|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| **Reflective Portfolio for Security and Risk Management** |
| |  |  |  | | --- | --- | --- | | Milad Chowdhury | 1/25/25 | Security and Risk Management October 2024 | |

Contents

[E-Portfolio URL: https://mc24887.github.io/Reflective-Piece-for-E-Portfolio 2](#_Toc188699059)

[Introduction 2](#_Toc188699060)

[Reflection Using Gibbs’ Reflective Cycle 2](#_Toc188699061)

[1. Description 2](#_Toc188699062)

[2. Feelings 2](#_Toc188699063)

[3. Evaluation 2](#_Toc188699064)

[4. Analysis 2](#_Toc188699065)

[Integrated Skill Development and Action Plan 3](#_Toc188699066)

[1. Certifications and Training Plan 3](#_Toc188699067)

[2. Skill Matrix and Action Plan 3](#_Toc188699068)

[3. Time Spent on Skill Development 3](#_Toc188699069)

[4. Skill Development Focus Areas 3](#_Toc188699070)

[5. Cognitive Development Using Bloom's Taxonomy 3](#_Toc188699071)

[Critical Assessment 4](#_Toc188699072)

[1. Strengths 4](#_Toc188699073)

[2. Areas for Improvement 4](#_Toc188699074)

[Conclusion 4](#_Toc188699075)

[References 5](#_Toc188699076)

# E-Portfolio URL: <https://mc24887.github.io/Reflective-Piece-for-E-Portfolio>

# Introduction

This reflective piece explores my academic and professional development during the Security and Risk Management (SRM) module. Using Gibbs’ Reflective Cycle (1988), I critically assess key experiences, challenges, and personal growth throughout the module. Drawing on practical exercises, seminars, and collaborative projects, this reflection highlights the evolution of my skills and outlines actionable steps for future improvement.

# Reflection Using Gibbs’ Reflective Cycle

## 1. **Description**

During this module, I engaged in several hands-on activities, including:

* Conducting Monte Carlo simulations to quantify risks (e.g., supply chain delays and cybersecurity breaches).
* Participating in a collaborative threat modelling exercise using the STRIDE and DREAD frameworks.
* Contributing to developing a Disaster Recovery (DR) strategy with considerations for RPO and RTO metrics.

These experiences allowed me to apply theoretical knowledge to practical scenarios, enhancing my understanding of risk identification and mitigation strategies.

## 2. Feelings

Initially, I felt overwhelmed by the complexity of integrating multiple frameworks and methodologies. For example, using STRIDE and Monte Carlo simulations simultaneously required careful attention to detail. However, collaborative discussions and peer feedback boosted my confidence, particularly during seminars where my contributions were acknowledged. By the end of the module, I felt a strong sense of accomplishment in applying these skills effectively.

## 3. Evaluation

**Strengths:**

* My ability to synthesise data from different frameworks (e.g., STRIDE and Monte Carlo) was instrumental in identifying vulnerabilities.
* Active participation in group discussions improved my collaborative and analytical skills.

**Weaknesses:**

* My initial threat models lacked depth, as I often focused on isolated risks without considering compounded impacts.
* Time management was a challenge when balancing individual tasks and group contributions.

## 4. Analysis

The module underscored the importance of structured frameworks for effective risk management. For instance, combining STRIDE with DREAD provided a balanced perspective on vulnerabilities, aligning with the best practices outlined by Shostack (2018). Additionally, feedback during group projects revealed areas for improvement, such as adopting a more holistic approach to risk prioritisation.

**Linking Theoretical and Practical Knowledge:** The iterative learning process throughout the module aligned with Kolb’s experiential learning cycle (1984), where reflective observation and abstract conceptualisation reinforced my understanding of core SRM principles. Additionally, Gibbs’ framework allowed me to critically evaluate each stage, providing a structured approach to my learning journey.

# Integrated Skill Development and Action Plan

## 1. Certifications and Training Plan

|  |  |  |
| --- | --- | --- |
| **Certification** | **Purpose** | **Timeline** |
| CISSP | Deepen expertise in cybersecurity and risk management. | 12 months |
| CRISC | Enhance skills in enterprise risk management. | 18 months |
| ISO 31000 Certification | |  | | --- | | Gain advanced risk management knowledge. |  |  | | --- | |  | | 12 months |
| Agile Project Management | Improve efficiency in managing security projects. | 9 months |

## 2. Skill Matrix and Action Plan

|  |  |  |  |
| --- | --- | --- | --- |
| **Skill** | **Initial Proficiency** | **Current Proficiency** | **Development Plan** |
| Threat Modelling | Intermediate | Advanced | Deepen use of MITRE ATT&CK |
| Risk Assessment | Beginner | Intermediate | Pursue formal certifications |
| Communication | Intermediate | Advanced | Practice scenario-based communication |
| Technical Proficiency | Intermediate | Advanced | Gain expertise in advanced frameworks |
| Time Management | Intermediate | Intermediate | Use project management tools |

## 3. Time Spent on Skill Development

|  |  |
| --- | --- |
| **Skill** | **Percentage (%)** |
| Risk Management | 40 |
| Threat Modelling | 35 |
| Communication and Teamwork | 15 |
| Report Writing | 10 |

## 4. Skill Development Focus Areas

|  |  |  |
| --- | --- | --- |
| **Focus Area** | **Target Improvement** | **Planned Actions** |
| Analytical Proficiency | Enhanced scenario analysis | Perform detailed risk modelling using new tools |
| Communication Skills | Improved stakeholder engagement | Develop scenario-based presentations |
| Time Management | Efficient task prioritisation | Utilise advanced project management software |

## 5. Cognitive Development Using Bloom's Taxonomy

Bloom’s Taxonomy provided a structured approach to learning progression, moving from foundational knowledge to higher-order cognitive skills.

**1. Remember:**

* Memorised foundational concepts like STRIDE, DREAD, and GDPR compliance requirements.
* Recalled key cybersecurity standards, such as ISO 31000, and their applications to real-world scenarios.

**2. Understand:**

* Gained a deeper understanding of how threat modelling frameworks like STRIDE categorise risks and aid in designing mitigation strategies.
* Interpreted Monte Carlo simulations to quantify risk probabilities and impacts.

**3. Apply:**

* Applied DREAD to evaluate the severity and prioritisation of threats in the Pampered Pets and banking scenarios.
* Implemented risk management practices like encryption protocols to enhance GDPR compliance.

**4. Analyse:**

* Critically analysed risk mitigation frameworks by comparing STRIDE to alternatives like PASTA.
* Evaluated gaps in organisational risk strategies and provided actionable recommendations for improvement.

**5. Evaluate:**

* Assessed the effectiveness of disaster recovery solutions based on RPO and RTO metrics.
* Critically evaluated team contributions in group projects, identifying collaboration strengths and weaknesses.

**6. Create:**

* Designed tailored disaster recovery plans for varying RPO and RTO requirements.
* Created risk prioritisation matrices and actionable strategies for threat mitigation.

# Critical Assessment

## 1. Strengths

* **Analytical Proficiency:** Conducting Monte Carlo simulations and STRIDE assessments significantly enhanced my analytical capabilities.
* **Collaboration:** Facilitating discussions during team projects improved my ability to align group efforts with project goals.

## 2. Areas for Improvement

* **Depth in Analysis:** My initial assessments lacked a comprehensive exploration of alternative strategies.
* **Time Management:** Balancing individual and group tasks required better prioritisation and scheduling.

# Conclusion

Reflecting on this module has provided valuable insights into my strengths and areas for improvement. The resources in my e-portfolio better prepare me for cybersecurity and risk management challenges, emphasising continuous learning and collaboration.

Using frameworks like STRIDE and DREAD has reinforced best practices in risk assessment, while team feedback has enhanced my technical skills and stakeholder engagement. Developing scenario-based approaches and improving my communication skills will support my growth.

The module also highlighted the importance of aligning risk management strategies with global standards, including ISO 31000 and GDPR, to ensure compliance and resilience. This experience has equipped me with analytical tools and a collaborative mindset for complex cybersecurity challenges. As Gibbs (1988) suggests, reflective practice is essential for continuous improvement, and I am committed to applying this principle in my career.

# References

* Gibbs, G. (1988). *Learning by Doing: A Guide to Teaching and Learning Methods*. Oxford: Oxford Polytechnic.
* Bloom, B. S. (1956). *Taxonomy of Educational Objectives: The Classification of Educational Goals*. Handbook I: Cognitive Domain. New York: Longman.
* Kolb, D. A. (1984). *Experiential Learning: Experience as the Source of Learning and Development*. Englewood Cliffs, NJ: Prentice Hall.
* Shostack, A. (2018). *Threat Modelling: Designing for Security*. New York: Wiley.
* Zaoui, F. and Souissi, N. (2020). *Roadmap for Digital Transformation: A Literature Review*. Procedia Computer Science, 175, pp.621-628.
* Christopher, M. (2016). *Logistics & Supply Chain Management*. 5th ed. Harlow: Pearson Education Limited.
* NIST (2015). *Guide to Data-Centric System Threat Modeling*. [Online]. Available at: [Insert URL here].
* ENISA (2022). *Cybersecurity Risk Trends in Supply Chains*. [Online]. Available at: [Insert URL here].
* Trott, J. (2019). *Emerging Attacks on AI Systems*. International Journal of Cybersecurity, 12(4), pp. 56-72.
* Varshney, K. R., & Alemzadeh, H. (2017). *Safety in Machine Learning Systems*. Security and Risk Journal, 45(3), pp. 89-102.
* Hubbard, D. W. (2020). *Risk Modelling for Decision Makers*. Wiley.