh Harahsheh, presented an informative discourse citing Kovaite and Stankeviciene (2019), who reported Industry 4.0 as the merge of modern digital technologies namely, artificial intelligence (AI), the Internet of Things (IoT), big data, and cloud calculating in the industrial system. The post by him pointed out the fact that these technologies provide new possibilities of innovation but, simultaneously, they introduce new vulnerabilities and operating risks. Considering his reflections, the interrelation of digital transformation and risk management was one of the most interesting to me. Making smart systems to be integrated promotes productivity, at the same time, it also requires novel systems of securing interconnecting environments. This discussion has motivated me to deepen my research skills in topic of risk implication in AI-based ecosystems, which contributes to my analytical orientation on the adaptation of technology in risk management.

In Collaborative Learning Discussion 2, Femi Olowe explained the major criticisms of the Common Vulnerability Scoring System (CVSS) citing the works by Spring et al. (2021). In his analysis, it was determined that the CVSS will often give a generic score of the severity which is not reflective of the threat environment or business environment of the organisation. Moreover, he observed that the system is prone to cause a pretense of accuracy because it quantifies subjective data, which is likely to give wrong priorities of the security endeavors. This discussion proved beneficial especially in the consideration of the limitation of current tools of risk quantification. It prompted me to better consider vulnerability scoring and take into account extra non-numerical risk factors, including asset value and impact on the business, to the numerical score. Through this discussion, I have learned to be better in assessing security metrics and to realise that risk management should always be operationalised in the context of the operations of an organisation.

The group project that was created during the later part of the module was about drafting a systematic risk management plan of a simulated organisation. I was engaged in the detection of the key risks, their evaluation in terms of probability of occurrence and consequences, as well as the proposal of control measures. I was involved in the formulation of the sections of mitigation planning as well as operating response in the report. I also assisted the team to put together evidence of past units to make sure that what was eventually submitted would be a reflection of both theory and practice. The comparison between the first status document (Unit 6) and the last project (Unit 11) demonstrated a large amount of advancement. In our first paper we listed general risk concepts, and in the final product we were able to exhibit more of an integrated knowledge of threat analysis, governance alignment and practical recommendations. This development was not only shown through the increase of academic knowledge but also enhanced teamwork and coordination of projects.

The peer appraisal also assured that there was good cooperation. I have evaluated my input as being proactive, sharing project outlines, effective communication, and helping in the delivery of deliverables. Peter has had an outstanding involvement especially with his contribution to the risk mitigation methods that brought out the quality of the final project. Julian was a regular and technically accurate participant but sometimes made less contribution to discussions. These considerations demonstrate how our model of teamwork promoted group learning and problem-solving. The results of the peer evaluation are consistent with professional requirements in the field of team working with reliability, quality and collective responsibility.

The artefacts that have been created during this module show that I have practiced risk management methodologies. These can be the development of the risk register, a mitigation matrix design, and the recording of the strategies of responding to the incidents. All these artefacts are demonstrations of applied learning in various areas of learning and contributions to the learning outcomes of risk identification and mitigation with the help of the correct tools and frameworks. The assignments also improved my technical literacy and professional communication, preparing me to work practically in the area of cybersecurity jobs.

### **References**

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. [https://www.iso.org/standard/27001.html](https://www.iso.org/standard/27001.html%20)Kovaite, K. & Stankevičienė, J. (2019). Risks of digitalisation of business models. *Contemporary Issues in Business, Management and Economics Engineering*, May 2019. <https://www.researchgate.net/publication/333063956_Risks_of_digitalisation_of_business_models>

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