

Title: Individual Reflective Piece

Introduction

This reflection discusses my experiences and learning outcomes from the Information Security Management (ISM) module in my MSc in Computer Science. The module enhanced my technical proficiency and contributed to professional and personal growth. As a Data Protection Officer (DPO) interested in GDPR compliance, the knowledge gained has immense practical value.

Summary of Learning Outcomes

The ISM module explored information security management's legal, social, ethical, and professional dimensions. We learned techniques for threat modeling, risk assessment, and mitigation. The two main assignments, Risk Identification Report and developing Python application for Attack Tree Visualization, applied theoretical concepts practically.

Assignment 1: Risk Identification Report

The first assignment involved conducting comprehensive risk assessment for Pampered Pets (Appendix 1), considering both pre- and post-digitalization threats. Using the OCTAVE-S method, I honed my skills in identifying and evaluating potential risks, gaining insights into mitigating these risks. This assignment deepened my understanding of critical assets, threat profiles, and strategies for safeguarding organizational data.

Assignment 2: Attack Tree Visualization Application

The second assignment required developing Python application to visualize and evaluate attack trees (Appendix 2). With no prior experience in Python visualization tools, I researched libraries like PyVis, NetworkX, and Tkinter. Unlike the previous module, this one did not provide Codio training and an Integrated Development Environment (IDE) for our coding assignment. Therefore, I self-learned and utilized Visual Studio Code (VS Code), which I intend to continue using. This assignment pushed me beyond the provided learning resources, refining my programming abilities and equipping me with the skills to present complex security concepts clearly.

Unit 1: Introduction to Security and Risk Management

Unit 1 provided a foundation in security and risk management basics. We discussed various definitions and concepts of risk, enhancing my understanding of the complexities involved. Real-world discussions, like those on data privacy and security risks at UnitedHealth Group and Boeing 737 MAX, highlighted the importance of effective risk management (Appendix 3).

Unit 2: Threat Modelling Exercises

In Unit 2, we focused on threat modeling and management. I selected large international bank for Threat Modeling Exercises (Appendix 4), improving my understanding of tools like STRIDE, DREAD, OWASP, and the ATT&CK framework. Applying these tools in realistic scenarios helped me grasp their practical applications.

Unit 3: Introduction to Threat Modelling and Management

Security Standards Exercise (Appendix 5) where we researched regulations like GDPR, PCI Security Standards, and HIPAA. We applied this knowledge to Pampered Pets, building my understanding of how regulations impact digital security.

Unit 4: Security Standards, Frameworks, and Disaster Recovery

As a DPO with PECB ISO/IEC 27001 Foundation certification , this unit was my favorite and particularly relevant. Collaborative Wiki (Appendix 6) taught me how to choose the right framework based on an organization's needs and regulations. GDPR CCTV case studies (Appendix 7) directly related to my job, aiding in creating a Data Protection Policy for CCTV monitoring. The Disaster Recovery Solutions Design and Review activity (Appendix 8) was timely, coinciding with discussions on system downtime tolerance with our headquarters IT department.

Unit 5 and 6: Future Trends in ISM

The final units focused on future trends in information security management, including AI and automation. Collaborative Wiki (Appendix 9) and debates on impactful trends highlighted the evolving landscape of ISM.

Professional Skills Matrix and Action Plan (PDP)

This module significantly improved my professional skills. I am now better at threat modeling, writing assessment reports, and understanding GDPR, essential for my role as DPO. Clear communication of risk assessments has enhanced interactions between management and IT teams.

Professional Skills Matrix

Level of competence (Rewo, 2024)



No Competence



High Competence



Low Competence



Expert





Some Competence



Not relevant

Skills	Competence	Evidence
Time Management		Completed assignments on time despite a busy working schedule during the module.
Critical Thinking and Analysis		Used critical thinking in risk assessments and chose the best threat modeling approach for the case study.
Communication and Literacy		Participated in collaborative discussions, created risk identification report and developed attack tree visualization application.
IT and Digital		Self-learned VS Code and used PyVis, NetworkX, and Tkinter to complete the attack tree visualization.
Research		Researched OCTAVE-S, GDPR, and relevant security frameworks for different assignments.
Interpersonal		Kept an e-portfolio with reflections and key takeaways for each ISM unit.

Problem-Solving		Explored and used a new IDE for Python assignment when existing resources were not enough.
Ethical Awareness		Analyzed the GDPR CCTV case study, increasing awareness of data protection and privacy issues.

Action Plan

- **Exploring Advanced Topics:** Further study in advanced data protection, GDPR compliance, and related frameworks.
- **Practical Application:** Applying new knowledge in my role, particularly in GDPR compliance and data protection.
- **Continuous Learning:** Staying updated on the latest tools and techniques in information security through ongoing education, professional development, and certifications like ISO/IEC 27001 Lead Auditor.
- **Ethical Practices:** Ensuring all data protection and compliance projects adhere to ethical guidelines and best practices.
- **Dissertation Topic:** Considering focusing on compliance and framework development for specific digitalization use cases as my dissertation topic.

Conclusion

This module has been a transformative learning experience. Practical applications through assignments and real-world case studies solidified my understanding of complex

security concepts and equipped me with valuable skills directly applicable to my role as a DPO. The insights gained into GDPR compliance and security framework implementation are actively applied in my professional work. I look forward to continuing to expand my expertise and contribute to the evolving field of information security.

References

Di Silvestro, F. & Nadir, H. (2021) The Power of ePortfolio Development to Foster Reflective and Deeper Learning in an Online Graduate Adult Education Program. *Adult Learning* 32(4):154-164.

Rewo. (2024) What is a skills matrix. Available from: <https://www.rewo.io/skills-matrix-for-manufacturing/> [Accessed 21 July 2024].

University of Essex Online. (2024) *University of Essex Online Writing Guide Series – A short guide to Reflective Writing*. Essex: University of Essex Online.

Appendix 1 Risk Identification Report

→ https://helenhelene.github.io/eportfolio/ISM/ISM_A1.html

Assignment 1: Risk Identification Report

Table of Contents

1. Executive Summary
2. Methodology
3. Risk Assessment
 - 3.1. Maintain Status Quo
 - 3.1.1. Threat Profiles
 - 3.1.2. Mitigation Plan
 - 3.2. Proposed Changes
 - 3.2.1. Threat Profiles
 - 3.2.2. Mitigation Plan
4. Recommendations
5. Timeline
6. Conclusions Abbreviations and Acronyms Reference

1. Executive Summary


Pampered Pets (Figure 1) is considering a digital transformation to expand its business. This report evaluates the risks associated with current operations and proposed digitalization, offering risk mitigation strategies and assesses the advisability of this transformation.

Figure 1: Business Overview

Pampered Pets
Location: Haslington-on-the-Water
Product: Pet foods
Supply Chain: Local firm within a 10-minute driving distance
Employees:

- Alice - Owner/Manager
- Cathy - Shop Manager
- Andrea - Store Assistant
- Harry - Warehouse Manager

Operations:



Appendix 2 README of Attack Tree Visualization Application

→ https://helenhelene.github.io/eportfolio/ISM/ISM_A2.html

Assignment 2: README - Attack Tree Visualization Application

Attack Tree Visualization Application - Python Scripts

Overview

This application was developed to analyze the risks associated with Pampered Pets, a business considering digital transformation. The goal was to evaluate both the current operational risks (Pre-digitalisation) and the potential risks introduced by digitalisation (Post-digitalisation).


This Python application visualizes an attack tree based on a JSON input specification. The attack tree represents potential threats to a system, and users can assign values (monetary amounts or probabilities) to the leaf nodes. The application aggregates these values to determine the overall impact of identified threats. It uses the PyVis library to create an interactive graphical representation of the attack tree. The application is designed to be user-friendly and interactive, leveraging Python libraries to handle graph structures and visualizations. Users can easily input data and receive meaningful visual and numerical outputs.

Below Figure 1 illustrates the threats assessed by the OCTAVE-S method in the previous Risk Identification Report.

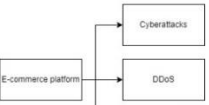
Figure 1: Threats of Pre-digitalisation and Post-digitalisation

Pampered Pets

Pre-digitalisation



Post-digitalisation



Appendix 3 Collaborative Discussion (Unit 1)

my-course.co.uk/mod/forum/discuss.php?d=235886

University of Essex Online

Search

2. Give two real-world examples of risks that fit into the authors' categories.

Kovaité & Stankevičienė (2019) list six types of risks with digitalisation: technical, competence, acceptance by staff, acceptance by customers, data privacy and security, and financial risks.

Data Privacy and Security Risks: A recent incident involved a cyberattack on UnitedHealth Group's claims processing unit, Change Healthcare. This unit processes 15 billion healthcare transactions annually and handles nearly half of all U.S. medical claims, involving one in every three patient records (Campisi, 2024).

Competence Risks: Boeing introduced the Maneuvering Characteristics Augmentation System (MCAS) in the 737 MAX, designed to automatically correct the aircraft's angle of attack. In 2018 and 2019, two Boeing 737 MAX aircraft were involved in fatal crashes—Lion Air Flight 610 and Ethiopian Airlines Flight 302. These disasters resulted in the loss of 346 lives and led to the global grounding of the 737 MAX fleet.

Investigations revealed that the Federal Aviation Administration (FAA) had inadequate awareness of the MCAS function, which allowed Boeing to have significant influence over the certification process of the 737 MAX (Herkert, 2020; Wasson, 2019).

Moreover, Boeing assured airlines that the MAX would handle exactly like the previous version of the 737 and recommended only a 30-minute self-study course for pilots on MCAS, rather than additional simulator or classroom instruction (Campbell, 2019).

This competence risk extended to both Boeing and regulatory bodies, showing a lack of comprehensive training, thorough testing, validation, and certification processes.

Knowledge Base

Appendix 4 Threat Modeling Exercises (Unit 2)

https://helenhelene.github.io/eportfolio/ISM/ISM_Unit02_Seminar.html

Unit 2 Seminar Exercise – Threat Model for a Large International Bank

Threat Modeling Process Summary

1. **Define the Scope:** Identify the system components and boundaries.
2. **Identify Assets:** Determine critical assets that need protection.
3. **Identify Threats:** Use STRIDE to categorize and identify potential threats.
4. **Analyze and Evaluate Threats:** Leverage frameworks like DREAD or ATT&CK to evaluate threats.
5. **Develop Mitigations:** Implement mitigations using guidelines from the OWASP Threat Modeling Cookbook.
6. **Validate:** Regularly review, test, and update the threat model.

Step 1: Define the Scope

System Description:

- Online banking platform
- Mobile banking applications
- Internal banking systems
- ATMs and physical branches
- Communication networks
- Data centers and cloud services

Step 2: Identify Assets

Critical Assets:

- Customer data (PII, financial information)
- Transaction data
- Online and mobile banking platforms
- Internal banking systems
- Network infrastructure
- Physical security systems (ATMs, branch security)
- Data centers and cloud services

Appendix 5 Security Standards Exercise (Unit 3)

https://helenhelene.github.io/eportfolio/ISM/ISM_Unit03_Exercise.html

Exercise: Security Standards

Introduction

This exercise is reviewing the following links/ websites and answer the questions below.

- [ICO - Guide to the General Data Protection Regulation \(GDPR\)](#).
- [PCI Security Standards.org](#). - Official PCI Security Standards Council Site - PCI Security Standards Overview.
- [HIPAA - HIPAA For Dummies – HIPAA Guide](#).

These standards are essential for protecting personal data, payment information, and health information. They provide guidelines for organizations to implement strong security measures and maintain compliance to protect sensitive information. Below are the key aspects of each standard:

General Data Protection Regulation (GDPR)

The GDPR is a comprehensive data protection law implemented by the European Union (EU) that has been in effect since May 25, 2018. GDPR is designed to protect the personal data and privacy of individuals within the EU and the European Economic Area (EEA). It also regulates the transfer of personal data outside these regions.

Key aspects of GDPR include:

- **Data Protection Principles:** Ensuring personal data is processed legally, fairly, and transparently.
- **Data Subject Rights:** Giving individuals rights such as access to their data, the right to correct or delete it, and the right to data portability.
- **Accountability and Governance:** Requiring organizations to show they comply with GDPR through proper documentation and assessments.
- **Penalties:** Imposing high fines for non-compliance, up to €20 million or 4% of the global annual turnover, whichever is higher.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a set of security standards to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. These standards were developed by the Payment Card Industry Security Standards Council (PCI SSC).

Appendix 6 Collaborative Wiki (Unit 4)

https://helenhelene.github.io/eportfolio/ISM/ISM_Unit04_Wiki.html

Collaborative Wiki Development - Security Frameworks

This exercise is reviewing the following article/ websites and answer the questions below.

- [Barafort et al \(2018\)](#)
- [Kirvan \(2023\)](#)

Section 1 : FAQ (frequently asked questions)

Q1: What are IT security frameworks?

IT security frameworks are structured guidelines that define policies, procedures, and processes to manage and mitigate information security risks. Examples include ISO 27001, NIST SP 800-53, and COBIT.

Q2: Why is it important for organizations to comply with IT security frameworks?

Compliance with IT security frameworks ensures that organizations have robust security measures in place to protect sensitive data, meet regulatory requirements, and reduce the risk of security breaches.

Q3: How do I choose the right IT security framework for my organization?

The choice of an IT security framework depends on factors like the industry, regulatory requirements, the size of the organization, and specific security needs. For example, healthcare organizations often use HITRUST due to its alignment with HIPAA.

Section 2: Responses to the Questions

Q1: Which of the frameworks do you think would be applicable to the following organisations:

- International bank.
- Large hospital.

Appendix 7 GDPR Case Studies (Unit 4)

→ ↻ 🔍 https://helenhelene.github.io/eportfolio/ISM/ISM_Unit04_GDPR.html 🔍 ☆ 📌

Optional Activity – GDPR Case Studies

This exercise is to choose a case study from the [Data Protection Commission \(2020\)](#) concerning GDPR-related issues and breaches and answer the questions below.

Summary of the 2018 Case Study 5: Disclosure of CCTV footage from a direct provision centre.

A complaint was filed by solicitors on behalf of a resident of a direct provision accommodation centre about the alleged unauthorized disclosure of CCTV footage capturing the complainant's images. The centre is state-owned, managed by Aramark Ireland on behalf of the Reception and Integration Agency (RIA). The disclosure came to light during a radio program where the host claimed to have the footage, which showed an altercation involving the complainant.

The complainant made complaints to RIA, Aramark, and the radio station. An access request was sent to RIA for details of all recipients of the disclosed data. However, RIA did not respond within the required 40-day period.

The Data Protection Commission (DPC) investigated and found that:

- **No Written Contract:** There was no written contract between RIA and Aramark delineating their data processing responsibilities, breaching Section 2C(3) of the Data Protection Acts 1988 and 2003.
- **Security Failures:** Both RIA and Aramark failed to ensure appropriate security measures to prevent unauthorized disclosure, violating Section 2(1)(d).
- **Non-Compliance with Access Request:** RIA failed to respond to the access request within the prescribed timeframe, contravening their obligations under the Data Protection Acts.

Despite thorough forensic IT investigations, neither RIA nor Aramark could definitively confirm that the footage had not been disclosed to the radio station. The DPC concluded that the complainant's rights were infringed due to inadequate data protection measures and lack of clear, documented policies and procedures. This case underscores the significant consequences of non-compliance with data protection obligations.

What is the specific aspect of GDPR that your case study addresses?

- **Data Subject Access Requests (DSARs):** This aspect pertains to the requirement under GDPR for data controllers to respond to access requests from data subjects within prescribed timeframes. In this case, the RIA failed to respond to an access request within the 40-day timeframe as mandated by the Data Protection Acts 1988 and 2003.

Appendix 8 DR Solutions Design and Review Activity (Unit 4)

→ ↻ 🔍 https://helenhelene.github.io/eportfolio/ISM/ISM_Unit04_Seminar.html 🔍 ☆ 📌

Unit 4 Seminar Exercise – Disaster Recovery (DR) Solutions Design and Review

Activities before Unit 4 seminar.

Activity 1: DR Terms and Concepts






Read [Alhazmi & Malaiya \(2013\)](#) and then answer the following questions:

Summary of Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

- Critical components of disaster recovery plans.
- Define acceptable data loss and system restoration time.
- Lower RPO and RTO require advanced and costly solutions.
- Balance based on business needs and resources.
- Carefully assess RPO and RTO requirement to design effective and cost-efficient disaster recovery solutions.

Key Point	Recovery Point Objective (RPO)	Recovery Time Objective (RTO)
Definition	Maximum acceptable amount of data loss measured in time.	Maximum acceptable amount of time to restore business operations after a disaster.
Importance	Determines frequency of data backups or replications.	Minimizes downtime.
	Ensures data loss is within acceptable limits during recovery.	Ensures business continuity.
Implementation	Frequent data backups.	Robust disaster recovery solutions.
	Continuous data replication.	Hot standby systems.
	Technologies like synchronous replication for near-zero RPO.	Automated failover mechanisms.
		Pre-configured recovery environments.
Complementary Metrics	Addresses data loss tolerance.	Addresses downtime tolerance.

Appendix 9 Collaborative Wiki (Unit 5-6)

  https://helenhelene.github.io/eportfolio/ISM/ISM_Unit05_Wiki.html   

Collaborative Wiki Development: The Future of ISM

The general title for the wiki page is “Which factor will most affect the future direction of Security and Risk Management?”

Each student should create a minimum of two entries:

1. one based on the question chosen in this unit from the Aven (2016) reading, and
2. one that answers the questions in the Seminar preparation Unit 6.

1. Read [Aven \(2016\)](#) and answer below selected issue.

How can we describe and represent the results of risk assessments in a way that is useful to decision-makers, which clearly presents the assumptions made and their justification with respect to the knowledge upon which the assessment is based?

Introduction

Describing and representing risk assessment results effectively is crucial for aiding decision-makers. To ensure the information is both useful and transparent, it is essential to clearly present the assumptions made during the assessment and justify these assumptions based on the underlying knowledge. Aven (2016) emphasizes the importance of transparency and clarity in risk assessments.

Main Discussion

To address this issue, several strategies can be employed:

1. **Clear Communication of Assumptions and Uncertainties:**

- **Explicit Assumptions:** Clearly state all the assumptions underlying the risk assessment. This includes specifying the scope, data sources, and any constraints faced during the analysis (Aven, 2016). For example, if certain risk scenarios are based on historical data, this should be explicitly mentioned.
- **Uncertainty Quantification:** Use both qualitative and quantitative measures to express uncertainties. Methods such as confidence intervals, probability distributions, and scenario analysis can help convey the degree of uncertainty in risk estimates (Aven, 2016). This can be represented visually using error bars or