**Reflective Summary**

**STUDENT NAME**

**PROFESSOR NAME**

**UNIVERSITY NAME**

**DATE**

# **Part 1: Summary of Artefacts**

**Artefact 1**

**Title:** *Risk Estimation for Product Quality and Supply Availability under Digitalization and Global Supply Chain Transformation*

**Related Unit:** Unit 8 – *Implementing Quantitative Risk Models*

**Activity Type:** Individual Assignment

In this artefact, quantitative risk modelling is used, which is based on FMEA, Bayesian networks, and Monte Carlo simulation as part of risk assessment of the quality of the product and supply-chain reliability. The probability of the quality failure of software (~40%) and software supply stock-outs (~5–6%) provided quantitative indicators of competence and mastery of the art of statistical modelling and arguments of probability in the analysis. The Units 7-9 knowledge was applied to the project because of the interrelation between quantitative models and Business Continuity and Disaster Recovery design through RPO/RTO metrics.

The work of the individual was taken in the formulation of parameters of the simulation, the organization of the Bayesian dependency model, and the derivation of probability results on the operation-based decision-making. Other productive ideas of risk mitigation plans that were adhered to in the work to demonstrate good analytical research and applied research were multi-region replication, supplier misrepresentation, along automated rollback schemes.

Performing a comparison with the Unit 6 status document, one can observe that it has transformed the methods of qualitative analysis (insurance by ISO standards and complement ability by GDPR) towards data-based, quantitative analysis. There was also cooperation in both the model design peer review and literature integration. This artefact heralds the advancement of risk measurement, analytical modelling, and the combined synthesis of interdisciplinary systems.

**Artefact 2**

**Title:** *Industry 4.0 Risk Assessment Discussion*

**Related Unit:** Unit 2 – *Users, Assessments, and the Risk Management Process*

**Activity Type:** Discussion Post

This artefact argues about the signs of Industry 4.0 through the critical analysis and academic synthesis. In accordance with the aspect of qualitative and quantitative evaluation of Unit 2, the post discusses the technological, organizational, and environmental risks brought about by digitalization. The frameworks of user participation and assessment were used in the discussion, and a combined literature on Hancock et al. (2024) and Liao et al. (2017) was used to enumerate the cyber, competency, and behavioural risks (Hancock, et al., 2024; Liao, et al., 2017).

Individual contribution is one of the offerings in proving the relationship between theory and life examples, such as WannaCry ransomware attacks and the problems concerning the AI application, and engaging others in the academic discussion. The introduction of the feedback, gained by the classmates, contributed to the widening of the range of risks towards the regulatory (GDPR) and sustainability one, which reflects collaborative learning and reflexivity.

More than just intellectual knowledge is needed in this exercise, as well as group discussion skills, which involve the development of risk management activities, with the involvement of the users and the adoption of technology. Moreover, comparing the final project (Unit 11) to that of the status document (Unit 6), the progress was evident in the shift in the direction of the qualitative regulatory analysis to being forward-thinking and data-informed when making decisions. The Unit 11 project also included predictive modelling and collaboration with other units, unlike Unit 6, which was concerned with compliance reviews (GDPR, PCI-DSS).

**Artefact 3**

**Title:** *Critical Analysis of CVSS and SSVC Frameworks in Vulnerability Management*

**Related Unit:** Unit 7 – *Introduction to Quantitative Risk Modelling*

**Activity Type:** Individual Discussion Post

This artefact is the evaluation of the Common Vulnerability Scoring System (CVSS) as compared critically with the Stakeholder-Specific Vulnerability Categorisation (SSVC) model. It demonstrates the level of analysis regarding quantitative and semi-quantitative risk structure raised in Unit 7. The authors in their discussion turn out the non-empiricism of CVSS, the sensitivity of context and prediction mistakes, and advise SSVC, a prediction rule, a context-sensitive and action-oriented rule.

The individual work will involve the summation of the findings of Spring et al. (2021), Jacobs et al. (2020), and Allodi and Massacci (2017), along with the clarification on how the process of SSVC improves the decision-making process in terms of the parameters of stakeholders. To support the argument that the concepts of quantitative modelling (e.g., probabilistic weighting and contextual decision metrics) apply to practice management of cybersecurity, they also provided literature (Spring, et al., 2021; Allodi & Massacci, 2017).

This artefact demonstrates how the conceptual to methodological critique has evolved, in which the risk modelling theory is applied. It is devoted to the change between the theory and practical governance of cybersecurity and exemplifies an autonomous evaluation, scholarly rigour, and convergence of the techniques of courses. Comparing the final project (Unit 11) and the status document (Unit 6), the development was clearly traced in the use of the concepts of quantitative reasoning due to the contextual framework of SSVC, to the integration in practice of the empirical validation, and the compliance mapping.

**Artefact 4**

**Title:** *Pampered Pets – Cyber Risk Identification and Mitigation Report*

**Related Unit:** Unit 5– *Security and Risk Standards in Industry and the Enterprise*

**Activity Type:** Group Report

The group artefact is built on ISO/IEC 27005:2022 and NIST CSF v2.0 to examine cyber risks to a small business that has chosen to go through a digital transformation. It refers to the practiced industry standards and threat modelling (STRIDE) learnt during Units 5 and 6. The report separates and handles the threats in phishing, insider risks, and non-reliance on GDPR, which includes ISO motivations, ENISA reports, and NCSC frameworks.

A portion of these contributions was done separately and went as far as implementation of the STRIDE threat model, a model of probability and impact measurements, and mitigation plans that encompassed MFA, encryption, vendor risk evaluation, and security awareness training. The report is a mixture of the standards collaboration, where scoring is incorporated into a structured mitigation design driven by the SME contexts (Joel Chagadama & Luamba, 2022).

Its comparison with the status document (Unit 6) reflects better performance in familiarity with regulatory frameworks and operationalization of the same in a real-life situation. The artefact focuses on teamwork in the team, the introduction of the ISO/NIST standards, and strategic communication, which are vital skills in enterprise cybersecurity planning.

# **Reflection**

## The Security and Risk Management Process

The module has transformed the conceptual approach that I have towards the study of security and risk management as an abstract subject into a systematic methodology that is informed by data. To begin with, I attempted to get a grasp of the notion of digitalization as a factor in technological and organizational susceptibility using Artefact 2 (Industry 4.0 discussion). The execution of the framework depicted that user participation is the key to ensuring the risks are identified at the initial stages. The assessment of the 2017 WannaCry ransomware virus (at least 200,000 systems were affected) has provided me with insight into the nature of the interaction between human and technical vulnerabilities and how it can affect my perception of my risk exposure in real life. Unit 8 (Artefact 1) involved quantitative modelling with a blended tool of FMEA and a combination of Bayesian networks and Monte Carlo simulations.

Inputting a daily demand of 100 units (SD 20), lead time of 10 days (SD 3), and 10,000 trial simulations, I obtained a probability of 40 per cent of probability of software-quality failure occurrence and 5-6 per cent risk of stock-out at a service level of 95%. The abstraction of the theory reality was brought about by the making concrete theory of the probability, which related probability to the operational limits through the calculation of **Safety Stock ≈ 504 units** and **Reorder Point ≈ 1,504 units**. The ISO/IEC 27005 and NIST CSF v2.0 risk in governance and compliance were then contextualized in the Pampered Pets report (Artefact 4). Phishing, insider error, and weak access control were the most important threats used in the application of the STRIDE model. Concession points - WPA3, MFA, and encrypted hybrid backups, there was a mention of GDPR policies, which implied the presence of qualitative frameworks and quantitative prioritization.

## My Individual Contributions to Team Activities

The most important contribution I would make to the Pampered Pets project is the development of the STRIDE threat model and measuring the risks following the ISO 27005 in terms of likelihood-impact matrices. I wrote entries on the mitigation, such as the proposal of MFA, vendor-risk reporting, GDPR consent management, and ensured compliance with the ENISA (2023) and NCSC (2023) recommendations. I have standardized team jargon, too, between the ISO and NIST models, and made references that add to the academic integrity and cohesion. Among other things, I worked as an analyst, coordinator, organizer of little research, writing, and scrutiny, managing the version through Teams.

The posts of academic materials that I made in the peer discussions (Artefacts 2 and 3) provided me with the possibility to participate in the academic discussion. When discussing Industry 4.0, I have tried to tie theory with real-world examples, including the case of WannaCry and the adoption of AI, within which my peers and I have had more detailed discussions about the issue of GDPR and sustainability risks. In Artefact 3, I compared CVSS and SSVC, using the articles of Spring et al. (2021) and Allodi and Massacci (2017), which demonstrated that less than 30 percent accuracy can deal with real exploitation with the use of CVSS. The discussion was enabled by the use of the arguments supported by information, making it easier to discuss on the premises of evidence-based conclusions (Spring, et al., 2021; Allodi & Massacci, 2017)

## My Experience as a Member of a Development Team

I was engaged in the cybersecurity professional teamwork on the Pampered Pets group report. Firstly, there was no simple example of finding the schedule and the amount of expertise. I exhibited an agile-like process of development in the short development cycles and continuous feedback loop, which proved to be efficient in the of accountability and cohesion. The phase of threat-modelling has been marked by opposing opinions between the technical and policy perspectives. I was expected to make analytical discoveries understandable to other teammates without technical backgrounds, that have assisted me in mastering the art of mediation and simplification of complex topics. It was demonstrated by this experience that multidisciplinary diversity adds risk in plain view: the moment that I perceived statistical uncertainty, other individuals perceived behavioural or regulatory effects. The reflections provided made me more concise and conscious of people. It was the exposure to too technical tables whereby feedback was used to formulate more simplistic summaries, which is also crucial when delivering risk information to executives. My awareness was heightened after realizing that cybersecurity leadership does not mean some form of technical superiority but rather enabling interpersonal understanding through functional disciplines.

## Impact on My Professional and Personal Development

The module made an indelible mark on my professional and technical identity. I have learned to execute quantitative risk analysis to conduct Monte Carlo simulations, Bayesian reasoning, and interpretation of probabilistic outputs to make decisions. These solutions are directly connected with resiliency of the supply chain, business continuity, and cyber-risk analytics. I also learned about the concept of compliance-based security better using both ISO 27005 and NIST CSF, since they lead to the linkage of technical controls with governance or legal metrics, or indicators. This has now become clear to me that this process of security risk management is about trading off between quantitatively measuring likelihood and qualitatively measuring assessment, and is a policy, ethics, and business matter.

On the personal level, I became more critical and able to communicate. This also helped me to develop my analytical response and evidence-based thinking by trying to make sure that my outputs were often compared to the scholarly research (Spring, et al., 2021). Teamwork helped me to be humble and flexible, which is more significant to me to share the peer insight in the same manner as my gathered data. Critical learning and technical expertise are combined with teamwork and have transformed my professional outlook. Now, I have understood cybersecurity as a strategic discipline that simultaneously connects exactness and moral responsibility as well as human unity.

# References

Allodi, L. & Massacci, F., 2017. Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis,* pp. 1606-1627.

Hancock, J., Hui, R., Singh, J. & Mazumder, A., 2024. Trouble at Sea: Data and digital technology challenges for maritime human rights concerns. *In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency,* pp. 988-1001.

Joel Chagadama, D. B. A. & Luamba, D. S., 2022. Cyberattacks: A Huge Concern for Small Business Sustainability.

Liao, Y., Deschamps, F., Loures, E. D. F. R. & Ramos, L. F. P., 2017. Past, present, and future of Industry 4.0-a systematic literature review and research agenda proposal. *International Journal of Production Research,* pp. 3609-3629.

Spring, J. et al., 2021. Time to Change the CVSS?. IEEE Security & Privacy. *IEEE Security & Privacy,* pp. 74-78.