End of Module E-Portfolio

Module: SRM\_PCOM7E — Security and Risk Management

Student: Aisha Hussain Ahmed Alhussain

Group: 3

Submission Date: 20 October 2025

E-Portfolio URL: https://github.com/Aishahussain9/EPortfolio

# Executive Summary

This e-portfolio presents my learning, development, and project outcomes from the Security and Risk Management module. It compiles artefacts from module units from1 to 12 , at Units 6 and 11 my project was about the Pampered Pets case study, demonstrating my ability to apply structured risk management methodologies, coordinate teamwork, and lead a digital transformation project. Unit 6 focused on an initial risk assessment using the OCTAVE Allegro methodology, while Unit 11 expanded into an integrated Business Continuity and Risk Mitigation Framework using advanced techniques (ANP-TOPSIS, ISO standards).

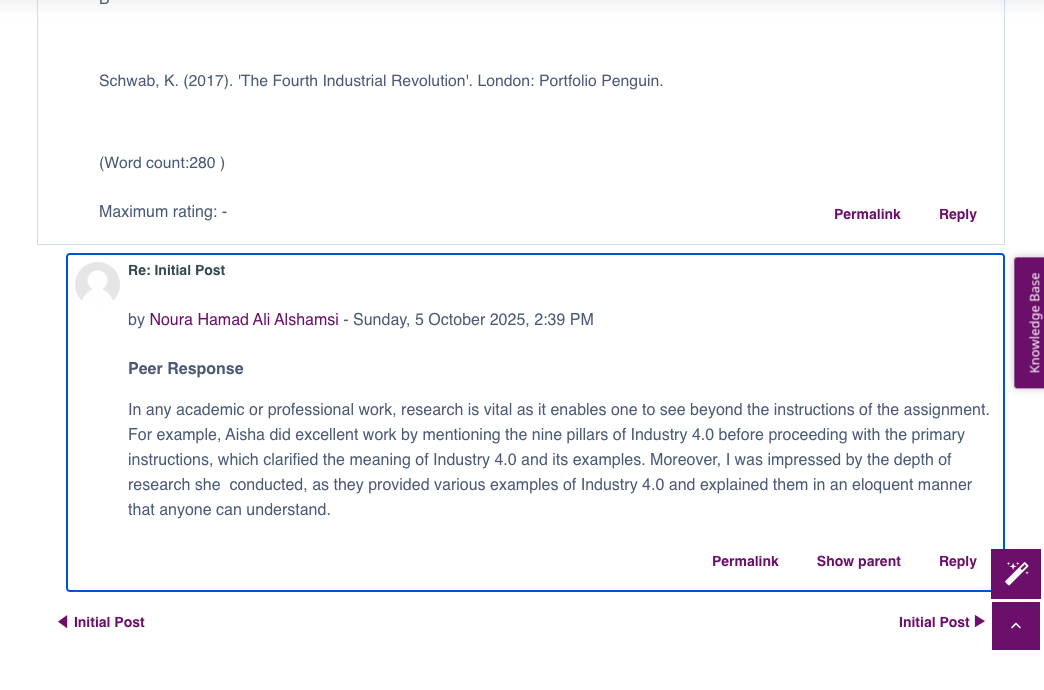
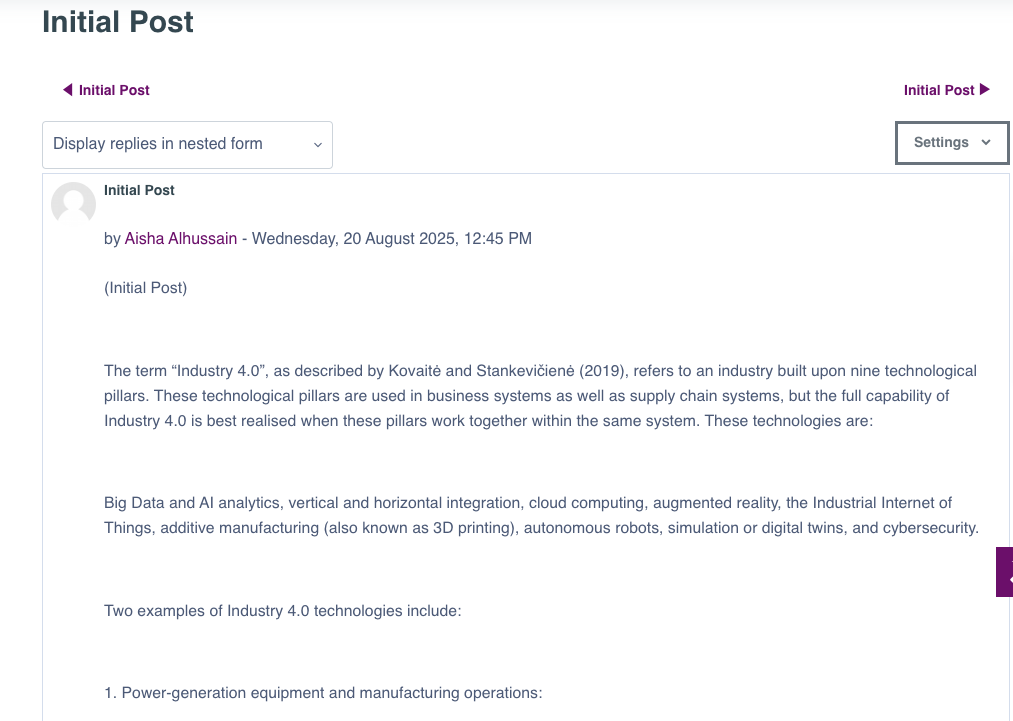
Security and Risk Management E-Portfolio

# 1. Unit 1 Artefact Summary: Introduction to Security and Risk Management

In Unit 1, I was introduced to the fundamentals of Security and Risk Management (SRM), exploring key concepts, terminology, and frameworks. The module emphasised the importance of understanding the threat landscape, risk assessment approaches, and organisational security posture. The activities included reflective exercises, collaborative discussions, and initial risk analysis tasks that allowed me to begin developing a practical understanding of risk environments. This unit laid the groundwork for subsequent units by highlighting how structured processes, such as identifying assets, threats, and vulnerabilities, underpin effective SRM strategies.

Learning outcomes met: LO1; LO2.

Figures 1 and 2: Unit 1 collaboration learning discussing of Kovaitė and Stankevičienė case study, 2019 and Peer review of my initial post of the case study.

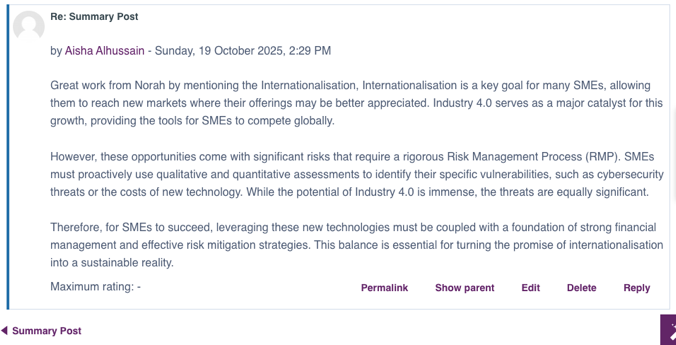
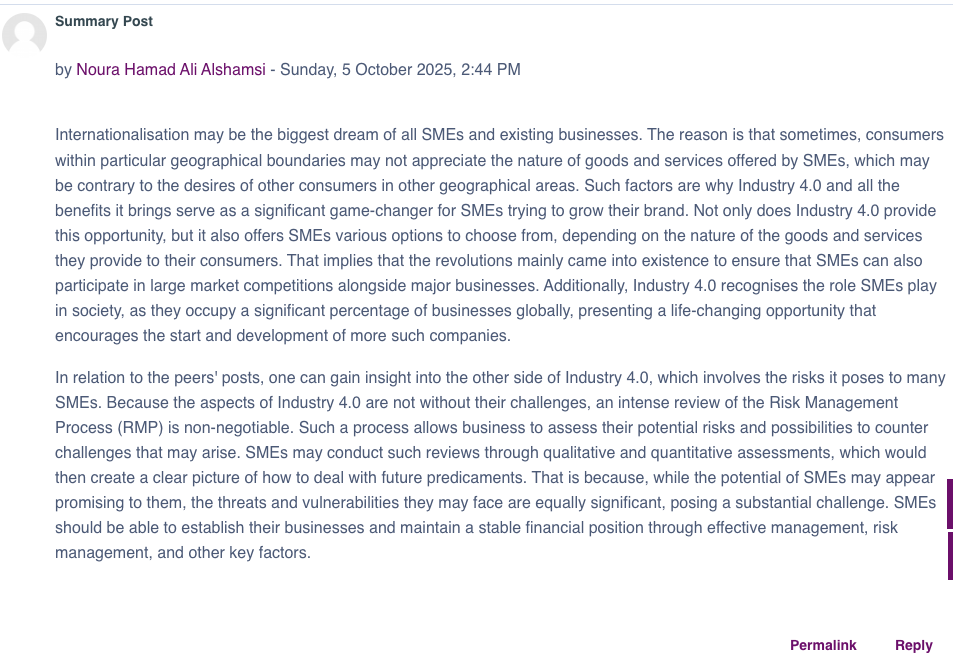


# 2. Unit 2 Artefact Summary: Users, Assessments and the Risk Management Process

Unit 2 focused on the Risk Management Process (RMP) with particular emphasis on user participation and assessment approaches (Qualitative vs. Quantitative). I explored the implications of different assessment methods, and how increased user involvement can improve the accuracy and applicability of risk mitigation strategies. The seminar and collaborative discussions enhanced my understanding of the RMP, demonstrating the significance of participatory risk evaluation and its effect on organisational decision-making.

Learning outcomes met: LO1; LO2.

Figures 3 and 4: Collaborative learning discussion in Unit 2 with my student colleagues and my peer review.

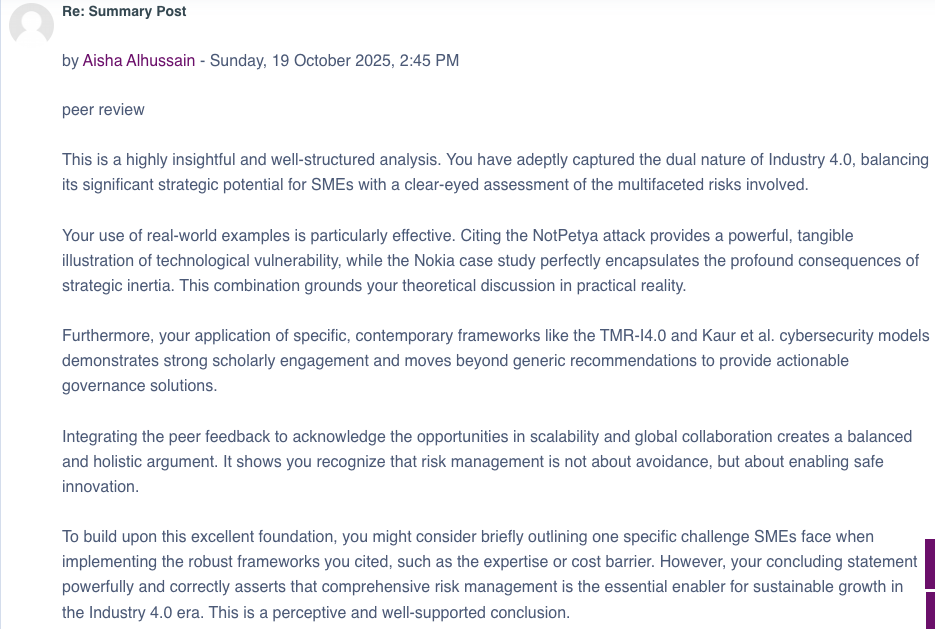


# 3. Unit 3 Artefact Summary: Introduction to Threat Modelling and Management

In Unit 3, I explored various threat modelling techniques including STRIDE, DREAD, Attack Trees, and PASTA. This unit helped me distinguish between threats and vulnerabilities, and provided guidance on selecting appropriate models for specific contexts. Activities included applying theoretical knowledge to case studies and evaluating different threat modelling tools, which strengthened my analytical and problem-solving skills in anticipating potential risks.

Learning outcomes met: LO1; LO2.

Figures 5 and 6: Collaborative learning discussion in Unit 3 with my student colleagues and my peer review.

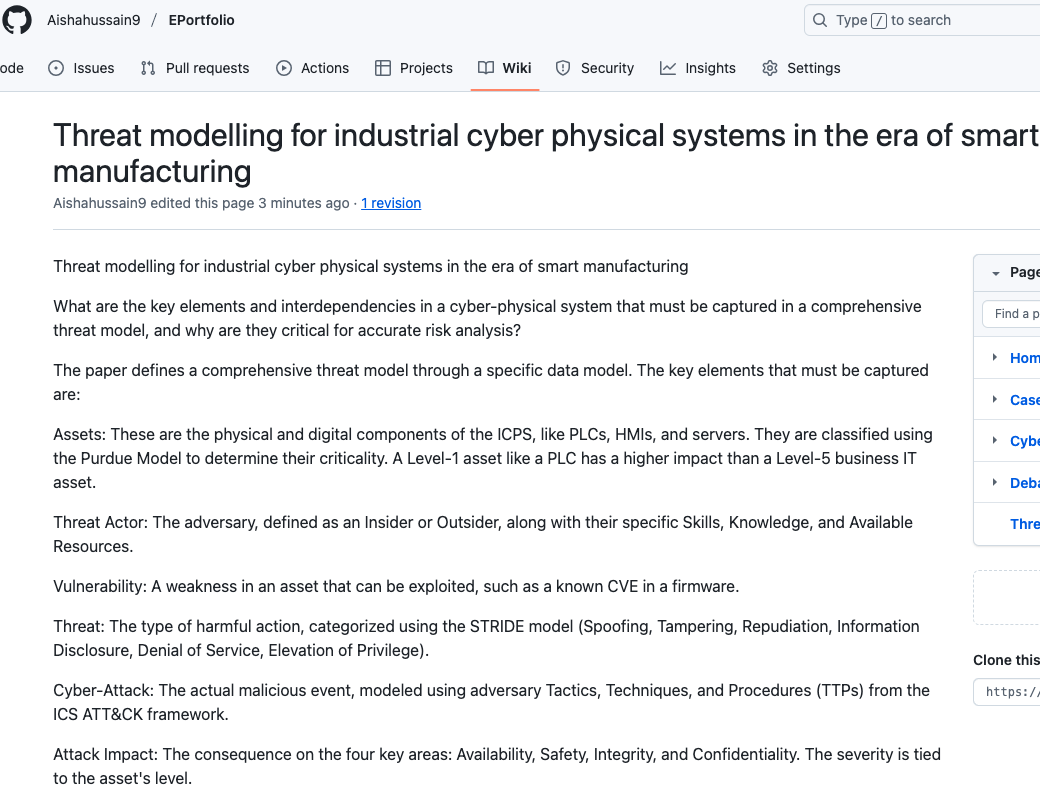


# 4. Unit 4 Artefact Summary: Application of Threat Modelling and Management Techniques

Unit 4 applied threat modelling concepts through practical exercises using tools such as OWASP cookbooks and Mitre ATT&amp;CK database. I developed threat models based on real-world scenarios and evaluated the effectiveness of different approaches. This hands-on experience deepened my understanding of selecting suitable threat management techniques, improving critical evaluation and decision-making skills in cyber risk contexts.

Learning outcomes met: LO1; LO2.

Figures 7: Case study activity of Unit 4 (Threat modelling for industrial cyber physical systems in the era of smart manufacturing) my solution page at GitHub in the below link: <https://github.com/Aishahussain9/EPortfolio.wiki.git>



# 5. Unit 5 Artefact Summary: An Introduction to Security and Risk Standards in Industry and the Enterprise

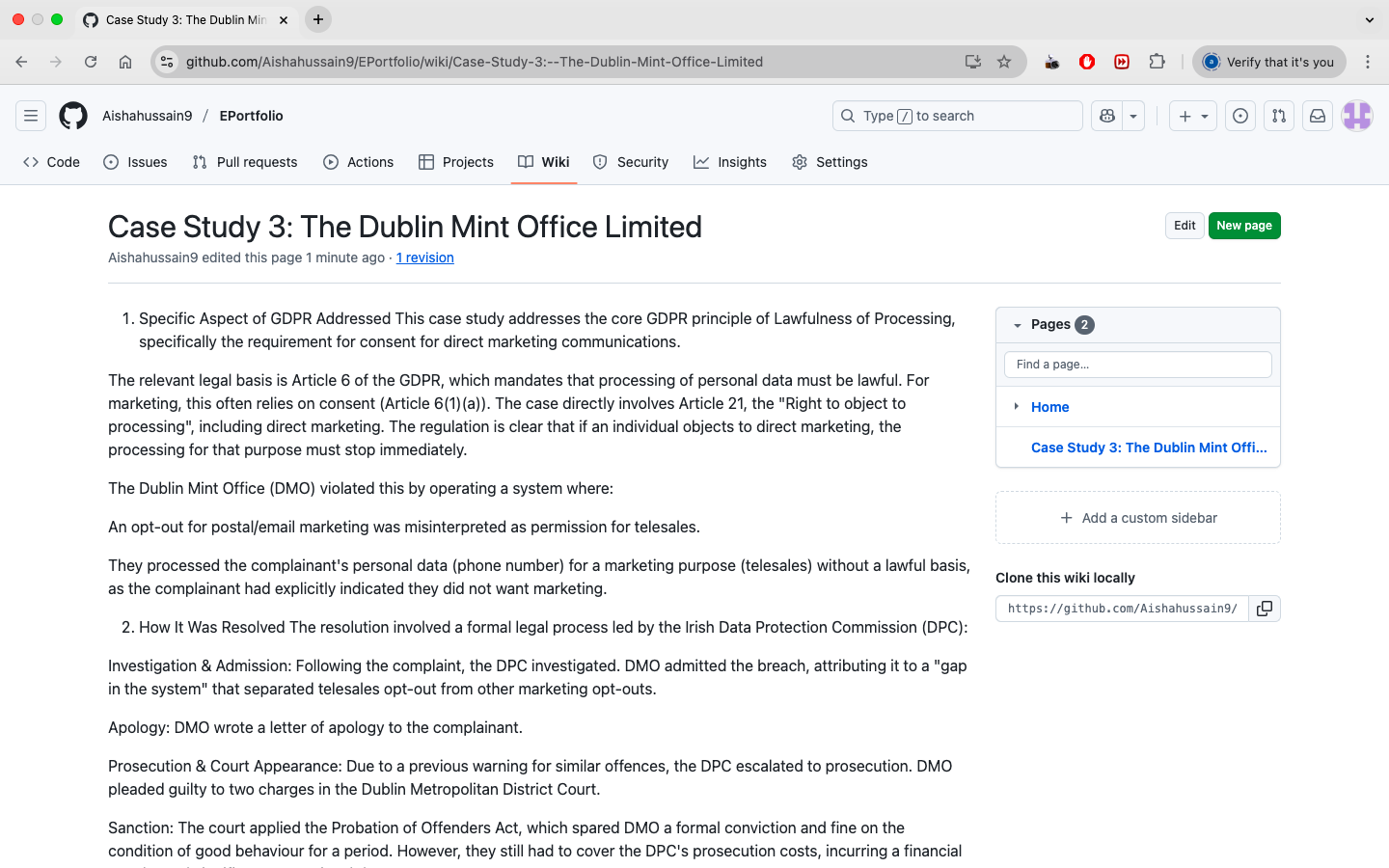
Unit 5 introduced industry and enterprise security standards, discussing their role in risk assessment and mitigation planning. I analysed standards such as GDPR, PCI-DSS, and ISO frameworks, applying them to hypothetical scenarios to evaluate compliance requirements. The unit fostered an understanding of how standards influence organisational policies and decision-making, reinforcing analytical skills and knowledge of regulatory frameworks.

Learning outcomes met: LO1; LO2; LO3.

Unit 5 (The Dublin Mint Office Limited) case study activity solved through my E-Portfolio WIKI page at GitHub check the link below:

<https://github.com/Aishahussain9/EPortfolio.wiki.git>

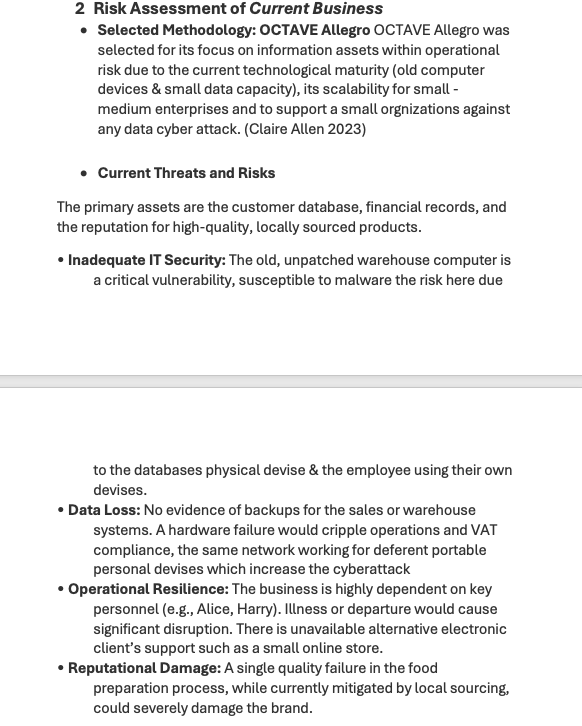
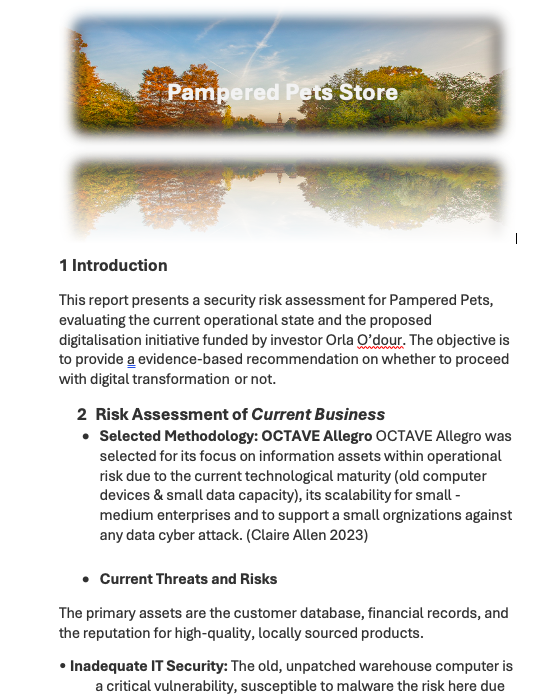
Figures 8: Case Study No3 of Unit 5 (The Dublin Mint Office Limited) activity solved through my E-Portfolio WIKI page at GitHub



# 6. Unit 6 Artefact Summary and Pampered Pets Risk Assessment Project Report

In Unit 6, I produced the Pampered Pets Risk Assessment Report independently due to limited team engagement. The report evaluated the organisation’s readiness for digitalisation, identifying major vulnerabilities such as unpatched systems, lack of data backups, and absence of formal security policies. Using the OCTAVE Allegro methodology, I assessed risks related to IT infrastructure, data loss, operational resilience, and reputational exposure.  
  
Key mitigation strategies included implementing a patch management policy a Deployments strategy by using structured 3-2-1 backup: three standby backup, and creating Standard Operating Procedures (SOPs). Additionally, GDPR compliance and other relevant standards were considered to ensure regulatory alignment. This project strengthened my analytical and technical understanding of small business risk environments and taught adaptability, resilience, and initiative as a team organiser.  
  
Learning outcomes met: Identified and analysed security risks (LO1); Applied systematic risk methodologies (LO3).

Figures 9 and 10: Using the OCTAVE Allegro methodology at Pampered Pets Risk Assessment Project Report

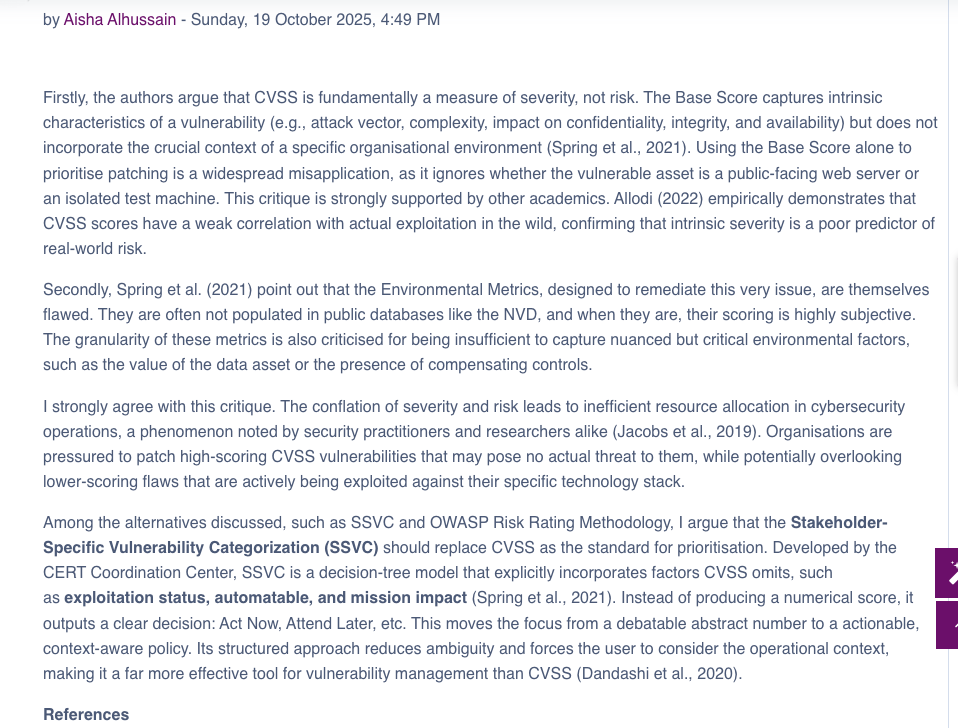


# 7. Unit 7 Artefact Summary: An Introduction to the Concepts of Quantitative Risk Modelling

Unit 7 provided an introduction to quantitative risk modelling (QRM) techniques, including Monte Carlo simulations, Bayesian models, and multi-criteria decision analysis (TOPSIS, AHP, ANP). I applied theoretical principles to evaluate real-world risk scenarios and critically assessed the suitability of various methods. This enhanced my ability to select and justify quantitative modelling approaches and reinforced my analytical skills in probabilistic risk evaluation.

Learning outcomes met: LO1; LO3.

Figures 11: my initial post at the Collaborative learning discussion at Unit 7 .



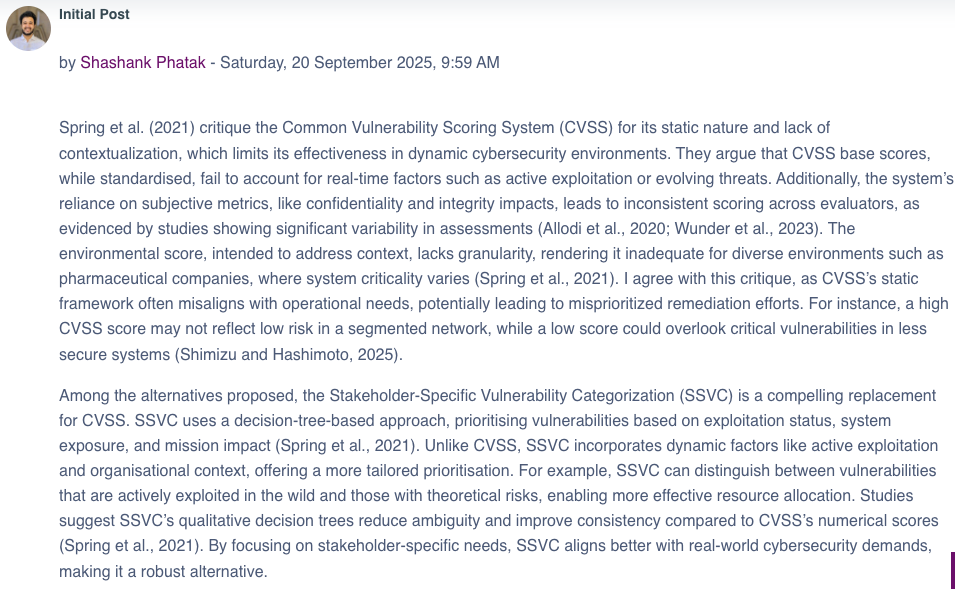
# 8. Unit 8 Artefact Summary: Implementing Quantitative Risk Models

Unit 8 focused on the practical implementation of quantitative risk models. I applied Monte Carlo simulations and Bayesian approaches to real-world case studies, creating quantitative models to predict and mitigate risks. This unit developed my capability to critically assess modelling results, select the most appropriate techniques, and integrate QRM into organisational risk management practices.

Learning outcomes met: LO1; LO3.

Figures 12 and 13: Collaborative learning discussion in Unit 8 with my student colleagues and my peer response.

A screenshot of a email

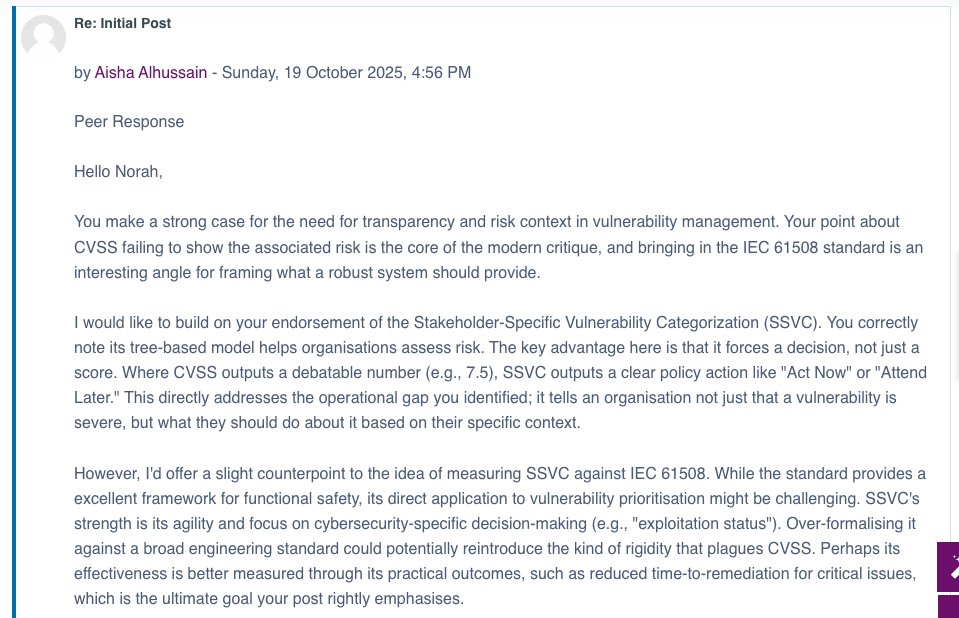
Description automatically generated

# 9. Unit 9 Artefact Summary: Risk, Business Continuity and Disaster Recovery

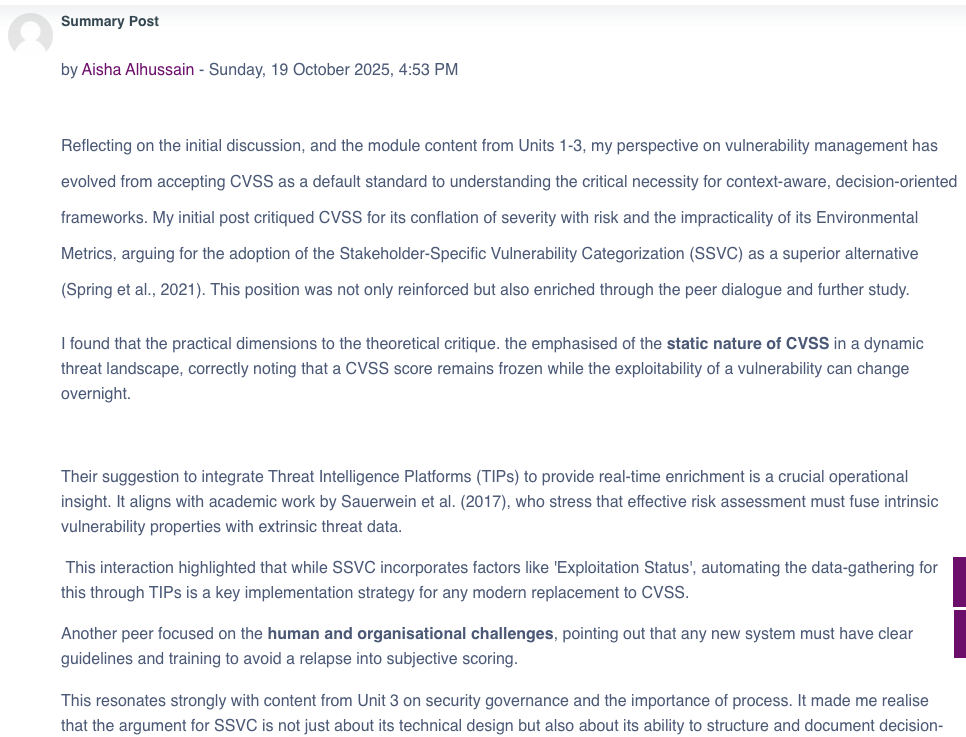
Unit 9 examined business continuity (BC) and disaster recovery (DR) planning. I explored factors such as Business Impact Assessments (BIA), Recovery Time Objectives (RTOs), and Recovery Point Objectives (RPOs). The unit emphasised the importance of proactive planning and strategic response to mitigate operational disruptions. Activities included analysing case studies and evaluating emerging trends in information risk management, strengthening my strategic planning and risk evaluation capabilities.

Learning outcomes met: LO1; LO2; LO3.

Figures 14 and 15: Collaborative learning discussion in Unit 9 with my student colleagues and my peer response.



Figures 16: my summary post at the Collaborative learning discussion at Unit 7 .



# 10. Unit 10 Artefact Summary: Practical Applications and Issues in DR Implementations

In Unit 10, I explored the practical implementation of disaster recovery (DR) solutions, including designing systems to meet specific RPO and RTO requirements. I critically assessed the advantages and limitations of DRaaS and other standby solutions, considering factors such as vendor lock-in, resilience, and network security. This unit reinforced practical problem-solving skills in implementing effective DR strategies.

Learning outcomes met: LO1; LO3.

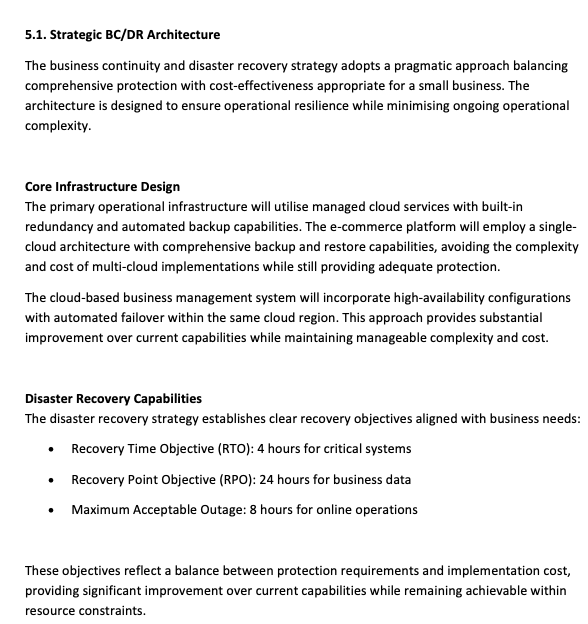
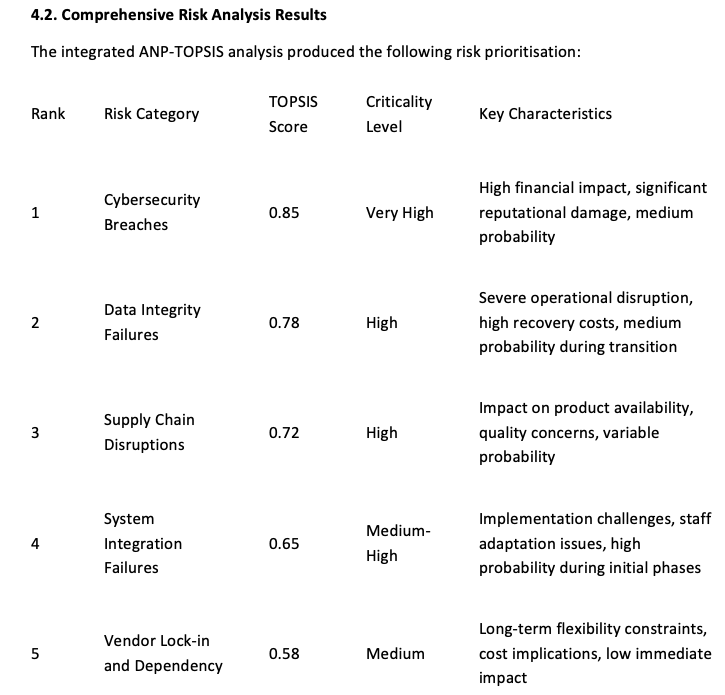
Unit 10 (Cyber‐Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies) case study activity solved through my E-Portfolio WIKI page at GitHub check the link below:

<https://github.com/Aishahussain9/EPortfolio.wiki.git>

# 11. Unit 11 Artefact Summary of Comprehensive Risk Assessment and Business Continuity Strategy

In Unit 11, I acted as project report leader, producing a professional executive report titled Comprehensive Risk Assessment and Business Continuity Strategy for Pampered Pets. This phase extended the earlier work by implementing advanced multi-criteria decision-making (MCDM) techniques such as Analytic Network Process (ANP) and TOPSIS to prioritise risks.  
  
The final strategy focused on integrating Business Continuity and Disaster Recovery (BC/DR) within a cloud-based transformation plan. It applied ISO 22301 and ISO/IEC 27001 frameworks to mitigate high-priority risks such as cybersecurity breaches, data loss, and vendor lock-in.  
  
Leading the project, I coordinated research, engaged the methods and the frameworks, and ensured structured presentation aligned with ISO standards. The project reporting management role improved my professionalism, technical, and risk quantification skills.  
  
Learning outcomes met: Applied technical frameworks for mitigation (LO3); Demonstrated collaboration and leadership (LO4).

Figures 17 and 18: implementing advanced multi-criteria decision-making (MCDM) techniques such as TOPSIS and Business Continuity and Disaster Recovery (BC/DR) at Comprehensive Risk Assessment and Business Continuity Strategy for Pampered Pets



# 12. Unit 12 Artefact Summary: The Great Debate: Future Trends in Security and Risk Management

Unit 12 concluded the module by debating emerging trends in Security and Risk Management (SRM) for the next five years. Drawing on Unit 11 readings and wiki entries, I critically evaluated the potential influence of trends such as AI, automation, and economic impacts on SRM. The debate facilitated reflective thinking and persuasive argumentation, strengthening my ability to anticipate future challenges and contribute informed recommendations to organisational strategy.

Learning outcomes met: LO3; LO4.

Unit 12 (Debate Brief: The Most Influential Trend in SRM in the Next 5 Years) case study activity solved through my E-Portfolio WIKI page at GitHub check the link below:

<https://github.com/Aishahussain9/EPortfolio.wiki.git>

# 13. Evaluation: Unit 11 (Final Project) vs Unit 6 (Status Report)

The progression from Unit 6 to Unit 11 marks clear professional and methodological growth. In Unit 6, the Pampered Pets Risk Assessment relied primarily on qualitative analysis using OCTAVE Allegro, producing high-level mitigation plans. However, by Unit 11, I evolved from simple identification to quantified and evidence-based risk prioritisation using ANP-TOPSIS models.  
  
The Unit 11 strategy also incorporated compliance frameworks (ISO 27001, ISO 22301, GDPR), demonstrating a shift toward a holistic and standard-driven approach. While Unit 6 addressed operational security gaps, Unit 11 presented an enterprise-level risk mitigation and continuity plan.  
  
As project report leader, I also improved in managing collaboration and quality control transforming a mostly individual exercise in Unit 6 as well as a structured, data-driven was managed at a professional way in project of Unit 11.

**Summary of my Progression**

This analysis shows a logical pedagogical structure of my learning outcomes:

* **LO1 & LO2:** form the foundational core, established in the first half of the module.
* **LO3:** represents the sustained application and technical that enhanced my deepening of skills, becoming my primary focus in the middle and later units.
* **LO4:** represents the culmination of the learning journey, where technical knowledge is integrated with essential professional skills like leadership and strategic communication in my real-world context.

My learning outcomes through module of Security and Risk Management:

|  |  |  |  |
| --- | --- | --- | --- |
| **LO** | **Definitions** | **Evidence** | **Coverage** |
| **LO1** | Identified and analysed security risks by Understand fundamental concepts, principles, and the threat landscape of Security and Risk Management. | This outcome is met in almost every unit, especially the early ones, which cover fundamentals, terminology, threat modelling techniques (STRIDE, DREAD, PASTA, Attack Trees), and understanding the general risk environment. | Unit 1 to 10 |
| **LO2** | Understand fundamental concepts, principles, and the threat landscape of Security and Risk Management. | This is covered in units focusing on the Risk Management Process (RMP), assessment approaches (Qualitative vs. Quantitative), applying threat modelling, and business continuity planning (BIA, RTO, RPO). It is less frequent in units focused purely on advanced quantitative modelling or leadership. | Unit 1 to 5 and unit 9 |
| **LO3** | Applied systematic risk methodologies, frameworks, standards, and advanced analytical techniques to assess and mitigate risk. | This outcome becomes prominent from Unit 5 onwards. It relates to the practical application of standards (GDPR, PCI-DSS, ISO), quantitative models (Monte Carlo, Bayesian), multi-criteria decision-making techniques (ANP, TOPSIS, AHP), and designing practical disaster recovery solutions. | Unit 5 to 11 |
| **LO4** | Demonstrate professional skills, including collaboration, leadership, and communication, in the context of risk management. | This is exclusively met in the final, capstone-style units (Unit 11 and Unit 12) where you took on a leadership role in a project, managed collaboration, and engaged in persuasive communication and debate on future trends. | Unit 11 and 12 only |

# 14. Reflective Piece (Rolfe’s Model: What? So What? Now What?)

**WHAT?**

This reflection analyses my learning and personal growth throughout the Security and Risk Management module.  
At the start, I approached risk management as a checklist activity identifying threats and suggesting basic mitigations.

on my journey through the fundamentals of Security and Risk Management, I have gained a comprehensive understanding of the Risk Management Process, appreciating the critical role of user participation and mastering the nuanced application of both qualitative and quantitative assessment approaches; this was brought to life as I explored various threat modelling techniques like STRIDE, DREAD, Attack Trees, and PASTA, and applied these concepts practically using resources such as the OWASP cookbooks and the Mitre ATT&CK database.

My analysis extended to critical standards including GDPR, PCI-DSS, and ISO frameworks, where I honed my ability to identify vulnerabilities like unpatched systems, insufficient backups, and absent formal policies, often employing the OCTAVE Allegro methodology to structure these assessments. The course further provided a solid introduction to quantitative risk modelling, demystifying techniques like Monte Carlo simulations and Bayesian models, which I then applied to real-world case studies, while also implementing advanced multi-criteria decision-making methods such as ANP and TOPSIS to systematically prioritize risks.

Finally, I examined the vital disciplines of business continuity and disaster recovery planning, delving into Business Impact Assessments, RTOs, and RPOs, and explored the practical implementation of DR solutions by designing systems tailored to meet specific recovery objectives, thereby connecting strategic policy with technical resilience.

I examine my experience in leading the Pampered Pets Digital Transformation project, my understanding of risk management frameworks, and my professional development.

In Unit 6, I independently completed the risk assessment using OCTAVE Allegro, due to limited team engagement. This experience forced me to apply theory practically, make rapid decisions, and deliver a complete report on time.  
  
By Unit 11, my understanding evolved significantly. As a security consultant, I integrated quantitative and multi-dimensional methods (ANP-TOPSIS) and aligned the strategy with international standards such as ISO 27001, ISO 22301, and GDPR. I led the report drafting, coordinated feedback, and ensured consistency between technical and business objectives.  
 **SO WHAT?**

This journey taught me several key lessons about both security risk management and teamwork.  
  
**Understanding the Risk Management Process:**I realised that risk management is not simply about listing vulnerabilities; it is a continuous, data-driven process. Moving from qualitative (OCTAVE) to quantitative (ANP-TOPSIS) frameworks helped me appreciate the value of measurable prioritisation. I learned to balance impact, probability, and interdependence among risks through my projects at this module .

The Unit 11 report’s integration of financial, operational, and reputational criteria demonstrated how technical risks translate into business consequences a critical skill for a future cybersecurity leader or as a business owner also as a security consultant as well.  
  
**My Role in Team Tasks and Leadership:**  
In Unit 6, I experienced frustration due to minimal team communication.

However, this challenge revealed my natural inclination for leadership. I initiated early distributed tasks, and ensured the work progressed at the professional way.

This proactive behaviour continued into Unit 11, where I enhanced my expertise as a report consultant and project leader by orgnised the report tasks due to the requirements as well as leading the risk quantification process strengthened my analytical and management skills.

Further, I successfully developed my project leadership capabilities by independently managing my time and tasks to deliver projects.  
  
**Teamwork Experience:**  
My teamwork journey improved from my independently. Initially, I struggled with lack of engagement from peers, but through this challenge improved my natural inclination for project and report management. I initiated early tasks schedule time by my own, and ensured the work progressed at the time.

**Personal and Professional Growth:**  
This module profoundly improved my technical and interpersonal competencies. I enhanced project report management skills, time management, technical risk analysis, problem solving, and confidence.  
  
**NOW WHAT?**

Moving forward, I intend to apply these lessons to my academic and professional development. Specifically, within my current career, I will leverage this expertise to enhance my contributions to projects by implementing the various models, methodologies, and standards across the company's project systems.  
  
**Continuous Learning and Certification:**  
I plan to enhance my risk management expertise by pursuing professional certifications such as CompTIA Security+, ISO 27001 Lead Implementer, and BCI Business Continuity Certification.  
  
**Improving Leadership and Collaboration:**  
I will continue developing my leadership style by applying servant-leadership principles focusing on empathy, communication, and accountability. In future group projects, I will establish early communication channels, define roles clearly, and use collaborative tools to prevent miscommunication.  
  
**Applying Risk Frameworks in Real Scenarios:**  
The analytical approaches (ANP-TOPSIS) and frameworks (ISO, NIST, OCTAVE) have given me confidence to analyse complex business systems. I will use these methods in future work placements or consultancy projects, adapting them to real-world organisations.  
  
**Personal Growth and Lifelong Reflection:**  
Reflecting through this module made me realise that learning is iterative.

Every challenge from team delays to complex frameworks contributed to my resilience and adaptability.

I will maintain reflective journaling as part of my professional development plan (PDP) to continuously assess my growth, identify weaknesses, and plan improvement actions.

In summary this module fundamentally transformed my approach from merely identifying security risks to managing them strategically within broader business and human contexts. Moving beyond foundational concepts, I applied the full Risk Management Process, emphasizing user participation and mastering both qualitative and quantitative assessment methods.

This involved exploring threat modelling techniques like STRIDE and PASTA with OWASP and MITRE ATT&CK, analysing standards from GDPR to ISO, and identifying critical vulnerabilities.

The module equipped me with a robust analytical toolkit from applying OCTAVE Allegro and quantitative models like Monte Carlo simulations to real-world cases, to using advanced MCDM techniques like ANP and TOPSIS for risk prioritization.

Furthermore, examining business continuity and designing disaster recovery plans against specific RTOs and RPOs grounded strategic policy in technical reality.

The confidence and analytical discipline I gained will guide me in future roles as well as in my current career at a system provider company as a business development engineer and particularly in leading secure digital transformations that balance innovation with risk resilience, ensuring security is an integral enabler of business objectives.

# 6. References

Rolfe, G., Freshwater, D., & Jasper, M. (2001). Critical Reflection in Nursing and the Helping Professions: A User’s Guide. Basingstoke: Palgrave Macmillan.  
University of Edinburgh (n.d.). Reflection Toolkit. Available at: https://www.ed.ac.uk/reflection/reflectors-toolkit/reflecting-on-experience (Accessed: 16 October 2025).  
Claire Allen (2023). Threat Modeling Methodology: OCTAVE. Iriusrisk. Available at: https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies (Accessed: 25 August 2025).  
NIST (2018). Cybersecurity Framework. Available at: https://www.nist.gov/cyberframework/csf-11-archive (Accessed: 25 August 2025).  
Saaty, T.L. (1996). Decision Making with Dependence and Feedback: The Analytic Network Process. Pittsburgh: RWS Publications.  
Hwang, C.L. & Yoon, K. (1981). Multiple Attribute Decision Making: Methods and Applications. Berlin: Springer-Verlag.  
ISO 22301:2019. Business Continuity Management Systems – Requirements.  
ISO/IEC 27001:2022. Information Security Management Systems.  
Adrienne Wilkerson (2024). Be Honest: Show Your Team Your Human Side. BeaconMM. Available at: https://www.beaconmm.com/2024/06/19/be-honest-show-your-team-your-human-side (Accessed: 6 September 2025).  
Andrew Langat (2024). Mastering Team Leadership: 10 Proven Strategies for Success. Highrise. Available at: https://www.tryhighrise.com/blog-posts/team-leadership (Accessed: 6 September 2025).  
British Retail Consortium (2024). Digital Transformation in SME Retail.