Final project evaluation vs design document

Our initial design was more network and vulnerability oriented, perhaps because we were biased from the network fundamentals and the penetration testing case study (Compromising a Medical Mannequin) that was the module's flow at that time. Threat modelling we first thought was STRIDE, and we tried to match our methodology to combine STRIDE properties with an OSI layer's bottom-up approach.

Having utilised many tools for mapping the provided server's network, combined with Kali Linux tools, the design document focused more on the vulnerabilities and the penetration testing part.

Compliance and security standards that were module's part at the latter units were also required to the final project. The project had to be more business-oriented and to combine all the previous evidence with GDPR and PCI compliance and risk assessment.

Our team agreed to create a table to match business risks with vulnerabilities found from the first assignment and present the report holistically. We perceived this method as the best way to approach the project (360-approach). The following parts were focused on GDPR and PCI compliance, and finally, we proposed technical mitigations and non-compliance points

In conclusion, I think the final result was comprehensive and complete, given the server's limitations (Little services and apps running) and the time we had to deliver.