End of Module Assignment – e-Portfolio Submission

Module: Security and Risk Management (July 2025 B)
Student: Pragadheesh Marimuthu
Word Count: Approx. 2 000 words (Reflection ~ 1 000 words)
e-Portfolio Web Link:
https://pragadheesh-dev.github.io/security-risk-management
(The full e-Portfolio containing artefacts from Units 1–12, assessments, and evidence is accessible via the web link above.)

---

1. Overview

This e-Portfolio represents my complete learning journey through the *Security and Risk Management* module. It integrates artefacts, seminar reflections, collaborative discussions, and project outputs from all twelve units. The portfolio demonstrates how my understanding evolved from basic risk definitions to complex quantitative modelling, disaster-recovery design, and critical evaluation of emerging trends.

The main focus of this submission is on reflective synthesis how I developed practical competence in risk assessment, threat modelling, and business-continuity planning while strengthening analytical and professional skills. Artefacts from each unit showcase applied knowledge, collaboration, and continuous improvement. The final 1000-word reflection consolidates my insights, aligning with the learning outcomes of identifying, analysing, and mitigating security risks using structured and quantitative methods.

---

2. Summary of Artefacts (U1–U12)

UNIT	ARTEFACT / ACTIVITY	DESCRIPTION & LEARNING OUTCOME
1 – 3	*Collaborative Discussion 1*	Explored user participation in the Risk Management Process (RMP) through forum posts and peer responses. Recognised how stakeholder input shapes control effectiveness.
4	*Threat Modelling Exercises*	Applied STRIDE, attack trees, and DREAD/CVSS scoring. Learned structured analysis and prioritisation of threats vs business impact.
5	*GDPR Case Study*	Evaluated controller/processor obligations and data-protection impacts under GDPR; developed a compliance mapping approach.
6	*Team Risk Identification Report*	Conducted dual risk assessments (Pampered Pets current vs digitalised state). Linked ISO 27000, PCI-DSS and GDPR controls to identified threats.
7 – 9	*Collaborative Discussion 2*	Critiqued CVSS limitations and integrated SSVC/EPSS models to inform risk-based decision making for BC/DR planning.
9	*BC/DR Design Artefacts*	Produced RTO/RPO tables, tiered recovery plans, and test cadence notes to link risk scores to resilience targets.
10	*DR Solutions Workshop*	Analysed readings (Sutton 2021; Popov et al. 2021) to compare DRaaS, hybrid cloud, and vendor lock-in issues. Documented assumptions and control options.
11	*Individual Executive Summary*	Modelled supply-chain risk using Monte Carlo simulation and Bayesian probability; recommended continuity design and hosting platform selection.
12	*The Great Debate + Final Reflection*	Analysed emerging SRM trends (AI, Zero-Trust, Automation). Consolidated learning through final reflection and professional development evaluation.

Note: All artefacts are available in the GitHub portfolio and represent both individual and team-based learning activities.

---

3. Final Reflective Piece (≈ 1 000 words)

Completing this module has reshaped my understanding of **Security and Risk Management (SRM)** from a compliance checklist into a **strategic, evidence-based discipline**. I learned to connect theory with practice from identifying threats to modelling their probability and implementing resilience strategies. My journey through the twelve units reflects both **technical progression** and **professional growth**.

Understanding the Foundations

In the first two units, I learned the fundamentals of the Risk Management Process (RMP): defining risk, understanding organisational context, and recognising the influence of **user participation**. I realised that stakeholder input is critical for identifying real operational vulnerabilities often missed by purely technical assessments. Through discussions, I developed an appreciation for balancing **qualitative vs quantitative** methods understanding that numbers provide structure, but human judgement ensures relevance.

Developing Analytical Techniques

Units 3 and 4 introduced me to structured threat-modelling frameworks such as **STRIDE**, **DREAD**, and **attack trees**, which replaced my earlier ad-hoc approaches. By constructing models for the Pampered Pets scenario, I learned how to connect specific threats to potential mitigations and then to relevant industry standards. The hands-on practice deepened my analytical thinking and improved my ability to communicate risk relationships visually and logically.

Applying Standards and Compliance Frameworks

In Units 5 and 6, my focus expanded to security standards such as **GDPR**, **ISO 27000**, and **PCI-DSS**. The *GDPR case study* and *Risk Identification Report* taught me to translate compliance into measurable control objectives. Collaborating with peers on the team project improved my coordination and version-control skills using GitHub. I learned to justify why specific frameworks fit the company's context rather than applying them generically.

Quantitative Thinking and Modelling Risk

Units 7 to 9 were transformative. I transitioned from descriptive risk scoring to **quantitative risk modelling** using tools like **Monte Carlo simulation**, **Bayesian analysis**, and decision trees (**SSVC**). These methods helped quantify uncertainty rather than eliminate it. Critically, I learned the limitations of **CVSS**, its static scoring and subjectivity and explored **EPSS** to predict real-world exploitation probabilities. This blend of models allowed me to derive probabilities of disruption and prioritise mitigations based on empirical data.

The link between quantitative modelling and **Business Continuity and Disaster Recovery (BC/DR)** became clear during these units. I used RTO/RPO values to translate risk scores into resilience targets. This marked my shift from theoretical modelling to operational planning.

Designing for Continuity and Resilience

Unit 10 strengthened my applied skills through a *DR Solutions Design and Review* workshop. Analysing readings by **Sutton (2021)** and **Popov et al. (2021)** helped me evaluate **DRaaS** options, hybrid cloud setups, and the risks of vendor lock-in. I learned that effective DR design relies on defining *assumptions*, *dependencies*, and *verification cycles*. The practical emphasis on testing recovery objectives reinforced the importance of documenting decisions (Sutton, 2021) and maintaining transparency in resilience planning.

Understanding Future Trends

In Unit 11, I produced the *Executive Summary* my most demanding and rewarding assessment. It required applying **Monte Carlo** and **Bayesian** modelling to evaluate the impact of digitalisation on supply-chain quality and continuity. This unit taught me to blend academic reasoning with business communication skills producing concise, executive-level recommendations grounded in quantitative analysis. I also explored future SRM trends such as **AI-driven threat detection**, **Zero-Trust architecture**, and **automation of control verification**, evaluating how these shape risk governance.

Synthesising Learning and Reflection

The final debate in Unit 12 connected the entire module. It challenged me to justify which SRM trend would dominate the next five years and to articulate the reasoning behind that prediction. I recognised that the **future of SRM** lies in balancing automation with human oversight combining predictive analytics with ethical decision-making.

Across the module, I improved not only my technical competence but also my **reflective and collaborative practice**. Working with peers taught me negotiation, documentation, and critical feedback skills. I also learned to see uncertainty as a variable to be managed, not feared. A mindset essential for cybersecurity leadership.

Professional and Personal Development

Professionally, this module advanced my ability to think like a **security risk analyst** interpreting data, justifying controls, and communicating risk impact to stakeholders. Personally, it strengthened my resilience, time management, and adaptability. I now appreciate that the most effective SRM practitioners combine technical depth with ethical awareness and continuous learning.

Moving forward, I plan to:

1. Pair qualitative judgement with quantitative modelling (SSVC + EPSS + Monte Carlo).
2. Maintain a live standards-to-controls register aligned with data flows.
3. Express resilience in tested RTO/RPO metrics.
4. Document uncertainty and assumptions for transparency and auditability.
5. Continue developing through professional certifications and industry engagement.

In essence, this e-Portfolio captures my evolution from understanding isolated security concepts to mastering an integrated, data-driven approach to risk management. The journey reinforced that **effective SRM is not about eliminating risk but about understanding, quantifying, and managing it strategically**.

---

4. Conclusion

This portfolio reflects my learning trajectory across all twelve units from foundational definitions to quantitative risk modelling and future-trend evaluation. The artefacts and reflections demonstrate consistent progress towards critical thinking, technical competence, and strategic awareness. The integration of qualitative and quantitative methods has enhanced my ability to link risk data with organisational priorities and to propose resilient, ethically sound solutions.

---

5. References

Aven, T. (2016) *Risk assessment and risk management: Review of recent advances on their foundation.* European Journal of Operational Research, 253(1), 1–13.

Aven, T. and Thekdi, S. (2024) *Risk Science: An Introduction.* 2nd ed. Oxon: Routledge.

Popov, G., Lyon, B.K. and Hollcroft, B.D. (2021) *Risk Assessment: A Practical Guide to Assessing Operational Risks.* Wiley.

Sutton, D. (2021) *Resilient Cybersecurity for Business Continuity.* London: Kogan Page.

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

The University of Edinburgh *Reflection Toolkit.* Available at: https://www.ed.ac.uk/reflection/toolkit (Accessed 19 October 2025).
