Task ‘An Introduction to Security and Risk Management’ Unit 1

Collaborative Learning Discussion 1 – Summary

Across the three units, starting with unit 1, I developed my knowledge using the clear progression path that emerges from understanding foundational definitions of risk and security management concepts, through different terminology and approaches toward risk in unit 2 **(Hubbard, 2020)**, for instance; the CIA triad, qualitative and quantitative risk management and the definition risk**,** to exploring threat modelling techniques in unit 3 and more.

My initial post and interactions with my peers were built upon these concepts by connecting theoretical frameworks to real-world ethical challenges in technology-driven human rights investigations. Those investigations helped me explore how technology can be used to protect privacy, while simultaneously technology can present some questionable and cultural constraints, in addition, how data and technology can enhance transparency but also increase risks to fairness and accountability. Biased datasets of black-box privacy and the exclusion of local communities can lead to misinterpreted evidence and reinforce inequality, nevertheless, such inclusion could help develop more ethical and privacy-aware thinking.

(Hancock, 2024)

Consistent with the argument that uncertainty, frequency, magnitude and perception are integral to risk science, these examples demonstrated how technological

interventions must be assessed quantitatively and qualitatively, addressing the context of improved communication, decision-making, and governance, as well as their related risks.

(Aven and Thekdi's 2025)

In peer discussions, Victor and I emphasized that poorly measured or misunderstood risks, such as algorithmic bias, can undermine the very systems they aim to improve, and challenge technology such as blockchain, mesh networks, and satellite systems, although these offer benefits in remote locations, they still hold some limitations.

(Abraha, 2025; ***, 2025; **** ***** *****, 2025)**

Jens responded and recommended that it could be useful to use additional approaches to identify and analyze risk factors, such as threat capability and vulnerability, for instance the Open FAIR model, which may provide a more structured approach.

(**, 2025)**

Those discussions also extended and reinforced the points that human oversight must remain central to digital risk mitigation and that digitalization should be viewed as both an opportunity and a systemic risk and maintain a balanced approach.

(Renn, Beier, Schweizer's, 2021)

Finally, in unit 3, learning about threat modelling frameworks such as Attack Trees, OCTAVA, DREAD, STRIDE and PASTA, which are very interesting approaches and offer structured ways to identify vulnerabilities also in human centered approaches into such models within participatory approaches may help predict and mitigate socio-technical threats and help prepare proactive counter measures.

(Shostack 2020; Shevchenko, Chick, O'riordan, Scanlon, Woody, 2018)

Overall, the discussions enrich a maturing learning of security risk management shifting from conceptual definitions to applied, ethically grounded strategies for responsible digital governance.

References

- Abraha, D.T. (2025) Blockchain-based solution for addressing refugee management in the Global South: transparent and accessible resource sharing in humanitarian organizations', Frontiers in Human Dynamics, 6, p.1391163.
- **** ****** ****, V. (2025). Unit 1: An Introduction to Security and Risk Management: *Collaborative Learning Discussion 1, Initial Post,* University of ****** Online, Available at: https://www.my-course.co.uk/mod/forum/discuss.php?d=330362 [Accessed 6 November 2025].
- Hancock, J., Lee, S. and Martín, P. (2024) Trouble at Sea: Data and digital technology challenges for maritime human rights concerns', Proceedings of the

2024 ACM Conference on Fairness, Accountability, and Transparency, pp. 988–1001.

- Hubbard, Douglas W. The Failure of Risk Management : Why It's Broken and How to Fix It. 1st ed. Hoboken, N.J: J. Wiley & Sons, 2009. Print.
- ******, J (2025). Unit 1: An Introduction to Security and Risk Management: Collaborative Learning Discussion 1, Initial Post, University of ****** Online, Available at: https://www.my-course.co.uk/mod/forum/discuss.php?d=330362 [Accessed 6 November 2025].
- *******, A. (2025). Unit 1: An Introduction to Security and Risk Management: *Collaborative Learning Discussion 1, Initial Post,* University of ****** Online, Available at: https://www.my-course.co.uk/mod/forum/discuss.php?d=330362 [Accessed 6 November 2025].
- Renn, O., Beier, G. and Schweizer, P.J. (2021) The opportunities and risks of digitalisation for sustainable development: a systemic perspective', GAIA – Ecological Perspectives for Science and Society, 30(1), pp. 23–28.
- Shevchenko, N., Chick, T.A., O'riordan, P., Scanlon, T.P. and Woody, C., (2018). Threat modeling: a summary of available methods (No. AFLCMCAZS).
- Shostack, A. et al. (2020) Threat Modeling Manifesto. Available at:https://www.threatmodelingmanifesto.org [Accessed 4 November 2025].
- Thekdi Shital, and Terje Aven. "Evaluating Risk Analyst Views on Uncertainty and Knowledge Aspects for Risk Characterization Approaches." Journal of risk research 28.8 (2025): 912–928. Available at: https://******.primo.exlibrisgroup.com/permalink/44UOES_INST/o3t9un/cdi_informaworld_taylorfrancis_310_1080_13669877_2025_2553847 [Accessed 4 November 2025]

This document has been written solely for educational purposes. All references, names, and trademarks mentioned here remain the property of their respective owners and are used here strictly for the educational context. Grammarly was used exclusively for proofreading and enhancing the clarity and language of the text. All academic writing, analysis, argumentation, and conclusions are entirely the original work of the author.