

## Security and risk management - Reflective

<https://ashanmugam81.github.io/My-E-Portfolio/>

---

Security and risk management (SRM) have been my focus for the past year. We learned how to protect against IT threats in this unit. This module improved our SRM for a really time project.

It was clear to me after completing this session how crucial it is for organisations to take precautions and establish safety protocols. In addition, I was well-versed in the many safeguards and countermeasures in place to prevent data loss, theft, misuse, tampering, or omission. Course materials have helped me better understand information security. Information security can only be attained when privacy, accessibility, and unaltered records are all present.

The talk about Industry 4.0 helped me become more knowledgeable about CVSS. Prior to this lesson, I was only aware of CVSS in its capacity as a security risk assessment. My knowledge of CVSS has grown thanks to the forum's discussions, and I've picked up some useful tips from my fellow forumgoers as well. In reading the contributions of my classmates, I realised that CVSS isn't the sole scoring technique and that there are additional considerations that render it an untrustworthy source.

The case study on GDPR was quite helpful. Using the case study, data controllers may reply to access requests and provide evidence that they are in compliance with legislation, highlighting the need of such measures. The significance of the data protection rules of GDPR is shown by further case studies.

One of the most intriguing and useful parts of the group task was the chance to talk to others in the class. As we do these assessments, please allow me to get input from the wide range of persons with whom I work. Discussions between a diverse group of people are always fruitful and provide the chance to learn about something new.

This Unit 6 project, which asks us to assess dangers posed by the company's move to digitalize its traditional business operations, is both fascinating and applicable to my line of work. Considerations that should be made before, during, and after the digitalization process, such as the need for a business continuity and disaster recovery plan, and an analysis of the potential security risks that the organisation can face in the supply-chain and in the digitalization of their business.

The building of this module required a number of distinct actions to be completed in order to complete the various tasks involved. Students were given Excel-based activities to complete independently as part of a Monte Carlo simulation assignment. We used the AHP module in the previous 11 projects, and it proved to be a great asset in illustrating the relative importance of various risks that the Executive should take into

account when developing the strategy for the global supply chain and the digitization process. It is my firm belief that I will be able to put into practise the risk modelling strategies we examined in this assignment.

This programme was highly instructive and intriguing, especially in regards to catastrophe recovery. Essentially, this is what I do for a living now. For my customers, I facilitate the process of moving their data from on-premises facilities to the public cloud. Throughout this unit, I've learned a great deal that will help me in the future. Now I know what questions to ask the client to help me find the best options for them. This unit showed me the value of having a solid disaster recovery and business continuity strategy in place. The business lost data going back to two months and required a lengthy time to recover from the ransomware assault because of a weak recovery point objective (RPO) and recovery time target (RTO). Having learned the value of tabletop exercises for BCP/DR in the event that a DR test cannot be conducted, I can see why they are essential.

After completing this session, I can reflect on the period when our organisation was affected by a ransomware assault and understand the significance of reviewing our policies on a regular basis to ensure we were in line with all applicable regulations. I was able to do this by thinking back on what happened at the time. After a client's system was compromised by a ransomware assault, I was offered the chance to assist in the restoration process. Learning the value of SRM to a business helped me see where I could make the most impact. This lesson has helped me appreciate the need of informing both people and institutions about security threats and the steps that may be taken to lessen such dangers. If we can get more people thinking about and talking about these problems, we can assist those who aren't aware of the risks to learn about them and create strategies to reduce them.

When I started the course, I knew little anything about the subject. After completing the training, though, I felt much more confident in my ability to assess threats to IT systems and implement appropriate countermeasures. My knowledge of the many types of hazards I may encounter and how to handle them throughout the organization's IT infrastructure has improved as a result of this. The methods I learned about in this lesson have made a huge difference in my day-to-day job. My training expertise has grown in both breadth and depth as a consequence of my ability to utilise what I've learned about the topic in my present position to facilitate more effective work efforts.