Guidance for completing ICA

It is actually quite difficult to give guidance on completing your ICA without actually doing it for you! But below you will see some pointers which I hope will steer you in the right direction. The wording from the ICA specification is in blue.

Overall note: we've been asked how to approach the overall assessment (e.g. should I critique the scenario?)… our advice is to look at the marking criteria in the ICA specification very carefully. Stick to the Assessment Requirements and use the language in the Learning Outcomes and Knowledge, Skills and Behaviours to analyse whether you are addressing the requirements to the level described.

You do not need to critique the scenario – consider the first line of the case study: "You have been recruited by a specialist agency to manage the development of a new national transportation department which uses artificial intelligence (AI) to manage personal and corporate vehicular travel across the country". Your approach should be – this needs to happen, how do I make that work in the context of this assessment?

Part 1

The word count is 1200, which means you will have to decide which risks you would like to focus on for this part – there are too many risks to feasibly write about them all! You need to decide which risks you are going to include and write about in detail but you could, for example, select a range based on their overall risk score, based on specific categories (i.e. different types) or focus on the most extreme risks. You must only include risks relating to data and any systems/hardware that handle data. That could include human centric risks too, as long as they relate to data.

Part 2

A summary of ethical, social, legal and regulatory compliance issues relating to this case study, to include clear information on all applicable laws and industry best practice (such as ISO27K). The summary should demonstrate an understanding of the differences between ethical and legal considerations. It should include a clear list of controls you plan to implement with justification for each. **[35 marks]**

- Guide: 2000 words
- To include a comprehensive list of all pertinent legislation and ethical and social issues with clear controls identified and justified
- To include clear links between issues identified, suggested controls and associated legislation/standards
- To include an indication of consequences to the organisation in the event of non-compliance

I think the best way to tackle this section is to relate what you are writing to your risk analysis –

1. Think about what you have put in your “mitigation” column (or whatever you called it).
2. Now think about what controls (see week 7 lecture) you could use to try and implement these mitigations, you may wish to discuss these in the light of ISO27k (see week 7 lecture) The controls might be:
    a. a policy (can you give an example?)
    b. procedures the company might want to follow (give an example)
    c. some training or ISA campaign (again can you describe this or give examples) (see week 5 lecture)
    d. You could apply another recognised framework rather than ISO27K, but you would need to explain why this is more appropriate to use.
    e. You will only have the word count to discuss *some* of the mitigation controls you have listed in your risk assessment, so think about what you are going to include – perhaps consider importance, urgency, variety etc.
3. As you discuss a particular control objective you might also want to discuss what legislation the control might be ensuring the company complies with. See Teesside University’s Acceptable Use Policy for some of the legislation that this policy covers as a guideline. I would concentrate on the Data Protection Act 2018 as this is absolutely vital (I will be covering this in week 11). You need to do more than just provide a list of legislation (especially don’t just copy the list on the Teesside policy!), by all means list the legislation you think *appropriate* but provide more detail on a few key pieces and clearly *explain* why they are particularly important in relation to the company.
4. Part of your legal discussion should also include what the consequences might be to the company if any legislation was breached or there was evidence of non-compliance (breaching the DPA is important here), you could briefly include consequences to an individual, but this is more likely to be covered by a disciplinary policy and I wouldn’t spend too much time on impact to individuals (if any). We will also be discussing the legal concept of ‘vicarious liability’ in the week 11 lecture which may have implications for the company.
5. Addressing ethics in your discussion – I don’t particularly want to see a sub-section called “Ethics” as ethical considerations shouldn’t really be an “add-on” at the end. E.g. if one of the controls you suggest allows the company to monitor all internet traffic and emails of employees (as the Teesside University policy does) is this actually ethical – might it breach someone’s Article 8 rights under the Human Rights Act (again see lecture week 11)? You should really discuss this in the context of the control you are discussing. If the only way you can address ethical issues is in a separate section at the end this this would be better than not doing it at all.

General advice for Part 2

- You do NOT have the word count to either write a fully functioning ISMS, nor are you expected to do so, or to address *all* the control objectives of ISO27K
- Aim for depth rather than breadth in your discussions but explain why you are concentrating on particular controls.
- I will be looking for clear evidence that you understand *why* the controls you suggest are important.
- Make sure that your discussion is focussed on the case study company, you won't get very many marks for a very general and non-specific description.
- Those students aiming for very high marks will also be using *appropriate* references, case studies and other evidence to underpin their discussion. I have been giving you links to journal papers and extension activities in lectures and practicals (there is a reason for this!) but I would expect you to also be doing your own research as well.

Part 3

Again, read this section very carefully because the crux of this work is to produce a ***generic*** process flow **using formal process flow notation** that can be used in the event of **any** IT related disaster – this is not meant to be easy and will test your logic and creativity. **Don't leave this until last!**

Part 4

A reflection on the portfolio you have produced: its strengths and weaknesses and your own learning based on your degree route. **[10 marks]**

- Guide: 600 words
- The reflection needs to be honest and identify areas for improvement within the portfolio, with justifications
- You can reflect on every aspect of the portfolio you have produced, including presentation, your recommendations, content, references, time management etc.
- It should link to your prior learning, and future career choice

General Guidance for Part 4

1. Please write this section using the first person i.e. "I" & "me", we really want to hear your voice coming through here.
2. Reflection is really in three stages:
   2.1. Identifying issues, perhaps in how you tackled this assignment (did you give yourself enough time? Did you do extra reading or just rely on what was covered in class? Did you ask if were not sure about something? Etc). You can only do this if you are honest with yourself. You only have 600 words so perhaps pick out 3 or 4 key issues.
   2.2. Faced with a similar situation in the future what could/would you do differently next time? A small action plan might be useful here addressing each of the issues in the first stage of your reflection.

2.3. Finally feed your actions forward – how will your actions help you in the future, what about your long-tern employment aspirations?

Part 5

The entire portfolio needs to be professionally presented. [10 marks]

- References should be included in appropriate places
- It should be free from major spelling/grammatical issues and in a publishable state
- It should include page numbers, a table of contents, sensible headings, list of references and appendices (if appropriate).
- The structure should be easy to follow and logical
- Any assumptions you make in addition to what is in the case study should be listed throughout

General Guidance for Part 5

- References should be in Harvard style (see p.8 of the module guide for more detail on this). You should be using the "Cite them Right" guide available in book form and online via the library (if on Campus just Google this)
- Don't forget that we showed you options to collate your references and also how Refworks & Mendeley both integrate with Word to make citing and creating your reference list so much easier (if you are using Google docs you might find it useful to look at Paperpile). There really is no excuse not to reference correctly and you will need to do this for your FYP, so think of it as practice.
- Apart from the reflection part of your portfolio you should be writing in the 3rd person (i.e. you don't use "I" or "myself"). If you are struggling with this then I would suggest using the resources on writing from Library: https://libguides.tees.ac.uk/academic_writing you can also book yourself a tutorial with them to help you with your academic writing. Again this is the way you will be expected to write your final project.
- Structure - please separate your portfolio into 4 distinct parts, each clearly labelled. These should be altogether in one document though, *please* don't submit 4 separate docs.
- Give yourself time at the end to edit and re-read your work, if there are a lot errors (spelling, grammar, presentational etc) in it you will lose marks
- Try and stick to the word counts given - if you run over by more than 10% you will lose marks as we won't read it.
- Be careful about who you are writing your portfolio for, you can either think of it as myself and Vicky or the case study company. I don't mind which, either way you don't need to explain simple concepts (I really, *really* don't want to read yet another

explanation of what the internet is, seriously I get it at least once a year!). You can also assume that your audience has reasonable idea of what cybersecurity is.