Reflective Summary: My Learning Journey in Security and Risk Management

Structured using Rolfe's (2001) Model – What? So What? Now What?

Introduction

The Security and Risk Management (SRM) module has been one of the most valuable parts of my MSc Cyber Security studies. It helped me see security in a different way, not just as a technical function, but as something that connects people, trust, and governance. I'm using Rolfe's (2001). What? So what? Now what? model and the University of Edinburgh's (2020) toolkit. This reflection captures what I learnt, how I felt during this module, and how it has shaped me as a person and professional.

What?

When I started this module. I approached IT security as a technical job. But as I studied frameworks like ISO/IEC 27005 (2022) and NIST (2024) CSF v2.0, I realised that risk management is more than technical; it's about understanding how threats, vulnerabilities, and impact link together. Learning that **Risk = Threat × Vulnerability × Impact** gave me a more structured way of thinking (ISO/IEC, 2022).

The GDPR case study (European Union, 2016) really changed how I saw privacy. It wasn't just about laws; it was about people's trust. Seeing how one mistake could affect reputation made me understand that protecting data is also protecting values.

Working on the **Pampered Pets team project** was another turning point. At first, I was quiet during discussions, especially when I wasn't sure if my ideas would fit. But over time, I became more confident and started contributing to our report with ISO 27005 and NIST CSF. I reviewed risk matrices, checked our assumptions, and helped the group stay within word limits. I also learnt that teamwork isn't about control; it's about listening, compromise, and empathy. This module helped me grow as a collaborator and communicator.

One of the most challenging yet rewarding parts of this module was learning to apply **quantitative risk models** in real-world business situations. At first, I struggled to grasp probability concepts, but understanding **Monte Carlo simulation** and **Bayesian updating** completely changed how I viewed uncertainty, revealing that it can be both measurable and actionable (Hubbard, 2009). Exploring frameworks like **FAIR** *(*Böhme, Laube and Riek, 2020) and **CVSS** helped me see how probability and impact translate into practical insights that leaders can use to understand the risk. FAIR made me understand risk in financial terms, while CVSS showed how small vulnerabilities can cause serious disruption. When studying multi-cloud DR architectures, I could connect these academic ideas to my professional experience in hybrid failover and synchronous replication. It was satisfying to see that theory explained the rationale behind real-world scenarios I had already encountered at work. This experience also reminded me that being accurate and ethical with data is essential, because decisions in cybersecurity always affect people as much as systems.

So What?

This module taught me that technology alone is not enough, but it needs people who understand collaboration, communication, and ethics. During the project, I noticed how open communication helped us build trust. It reminded me that, in security, teamwork is just as critical as technical skill.

I also went through a tough period during the module. I fell ill and struggled with anxiety, which affected my focus and motivation. My wife kept encouraging me not to give up, and that support really helped me find balance again. When I joined the BC/DR seminar after recovering, I felt more focused. Learning about ISO 22301 (2019) and ENISA's (2022) guidelines made me see that resilience isn't only about systems, but it's about people too.

Another interesting part was the unit on behavioural economics. I learnt how bias affects our security choices. For example, I used to depend a lot on technical evidence and ignored emotional or user-driven aspects. Realising this helped me improve my judgement and understand that leadership in security requires both logic and empathy (Kahneman, 2011).

There were moments when I doubted myself, especially while balancing full-time work and deadlines, but those challenges made me more disciplined. I learnt that resilience is not just recovering from setbacks; it is the mindset of people who never give up.

Now What?

This module has completely changed how I see myself. I no longer think like just an IT engineer; I now think like a reflective professional who connects

ethics, data, and people. I've added these goals to my **Personal Development Plan (PDP):**

- **Technical Growth:** Keep improving my understanding of quantitative risk models (like Bayesian and FAIR) and build hands-on experience with AWS and Azure disaster recovery, following ISO 22301 (2019).
- **Ethical Practice:** Apply GDPR and (ISC)²'s (2023) Code of Ethics in my day-to-day decisions to make sure I act transparently and responsibly.
- **Continuous Reflection:** Maintain a small reflective journal for each project to track what went well, what didn't, and how I felt about it (University of Edinburgh, 2020).
- **Team Collaboration:** Continue practising active listening and empathy in team projects so everyone feels valued.

Looking ahead, I plan to approach future modules with more curiosity and self-awareness. I now see mistakes as checkpoints rather than failures. This connects directly with Rolfe et al.'s (2001) *"Now What?"* stage, turning learning into action.

On a personal level, this journey reminded me that vulnerability isn't weakness. Sharing challenges and emotions made me a stronger learner. I've realised that security comes from balance between people and systems.

Conclusion

Completing the SRM module has been **t**ransformative both professionally and personally. I started out seeing security as mostly technical, but now I understand that it's deeply human. I've learnt that protecting systems means protecting trust, and resilience applies as much to individuals as it does to networks. This module gave me not only academic knowledge but also confidence, empathy, and a new sense of direction. I'll carry these lessons into every project I work on, because being secure means being ethical, reflective, and human.

References

(ISC)² (2023) *Code of Ethics*. International Information System Security Certification Consortium. Available at: https://www.isc2.org/Ethics (Accessed: 23 October 2025).

Aven, T. and Thekdi, S. (2025) *Risk Science*. Abingdon: Routledge.

Böhme, R., Laube, S. and Riek, M. (2020) 'A fundamental approach to cybersecurity risk management based on FAIR', *Journal of Cybersecurity*, 6(1), pp. 1–16. Available at: https://academic.oup.com/cybersecurity/article/6/1/tyaa004/5852468 (Accessed: 23 October 2025).

ENISA (2024) *Best Practices for Cyber Crisis Management*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management (Accessed: 23 October 2025).

European Union (2016) *General Data Protection Regulation (EU) 2016/679*. Available at: https://gdpr.eu/ (Accessed: 20 October 2025).

FIRST (2021) *Common Vulnerability Scoring System v3.1: Specification Document*. Forum of Incident Response and Security Teams. Available at: https://www.first.org/cvss/v3-1/ (Accessed: 20 October 2025).

Fraser, J.R.S., Quail, R. and Simkins, B. (2021) *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Hoboken, NJ: Wiley.

Hubbard, D.W. (2009) *The Failure of Risk Management: Why It's Broken and How to Fix It*. Hoboken, NJ: Wiley.

ISO/IEC (2019) *ISO 22301:2019 Security and Resilience — Business Continuity Management Systems — Requirements*. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/75106.html (Accessed: 23 October 2025).

ISO/IEC (2022) *Information Security Risk Management (ISO/IEC 27005:2022)*. Geneva: International Organization for Standardization. Available at: https://www.iso.org/standard/80585.html (Accessed: 23 October 2025).

Kahneman, D. (2011) *Thinking, Fast and Slow*. London: Penguin.

Marks, L. (2019) 'The optimal risk management framework: Identifying the requirements and selecting the framework', *ISACA Journal*, 1(2019). Available at: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-optimal-risk-

management-framework-identifying-the-requirements-and-selecting-the-framework (Accessed: 23 October 2025).

National Institute of Standards and Technology (NIST) (2024) *Cybersecurity Framework v2.0*. Gaithersburg, MD: U.S. Department of Commerce. Available at: https://www.nist.gov/cyberframework (Accessed: 23 October 2025).

Rolfe, G., Freshwater, D. and Jasper, M. (2001) *Critical Reflection for Nursing and the Helping Professions: A User's Guide*. Basingstoke: Palgrave Macmillan.

University of Edinburgh (2020) *Reflective Writing: A Basic Introduction*. Available at: https://www.ed.ac.uk/reflection/reflective-writing (Accessed: 23 October 2025).