Within this module our main task was to provide a security risk assessment for a company that plans to implement an enterprise resource planning (ERP) system in three different ways.

We initially laid out a plan where we defined the various steps of our risk management process. We had discussions about the fact which approach to implement. We agreed that an approach based on ISO27001 would be a good idea, since the company also might use any certification in the future to gain competitive advantage. We also figured in discussions that the ISO27001 approach is a proven way for assessing IT security risks of companies, which did fit our assignment.

Another point of discussion was on how to identify risks. Whilst I suggested a structured approach (STRIDE) since I think that by using this you are likely to not forget elements, others suggested a scenario-based approach, which we then used for the security risk analysis.

While conducting the risk assessment we quickly figured out that some of the numbers for severity in case of a successful hack were guesswork, since we had little to no detail on the company and we did not know how much damage a compromised asset would create. While moving along we however figured that this lack of information was not an issue since we compared three solutions protecting the same assets.

While doing the risk assessment it also became quite apparent, that a quantitative assessment will always lead to a better result. It however also became quite apparent, that quantitative analysis does need more time to investigate and to collect reliable numbers. This plus the fact that the company was an example and did not have real data (e.g., damage in financial revenue by losing contracts) made us neglect the usage of quantitative only methods and we moved to semi-quantitative / qualitative assessment. Conducting the assessment, it came quite apparent, that a COTS version will be superior in terms of security risk, which was not a surprise.

Analyzing the requirements for Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for all three solutions discussed, made it very apparent, that only the COTS version can be operated economically. The result was also not surprising, but the numbers calculated nonetheless were a surprise, since COTS was so much better in comparison to the self-coded or open-source solution.

In my work life I must judge risk approaches from clients. We typically expect one approach to be used, since it is proven to be very useful in medical device development. With this assignment however I had to think about what options to use and why to take those options. This experience made me realize why some of our clients are having struggles creating their security risk assessments. Many seem to not realize the difference between quantitative and qualitative assessment. Some for example only use quantitative methods and create heavy weight assessments that take a lot of time and unfortunately sometimes even come to a wrong conclusion. Having truly learned the distinction between qualitative and quantitative assessment is the key take away from this module for me.