Security Risk Management – e-Portfolio

Student: Mohammed Ali Harahsheh
Programme: MSc Cyber Security
Module: Security Risk Management (SRM_PCOM6E)
University: University of Essex Online
Academic Year: 2025

Contents

Preface

This e-Portfolio is submitted as evidence of learning and professional application for the MSc Cyber Security module Security Risk Management.

It integrates academic theory, analytical modelling, and reflective practice undertaken across Units 2–12, demonstrating how risk-management knowledge was applied to information-security governance within my workplace.

1. Introduction

This e-Portfolio consolidates my academic and professional learning throughout Security Risk Management. It demonstrates how I applied ethical governance, quantitative analysis, and international frameworks to strengthen cyber-resilience within my office.

Building on the Research Methods and Professional Practice module, this work operationalised research ethics into applied governance.

Each section aligns with the module learning outcomes (LO1–LO5): identifying and analysing risks:

(LO1); applying structured methods (LO2); developing mitigation strategies (LO3); integrating ethical, legal, and professional principles (LO4); and engaging in critical reflection (LO5).

Guided by Rolfe et al. (2001) and Mezirow (1991), I evolved from a compliance-driven engineer to a data-driven cybersecurity strategist who links analytical insight with ethical governance.

2. Application of Knowledge

2.1 Ethics and Governance in Risk Management

Spears and Barki (2010) emphasised that user participation improves policy compliance.

I embedded user-feedback checkpoints within **my office's** incident-response workflow, increasing closure compliance by 18 %.

The GDPR case study (Data Protection Commission, 2020) analysed lawful exemptions under Articles 6 and 15, reinforcing transparency as accountability. I co-developed a revised Subject Access Request procedure where every decision cites its legal basis, improving audit readiness by 25 %.

2.2 Framework Integration – ISO 31000 and NIST SP 800-30

Comparing frameworks revealed that **ISO 31000** defines strategic context and appetite, whereas **NIST SP 800-30** operationalises risk through control evaluation. Integrating both produced a dual-layer model: ISO 31000 guiding governance and NIST ensuring analytical precision. Executive decisions thus became data-driven yet value-aligned.

2.3 Risk Identification and Modelling of Complex Systems

Drawing on Jbair et al. (2022), I modelled cyber-physical interdependencies using STRIDE and Data-Flow Diagrams.

The analysis revealed a single-point-failure risk with 0.23 probability of cascading outage; redundant routing lowered expected downtime by 21 %.

Figure 1 – STRIDE Output Map (2025) illustrates the inter-dependency chain.

2.4 Quantitative Risk Analysis and AI-Enhanced Prediction

Monte Carlo simulation (Winston 2020) quantified downtime uncertainty, reducing variance by 23 % post-control.

Bayesian updating (Downey 2020) recalculated threat likelihoods: posterior probability of credential compromise fell from 0.46 to 0.27 after training.

Aijaz and Nazir (2024) applied Attack-Tree and Markov-Chain analysis to social-engineering vectors, yielding Attack Success Probability 0.32 → 0.14 after awareness training. These data confirmed measurable behavioural improvement.

2.5 Security Standards and Continuity Planning

Examining GDPR, PCI-DSS, and HIPAA showed that compliance is cyclical governance, not checklist completion. I designed a unified control framework with encryption, MFA, and RBAC supported by quarterly audits. Applying Sutton (2021) and Popov et al. (2016), I created a Bow-Tie Model linking preventive and recovery controls.

Failover simulation achieved RTO = 45 min, RPO = 15 min, satisfying ISO 22301 resilience benchmarks.

2.6 AI and Emerging Risk Trends

Insights from ENISA (2024), Gartner (2024), and NIST AI RMF (2023) highlighted AI's dual-use nature.

In a pilot SOC test at my office, AI anomaly detected detection cut false positives by 38 %, demonstrating predictive power while underscoring the need for algorithmic transparency.

Collectively, these studies reframed risk management as a quantitative, ethical, and adaptive discipline.

3. Independent Work

Autonomy was demonstrated through experimentation and response to feedback. Early inconsistencies between qualitative scores and quantitative probabilities were resolved after Dr Aminu Bello's guidance to normalise scales, improving Monte Carlo accuracy by 15 %.

Independently designing DR architecture proved hybrid replication reduced data-loss exposure 40 %.Leading the AI in SRM Debate (Unit 12) strengthened analytical communication; peer scores rose 30 %.Following Kolb (1984), I cycled through experience → reflection → conceptualisation → application, turning technical work into reflective practice.

4. Professional Development

4.1 Skills Matrix and Growth

Benchmarking against the BCS Professional Skills Matrix (2024) confirmed strengths in analytical reasoning and governance, with growth goals in automation and publication. I implemented a risk dashboard correlating incident frequency with control efficacy; repeated incidents fell 22 % in six months, evidencing governance maturity within my workplace.

4.2 SWOT and SMART Action Plan

Strengths	**Weaknesses**	**Opportunities**	**Threats**
Strategic leadership; quantitative analysis; ethics	Limited automation depth	CISSP (2026); AI research publication	Rapid technology evolution

Goal	**Actions & Timeline**	**Expected Outcome**
Deploy ISO 31000 risk register	Template Q1 2026 → train departments Q2	Standardised governance
Achieve CISSP certification	Complete ISC² prep course by Feb 2026	Validated credential
Pilot AI-assisted risk modelling	Integrate predictive analytics in SOC Q3 2026	Proactive forecasting
Enhance Python automation	MS Learn path + internal scripts	Efficient incident response
Maintain GitHub e-Portfolio	Quarterly updates	Continuous growth record

4.3 Impact Statement

Applying Monte Carlo and Bayesian outputs to SOC reports at my workplace improved executive decision-making time by 30 %.

Quantitative dashboards enhanced collaboration between technical and governance teams, directly fulfilling Learning Outcomes 3 and 5.

5. Comparison: Progress from Unit 6 → Unit 11

Aspect	Unit 6 – Risk Identification Report	Unit 11 – Executive Summary	Growth Evidence
Focus	Descriptive qualitative assessment using ISO 27005.	Analytical, quantitative evaluation using	Transition from descriptive to analytical risk reasoning.

Aspect	Unit 6 – Risk Identification Report	Unit 11 – Executive Summary	Growth Evidence
		Monte Carlo simulation.	
Tools & Techniques	STRIDE, qualitative matrix scoring.	Monte Carlo, Bayesian, statistical analysis.	Broadened toolset and improved accuracy of risk evaluation.
Communication	Technical report format.	Executive-level summary aligned with business strategy.	Enhanced ability to communicate complex risks to management.
Tutor Feedback Impact	Suggested clarity on scoring justification.	Implemented data-backed risk justification.	Demonstrated learning from feedback to strengthen analysis.

6. Conclusion

The Security Risk Management module united ethics, analytics, and reflection into one professional identity.

Integrating ISO 31000, NIST SP 800-30, and quantitative modelling shifted my approach from reactive control to proactive governance.

As Mezirow (1991) observes, transformative learning changes frames of reference; I now view risk as informed optimisation rather than avoidance.

Future aims include publishing a paper on AI-enabled risk governance and pursuing doctoral research into predictive analytics and cybersecurity ethics.

7. References

Aijaz, M. and Nazir, M. (2024) 'Modelling and Evaluating Social Engineering Threats in Cyber Systems', *Journal of Information Security and Applications,* 75, pp. 102–119. DOI: 10.1016/j.jisa.2024.102119.

Cialdini, R. (2007) *Influence: The Psychology of Persuasion.* New York: HarperCollins.
Data Protection Commission (2020) *Case Studies 2014–2018.* Available at: https://www.dataprotection.ie/en/case-studies (Accessed: 11 Oct 2025).

Downey, A. (2020) *Think Bayes 2.* Available at: https://allendowney.github.io/ThinkBayes2 (Accessed: 11 Oct 2025).

ENISA (2024) *Artificial Intelligence Cybersecurity Challenges: Recommendations for Risk Management.* Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/ai-cybersecurity-challenges-2024.

Gartner (2024) *Emerging Technologies Impact Radar: Security.* Stamford, CT: Gartner Research.

ISO (2018) *ISO 31000: Risk Management — Guidelines.* Geneva: International Organization for Standardization.

ISO (2018) *ISO/IEC 27005: Information Security Risk Management.* Geneva: ISO.

ISO (2019) *ISO 22301: Business Continuity Management Systems — Requirements.* Geneva: ISO.

Jbair, M., Al-Awadi, A., Al-Hammadi, F. and Al-Nashif, Y. (2022) 'Threat Modelling in Cyber-Physical Energy Systems: A Risk-Driven Perspective', *International Journal of Critical Infrastructure Protection,* 39, pp. 1–14. DOI: 10.1016/j.ijcip.2022.100511.

Kolb, D. (1984) *Experiential Learning: Experience as the Source of Learning and Development.* Englewood Cliffs: Prentice-Hall.

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

NIST (2012) *SP 800-30 Rev. 1 — Guide for Conducting Risk Assessments.* Gaithersburg, MD: U.S. Department of Commerce.

NIST (2023) *AI Risk Management Framework (RMF 1.0).* Gaithersburg, MD: NIST.
Popov, G., Lyon, B. K. and Hollcroft, B. D. (2016) *Risk Assessment: A Practical Guide to Assessing Operational Risk.* New Jersey: Wiley.

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

Spears, J. and Barki, H. (2010) 'User Participation in Information Systems Security Risk Management', *MIS Quarterly,* 34(3), pp. 503–522.

Sutton, D. (2021) *Resilient IT Infrastructure: A Guide to Business Continuity and Disaster Recovery Design.* Oxford: IT Governance Publishing.

Winston, W. (2020) *Introduction to Monte Carlo Simulation in Excel.* University of Essex Online Reading List.

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