Please find the module ePortfolio under
https://essex.sevale.de/modules/infosec-management/eportfolio/

The Information Security Management (ISM) module followed two other security-related modules on the course, introducing additional approaches to achieving organisation's information security. The module covered the various standards, certifications, and frameworks (like OCTAVE Allegro, HIPAA, ISO 27000 family, and attack trees among others) (Schneier, 1999; Caralli *et al.*, 2007; Kirvan, 2025), as well as touched upon the topic of digital transformation. The tasks were diverse and included analysing the applicability of security standards to an organisation, performing a risk assessment for an enterprise, and developing a Python application implementing an interactive attack tree model. Gibbs' model will be used to guide this reflection (Gibbs, 1988; McLeod, 2024).

By the end of the module, I gained practical experience in selecting and working with a risk assessment framework, evaluating criteria relevant for a business considering a digital transformation, organising and processing attack trees, including implementing and adapting algorithms for their quantitative analysis. Participating in the module confirmed my understanding of the holistic nature of information security and made me more familiar with the industry-standard methodologies for risk assessment.

Feelings

Initially, at the beginning of the module, I felt overwhelmed: it followed another intense six-week module, and I did not have a chance to recharge.

When beginning the assignment for the risk assessment, I was a bit lost, as there were multiple objectives to cover, and I had to delve into risk assessment, which was a new area for me. However, as I progressed with the task, reviewed the different risk assessment frameworks, and selected OCTAVE Allegro (Caralli *et al.*, 2007) for my assignment, I felt more confident, as the methodology organised the vast task of thorough evaluation of an enterprise into manageable chunks and provided step-by-step guidance. At the same time, I found working with the framework tedious, as it required filling out numerous spreadsheets with terribly similar data.

The coding assignment involved a more familiar taskset, so it allowed me to experiment more, and I enjoyed developing a full-stack application and implementing the recursive data structures and algorithms, which I always appreciate as a challenge.

Another part of the course that I enjoyed has inclusion of the physical aspect of information security, which added nicely to the knowledge gained from the previous modules that were mostly focused on the digital assets.

Evaluation

Working on the first assignment, I could choose a suitable framework for the task that guided my next steps. Developing an application for the second assignment went smoothly, and it was possible for me to explore technologies such as Flask (Pallets, no date) and experiment a little with frontend development as well. Both tasks broadened my perspective on the information security management and highlighted the different challenges that ISM analysts face.

At the same time, at times I felt frustrated with the workload and some requirements, such as a very restrictive word limit for the first assignment, which left me struggling to

incorporate all the objectives of the analysis in a single report. Working with OCTAVE Allegro and attack trees required repeating same steps multiple times for slightly different inputs.

Some of the materials in the module, as well as papers that I researched while working on the assignment appeared quite dry, which I did not expect from an applied discipline.

Analysis

As with any other methodology that guides a comprehensive analysis, OCTAVE Allegro and attack trees inherently require a lot of repetitive work, so this aspect was expected. However, I believe Allegro could optimise at least some of this repetitiveness by organising some of the worksheets in form of a spreadsheet.

The frameworks once again highlighted the importance of holistic approach in security, where both digital and physical aspects of a system must be considered in evaluation. I appreciated the inclusion of physical security in this module, as the previous modules primarily focused on digital assets.

Conclusion

While progressing through the module I learned that ISM must account and balance multiple distinct aspects such as physical, digital, and human factor. I gained practical experience in working with methodologies such as OCTAVE Allegro and attack trees and discovered other frameworks each applicable to enterprises of different size and nature.

Completing the risk assessment made be better understand how the threat landscape changes after a digital transformation, how challenging this aspect must be for enterprises, and what important role employee education plays in such scenarios.

Working on the application for attack tree rendering highlighted how different organisations may be more perceptive to alternative report formats, especially interactive formats that allow to better contextualise the findings.

Action Plan

The module provided me with new tools that I can apply in my future assignments and knowledge that I can apply when making security-related decisions in my current position. At the same time, the vast scope of the security-related standards, regulations, and certification still feels to be complicated, so it will require more research and effort from me to confidently navigate it.

Overall, this module has strengthened my appreciation for interdisciplinary nature of information security and improved my ability to apply structured frameworks in real-world enterprises.

References

Caralli, R.A. *et al.* (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process:* Fort Belvoir, VA: Defense Technical Information Center. Available at: https://doi.org/10.21236/ADA470450.

Gibbs, G. (1988) “Learning by doing: A guide to teaching and learning methods,” *Further Education Unit* [Preprint].

Kirvan, P. (2025) *Top 15 IT security frameworks and standards explained | TechTarget*, *Search Security*. Available at: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one (Accessed: October 19, 2025).

McLeod, S. (2024) “Gibbs Reflective Cycle,” 2 September. Available at: https://www.simplypsychology.org/gibbs-reflective-cycle.html (Accessed: September 7, 2025).

Pallets (no date) *Welcome to Flask — Flask Documentation (3.1.x)*. Available at: https://flask.palletsprojects.com/en/stable/ (Accessed: October 18, 2025).

Schneier, B. (1999) “Attack Trees,” *Schneier on Security*, December. Available at: https://www.schneier.com/academic/archives/1999/12/attack_trees.html (Accessed: October 15, 2025).