1. Write a two page security policy for your example enterprise from the first exercise, aimed at senior managers and end users. Remember: short in length, long in duration. (5 marks)

2. Write a risk treatment plan (you can take it from the first exercise, taking account of feedback) covering what you see to be the top five risks. Summarise the risks, but do not do a full risk assessment: you do not have the facts to do this properly. (5 marks) Remember, you can transfer risks,

3. Write a residual risk statement, showing the things that you cannot treat. This is the key document for giving options to the business, so you could (for example) list the untreated risks, but then provide an appendix which gives options. Don't worry too much about concrete costs, but you should be able to use your wider knowledge and experience to give rough ideas of why the risks cannot be treated. (5 marks)

4. Make a short video, 5 minutes maximum, to be shown to the users in your enterprise as part of regular training. It should give both advice and justification: what to do, and why. Here's a very short, and very bad, example of the sort of thing: https://twitter.com/unibirmingham/status/1092734740208201728 (Links to an external site.) but you can use a presentation, slides, whatever (5 marks).