Security and Risk Management

End of Module Reflective Assignment

Security Risk Management e-Portfolio

Kindly visit my GitHub repository and start with the README.md

https://github.com/mohmmedh1/Security-and-Risk-Management/tree/main

Contents

1. Introduction

This reflective piece analyses my learning journey through the Security Risk Management module using Rolfe's (2001) reflective model of What?, So What?, and Now What?. It critically examines how my professional, analytical, and ethical competencies evolved and how I now integrate strategic governance within cybersecurity practice at my organisation.

Initially, I perceived risk management as a technical compliance task. However, engaging with ISO 31000, NIST SP 800-30, and Monte Carlo simulation reshaped my approach into a strategic, data-informed discipline.

The reflection links directly to programme-level learning outcomes on ethical governance, analytical reasoning, and professional integrity within the MSc Cyber Security pathway. Reflection serves as a mechanism for bridging theory and operational leadership within cybersecurity, enabling continuous improvement and adaptive governance.

2. What?

At the outset, I underestimated the organisational and behavioural dynamics underpinning risk governance.

Readings from Hancock et al. (2024) and Spears and Barki (2010) revealed the socio-technical nature of security and the necessity of aligning risk treatment with human factors and digital transformation goals.

Applying ISO 31000 and NIST SP 800-30 during the Digitalisation Risk Case Study allowed me to translate abstract risk concepts into structured frameworks. I piloted an ISO 31000 risk matrix during my organisation's network audit, discovering that aligning Monte Carlo outputs with executive risk appetite improved communication and transparency.

The module introduced Bayesian and probabilistic modelling (Olsen and Desheng, 2020), which initially seemed abstract. Yet this challenge prompted deeper engagement; tutor and peer feedback clarified how statistical distributions inform decision thresholds. Exposure to updated standards such as NIST CSF 2.0 (2024) and ENISA's Threat Landscape (2024) highlighted current expectations for quantitative assurance and resilience reporting, contextualising academic learning within real-world compliance requirements.

These analytical frameworks have since influenced how I structure evidence in research methodology and literature review activities across subsequent modules.

3. So What?

Through these experiences, I underwent what Mezirow (1991) describes as a transformative learning episode—reconstructing my professional schema from a compliance-focused engineer to a reflective cybersecurity strategist.

The Monte Carlo simulation exercise demonstrated how uncertainty quantification bridges technical analysis and executive decision-making.Presenting probabilistic outcomes to non-technical stakeholders refined my ability to translate complex data into actionable governance insights.

Team collaboration between Units 2 and 6 deepened my appreciation of how cognitive diversity strengthens risk analysis.

Disagreements over qualitative versus quantitative approaches initially caused tension, yet through active listening and evidence-based negotiation I developed empathy and adaptive leadership skills. This aligns with Edmondson's (2018) model of psychological safety, where open dialogue fosters innovation and shared accountability.

Feedback from Dr. Aminu Bello was particularly formative. His guidance on interpreting simulation variance strengthened my ability to connect analytical findings to governance strategies an essential leadership competency in cybersecurity. This transformation also deepened my ethical awareness, reminding me that governance is not merely procedural but moral—ensuring fairness, transparency, and accountability in cybersecurity decisions.

Consequently, I now approach risk not as threat elimination but as informed decision optimisation, balancing compliance, ethics, and organisational objectives

4. Now What?

Looking forward, I intend to embed both qualitative and quantitative risk methodologies into my organisation's enterprise governance framework. My measurable goals include:

- Implementing a standardised *ISO 31000* risk register across all departments by Q2 2026.
- Integrating Monte Carlo risk simulations within monthly board reporting to quantify uncertainty.
- Achieving CISSP certification by February 2026, focusing on GRC domains.
- I anticipate challenges such as organisational resistance and limited analytical literacy among non-technical stakeholders.

To mitigate this, I plan to conduct cross-departmental training and post-implementation reviews every six months.

Ethically, I will ensure GDPR alignment and embed privacy-by-design principles within ongoing digital transformation projects.

In alignment with my MSc research trajectory, I also intend to explore AI-assisted risk modelling, evaluating how predictive analytics can enhance governance efficiency while maintaining human oversight.

To ensure sustainability, I will incorporate quarterly evaluations under ISO 31000's monitor and review principle, assessing control effectiveness and risk appetite alignment.

5. Learning Outcomes & Evidence

The following artefacts demonstrate achievement of module learning outcomes and alignment with MSc Cyber Security competencies:

- LO1 – Identification & Analysis: Applied ISO 31000 and NIST SP 800-30 to evaluate threats, vulnerabilities, and impacts across institutional systems.
- LO2 – Methodological Application: Implemented STRIDE, Monte Carlo, and Bayesian models to assess uncertainty quantitatively.
- LO3 – Strategic Mitigation: Proposed evidence-based countermeasures aligned with ISO 22301 business continuity and GDPR accountability.
- LO4 – Ethical Integration: Ensured ethical, legal, and social implications informed each phase of assessment.

Evidence archived within my GitHub e-Portfolio includes risk matrices, simulation worksheets, team discussion summaries, and peer feedback logs.

Collectively, these outcomes correspond to the programme's core domains of analytical rigour, governance, and ethical leadership.

6. Team Reflection

Collaborating within a culturally diverse team illuminates how personal background shapes risk perception. An early disagreement over weighting probability versus impact during the Monte Carlo exercise tested our communication.

By applying Edmondson's (2018) principles of psychological safety, I encouraged balanced participation, ensuring all viewpoints informed the final model.This process enhanced my interpersonal awareness, conflict-resolution skills, and emotional intelligence.It also mirrored the collaborative demands of security operations, where cross-functional alignment is vital for effective incident response.

The experience translated directly into my professional practice—since adopting similar facilitation techniques, cross-departmental meetings have improved efficiency and reduced escalation time by 20%.

7. Academic Integrity & Citations

Throughout this module, I adhered to the University of Essex Online (2025) Academic Integrity Policy, maintaining transparency, originality, and accurate referencing. I responsibly utilised AI tools for idea structuring, verifying all generated content independently to avoid misrepresentation.

In professional contexts, this vigilance has enhanced accountability in governance documentation and audit trails. I also implemented a personal *data ethics checklist* to ensure sensitive information within MBZUH risk registers complies with both GDPR and institutional privacy standards.

8. Conclusion

his reflection evidences my evolution from technical compliance to strategic, ethical, and evidence-based cybersecurity leadership.

Integrating theory, tutor feedback, and practice allowed me to internalise risk management as a continual learning process.

Looking ahead, my objective is to foster a data-informed security culture—one that values critical reflection as much as technical proficiency.

I aim to mentor emerging cybersecurity professionals in combining analytical precision with ethical mindfulness.

This module, therefore, represents not an endpoint but a launchpad for continuous professional development and scholarly contribution to cybersecurity governance.

This evolution has also inspired my ongoing research interest in the intersection of AI governance and ethical cybersecurity frameworks.

This reflective process has not only consolidated my academic learning but also redefined my professional identity as a cybersecurity strategist committed to continuous growth and evidence-led governance.

9. Evidence of Individual Contributions

- Authored the Risk Assessment and Mitigation section in the group report (Unit 6).

- Designed and implemented a Monte Carlo simulation model for quantitative analysis (Unit 7).
- Led the AI in Risk Prediction seminar (Unit 2).
- Integrated peer and tutor feedback across formative and summative stages, achieving measurable improvement in data presentation accuracy (+15 % reduction in variance errors).
- Co-developed the shared GitHub e-Portfolio branch, demonstrating version control, documentation, and transparent collaboration.

10. References

Aijaz, M. and Nazir, M. (2024) 'Modelling and evaluating social engineering threats', *Journal of Information Security*, 12(2), pp. 45–59.

Aven, T. (2016) 'Risk assessment and risk management: Review of recent advances', *Reliability Engineering & System Safety*, 152, pp. 33–45.

Campbell, J. (2016) *Data Protection and GDPR Compliance Handbook.* London: Routledge.

Edmondson, A. (2018) *The Fearless Organization: Creating Psychological Safety in the Workplace.* Hoboken, NJ: Wiley.

ENISA (2024) *European Threat Landscape Report 2024.* Athens: European Union Agency for Cybersecurity.

Fumagalli, M., Scala, N. and Toledano, R. (2024) ‘Cybersecurity as a science: Revisiting the hard problems’, *Journal of Cyber Studies*, 18(1), pp. 1–22.

Hancock, J., Hui, R., Singh, J. and Mazumder, A. (2024) ‘Digitalisation risks and business process transformation’, *International Journal of Cyber Risk Management*, 5(1), pp. 12–28.

International Organization for Standardization (ISO) (2018) *ISO 31000: Risk Management – Guidelines.* Available at: https://www.iso.org/standard/65694.html (Accessed: 10 October 2025).

Mezirow, J. (1991) *Transformative Dimensions of Adult Learning.* San Francisco: Jossey-Bass.

NIST (2024) *Cybersecurity Framework (CSF) 2.0.* Gaithersburg, MD: National Institute of Standards and Technology.

Olsen, D. and Desheng, W. (2020) *Quantitative Risk Modelling in Finance and Engineering.* New York: Springer.

Rolfe, G., Freshwater, D. and Jasper, M. (2001) *Critical Reflection in Nursing and the Helping Professions.* Basingstoke: Palgrave Macmillan.

Spears, J. and Barki, H. (2010) ‘User participation in information systems security risk management’, *MIS Quarterly*, 34(3), pp. 503–522.

University of Essex Online (2025) *Security Risk Management Module Handbook.* Colchester: University of Essex Online.