**My Learning Journey in Security and Risk Management**

**Introduction**

The Security and Risk Management (SRM) module has been one of the most valuable parts of my MSc Cyber Security studies. It changed how I approach security, moving from focusing only on technical controls to understanding human behaviour, collaboration, and governance. I'm using Rolfe’s (2001) What? So What? Now What? model and the University of Edinburgh’s (2020) advice to reflect on my experience during this course.

**What?**

In the beginning, I approached IT security as a technical job. Standards like ISO/IEC 27005 and NIST CSF v2.0 seemed to be theoretical. But through my work on the first four units, I realised these frameworks actually help create processes around organisations. Understanding that risk = threat × vulnerability × impact changed how I assessed controls and made me realise that governance gives direction to technology.

The GDPR case study was a real eye-opener. Examining a real public-sector data breach that violated the GDPR act made me realise that data protection is fundamentally about respecting people's trust, not just encrypting files. Connecting technical steps with ethics made me appreciate privacy-by-design much more, and I became more aware of how mistakes can cause real data breaches.

The Pampered Pets project was a standout moment. Working in a team of five, we met three times on Microsoft Teams and used WhatsApp for coordination. I contributed by reviewing sections, monitoring the word count, and helping align the report with ISO 27005 and NIST CSF mappings. Initially, I hesitated to share opinions, preferring to complete my part quietly. With feedback and encouragement, I became more confident in discussing mitigation strategies and supporting the team. This shift helped me see that leadership is not about control; it is about listening and trust. Since my professional role already involves a high degree of collaboration, I was able to adapt naturally and work effectively within this team.

During quantitative risk modelling (QRM) and business continuity/disaster recovery (BC/DR), my analytical skills improved. I struggled with probability concepts at first, but understanding Monte Carlo simulation and Bayesian updating completely changed how I viewed uncertainty when it is actionable and measurable. I understood risk management as a balance between logic and interpretation rather than pure calculation. When studying multi-cloud DR architectures, I could connect these academic insights with my professional experience in hybrid failover and synchronous replication. It was satisfying to see that theory explained the rationale behind decisions I already experienced at work.

**So What?**

I learnt that technology can only succeed when supported by communication, empathy, and governance. While working with the team, seeking support and transparent communication helped to create healthier team dynamics. This mirrored NIST CSF’s “Communicate” and “Respond” functions, showing that transparency improves collective resilience.

Midway through the module, I faced significant personal and health challenges. Illness, stress, and anxiety made it hard to balance work, study, and family life. After completing the group project, I seriously considered taking a break from the course. It was my wife’s encouragement that helped me continue; she reminded me that giving up would only extend the struggle. Her belief restored my confidence.

During recovery, I missed several live seminars. I regained focus and joined the BC/DR seminar, which became a highlight. The discussion comparing on-premises, multi-cloud, and hybrid DR strategies led to an engaging debate on cost, latency, and compliance. Connecting these perspectives with ISO 22301 and ENISA guidance helped me critically evaluate resilience beyond tools and technical capabilities, focusing instead on organisational culture.

During this phase, I recovered from illness, which gave me a state of happiness that extended beyond grades. The unit on behavioural economics also changed my mindset. Understanding that biases influence professional judgement made me reflect on how sometimes I over-rely on technical evidence instead of considering cultural or emotional factors. This insight will help me approach future decisions with greater self-awareness, ensuring that I am accountable for both human and technical dimensions of security.

**Now What?**

This module has encouraged me to see learning as continuous improvement. Professionally, I want to expand my horizon on quantitative risk analysis, cloud resilience, and threat modelling, which directly relate to my current role in IT operations. These development goals are reflected in my skills matrix and PDP included within the e-portfolio, where I have outlined specific actions toward learning, such as AWS Disaster Recovery Solutions and Bayesian risk modelling, aligning with my plan to complete the GDPR Practitioner and AI in Cyber Security certifications.

Equally, I intend to strengthen my emotional intelligence and reflective habits. Inspired by the University of Edinburgh’s (2020) guidance, I now maintain a short journal after major work projects, noting what went well, what failed, and how I felt. This simple habit turns stress into something useful and keeps me focused when things get tough.

In collaborative environments, I will prioritise transparent communication. During the Pampered Pets project, I realised that teams thrive when members feel heard and respected.  Looking ahead, I plan to integrate the lessons from SRM into my career path. By combining frameworks like ISO 27005 with tools like QRM, now I can evolve from a technical engineer into a more strategic cyber-risk leader. The ultimate goal is not only to secure systems but also to strengthen a culture where trust, accountability, and continuous learning drive resilience.

**Conclusion**

Completing the SRM module has been transformative with analytical risk assesemnt. I started with limited awareness of governance, ethics, and human factors. However I see security as a living discipline that depends on both analytical precision and emotional strength. Through structured reflection, teamwork, and personal recovery, I have grown into a more self-aware and balanced professional. I understand that resilience applies to people as much as to infrastructure, and that risk management is not merely a compliance task but an ethical commitment to protect others. As I continue my MSc journey, I carry forward a new mindset where integrity, empathy, and continuous reflection define what it truly means to be secure.

**References**

ENISA (2022) *Business Continuity Management – Good Practices.* European Union Agency for Cybersecurity.  
European Union (2016) *General Data Protection Regulation (EU 2016/679).* Available at: <https://gdpr.eu/> (Accessed 20 Oct 2025).  
ISO/IEC (2022) *Information Security Risk Management (ISO/IEC 27005:2022).* Geneva: International Organization for Standardization.  
Ridley, M., Ng, W. and Johnson, S. (2018) ‘Autonomous Cyber Defence Systems: Opportunities and Challenges’, *Journal of Information Security,* 9(2), pp. 95–107.  
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.* [Online] Available at: <https://www.ed.ac.uk/reflection/reflective-writing> (Accessed: 20 Oct 2025).