# Cardiff School of Computer Science and Informatics

## Coursework Assessment Pro-forma

**Module Code**: CMT308

**Module Title**: Business Continuity and Transformation

**Lecturer**: [Dr Yulia Cherdantseva](https://www.cardiff.ac.uk/people/view/118119-cherdantseva-yulia)

**Assessment Title**: Assessment 1 - Individual Coursework

**Assessment Number**: 1 of 3

**Date Set**: Autumn, Week 3

**Submission Date and Time**: Autumn, Week 10 (by 6th December 2022at 9:30am)

**Feedback return date**: within 4 working weeks after the submission deadline (by 20th January 2023)

**Extenuating Circumstances submission deadline will be 1 week after the submission date above**

**Extenuating Circumstances feedback return will be 1 week after the feedback return date above**

This assignment is worth **50%** of the total marks available for this module. If coursework is submitted late (and where there are no extenuating circumstances):

1 If the assessment is submitted no later than 24 hours after the deadline, the mark for the assessment will be capped at the minimum pass mark;

2 If the assessment is submitted more than 24 hours after the deadline, a mark of 0 will be given for the assessment.

Extensions to the coursework submission date can ***only*** be requested using the [Extenuating Circumstances procedure](https://intranet.cardiff.ac.uk/students/study/exams-and-assessment/extenuating-circumstances). Only students with approved extenuating circumstances may use the extenuating circumstances submission deadline. Any coursework submitted after the initial submission deadline without \*approved\* extenuating circumstances will be treated as late.

More information on the extenuating circumstances procedure can be found on the Intranet: <https://intranet.cardiff.ac.uk/students/study/exams-and-assessment/extenuating-circumstances>

By submitting this assignment you are accepting the terms of the following declaration:

**I hereby declare that my submission (or my contribution to it in the case of group submissions) is all my own work, that it has not previously been submitted for assessment and that I have not knowingly allowed it to be copied by another student. I understand that deceiving or attempting to deceive examiners by passing off the work of another writer, as one’s own is plagiarism. I also understand that plagiarising another’s work or knowingly allowing another student to plagiarise from my work is against the University regulations and that doing so will result in loss of marks and possible disciplinary proceedings***[[1]](#footnote-2).*

## Assignment

In this coursework, you should develop a coherent case study and complete the tasks listed below in the context of the chosen company.

**Part 1 - Case Study Description**

* 1. Identify and describe a company for this case study (further in the document it is referred to as “the company”). *Note: This section is not included in the word count.*
* You can use the Translate case study which we study in the class as an example. The company that you choose to consider may be either a real company or you may prefer to construct an artificial company based on other case studies.
* The size of the company, the sector and the nature of business are at your discretion to choose.
* You should include in the description all the details about the company relevant to the following tasks to enable you to develop a coherent and logical case study.
* Describe in detail **one** specific cyber security incident that the company has experienced recently or may experience in future and analyse its impact on the business (you can use the details from other known cyber security incidents to complete the description).
	1. Analyse the legal cyber security landscape the company operates in, the effect it has on business operation (sector-specific discussion)

**Part 2 - Modelling**

1. Model **one** core business process of the company using BPMN or another process modelling language (if different from BPMN, then explain the choice of the modelling language/tool). All remaining tasks in this assessment should closely align with the business process that you are considering in this section. The process should be modelled in a sufficiently detailed manner. Provide a short narrative of the process *(Note: do not duplicate information that is clear from the process model, only include details that could not be inferred from the model)* and explain why this process is important for the continuous operation of the business under cyberattacks and other external disruptive events.
2. As a Business Continuity analyst, identify **two** key vulnerabilities in the business processes that could have an impact from the following perspectives:
* Legal and Regulatory,
* Productivity,
* Financial stability,
* Reputation and
* Loss of Customer Confidence.

Analyse how the cyber security resilience of these core processes could be improved with regards to the discussed vulnerabilities and related threats. Propose and discuss **two** mitigation measures that could be used in this process to reduce the impact of the cyber security threats. Justify your decisions and provide references to appropriate trustworthy sources.

1. Create one Dependency Model (DM) for the process described in Section 2.1. The DM should be sufficiently detailed, however, there is no aim to achieve completeness. Attempt to address technical & non-technical, internal & external dependencies.
2. Model **one** playbook to respond to the cyber incident you have described in task 1.1. You could use BPMN, another process modelling language or a playbook modelling standard. Justify the choice of modelling techniques and adhere to the modelling rules of the chosen technique.

The case study should be coherent and consistent across different tasks, all its elements should be closely aligned and interconnected. For examples, the DM should include the dependencies of the considered business process; the vulnerabilities and threats discussed should be relevant in the context of your company; and the analysis of the legal landscape and relevant guidelines should consider documents relevant to the sector and the size of the chosen company.

Your individual report must have an overall word count of no more than 2000 words**.** The description of your case study (section 1.1) should be provided in an appendix and will not be included in the word count.

### Writing Style, Report Presentation and Citations

The report should be professionally presented and adhere to the expectations for an academic report. It should have a clear structure, be concise and make your points clear.

This tutorial provides guidance on how to write critically and structure an essay: <https://xerte.cardiff.ac.uk/play_10353>

You should use an academic writing style and appropriate vocabulary. These tutorials provide guidance on Vocabulary, Grammar and Academic Writing Style: <https://intranet.cardiff.ac.uk/students/study/study-skills/english-language-support/online-modules>

You should appropriately cite and acknowledge the work of others. You must use a broad range of trustworthy peer-reviewed resources. The references must be provided at the end of the document and should be appropriately mentioned in the text. Microsoft Word provides an in-built tool for maintain references in a document[[2]](#footnote-3).

Citations should be provided using a consistent style. For this assessment you can choose one of these citation styles: **Cardiff Harvard or IEEE**.

You can find referencing guidance on these citations styles here: <https://intranet.cardiff.ac.uk/students/study/study-skills/academic-writing-communication-and-referencing/citing-and-referencing-support>

## Learning Outcomes Assessed

1. Critically analyse the potential impact of cyber threats on business continuity.

3. Evaluate threats to Small and Medium-Sized (SME) vs. large enterprises.

## Criteria for assessment

Credit will be awarded against the following criteria.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mark Range**  | **Knowledge & Understanding****30%**  | **Evidence & Analysis****30%**  | **Modelling Skills** **40%** | **Presentation** **of Report****10%** |
| 85 – 100%  | Outstanding subject knowledge. Excellent understanding of different recent debates and key issues in topic area under investigation which are relevant to the chosen context.  | Demonstrates an ability to construct a very well justified argument or position on the basis of appropriate evidence when developing a case study. Demonstrates an ability to evaluate a wide range of relevant material in order to produce a valid case study. Effective contextualisation of cyber security threats and analysis. | Evidence of the ability to choose and make effective use of modelling techniques for 1) process modelling; 2) dependency modelling and 3) playbook modelling. The modelling technique rules are followed precisely and any deviations are explained and justified. Demonstrates an ability to research for information to underpin the design of models independently and to approach design critically. Effectively adjust the models to a specific context. Critical analysis of the drawback of existing modelling tools. | Clear and articulate writing style with no spelling or grammatical errors. Complies with presentation criteria. Accurate referencing within the text and clear acknowledgement of sources used. Accurate and complete bibliography.  |
| 70 – 84%  | Wide knowledge of subject and ability to apply theory in a critical and thoughtful way. A thorough understanding of different debates and key issues in topic area under investigation.  | Strong evidence of the ability to make a sustained argument or position based on appropriate evidence. When developing a case study. Shows an ability to evaluate the evidence and synthesise material to form a coherent discussion. Effective contextualisation of cyber security threats and analysis. | Evidence of the effective use of appropriate modelling techniques. Uses evidence from independent research to support modelling decisions and arguments. Strong evidence of independent research and some critical reasoning when designing models 1), 2) and 3).  | Clear and engaging writing style that demonstrates very good command of English. Complies with presentation criteria, accurate referencing within the text and clear acknowledgement of source used.  |
| 60 – 69%  | Very good subject knowledge and understanding of cyber security key threats and debates in cyber security. Evidence of a good understanding of relevant theoretical material.  | Evidence of the ability to make a sustained and coherent argument using appropriate evidence when developing a case study. Evidence of ability to evaluate the evidence and synthesise generalisations, and vice versa the ability to apply generic conclusions to a specific case study.  | Evidence of appropriate reading about modelling techniques and ability to use modelling tools effectively to support 1),2), 3). Evidence of independent research on modelling techniques and the context of a chosen organisation.  | Clear writing style that demonstrates a good command of English. Few imprecise statements. Adheres closely to presentation criteria. Referencing mostly clear and accurate.  |
| 50 – 59%  | Sound subject knowledge and understanding of key issues and debates in topic area under investigation. Evidence of understanding some of the relevant theoretical material relevant to the assessment task.  | Evidence of the ability to construct an argument using appropriate evidence. Evidence of an ability to collate information and reach some general conclusions. Evidence of a satisfactory level of analysis of theoretical issues  | Evidence of ability to select appropriate modelling tool for some of the suggested tasks and accompany models by a coherent argument. Satisfactory use of modelling techniques, the core rules are followed, but there are minor deviations from the standards. The models [provided are aligned with and supported by the written argument. Some evidence of independent research on modelling tools, techniques, and business context.  | Correct English usage with few imprecise statements. Adheres to most aspects of presentation criteria and clear attempts made to acknowledge sources accurately within the text.  |
| 40 – 49%  | Evidence of some understanding of appropriate theory, but lacking depth. Limited understanding of key issues and debates in topics under investigation.  | Some evidence of analysis of relevant material but with limited argument and evidence. Evidence of the ability to construct a coherent response to the assessment task, but only a basic level of interpretation and evaluation  | Models are presented, but do not follow modelling rules, are not accurately presented or do not align with the business context. Processes/examples selected are narrow and not critical to business. Limited evidence of independent research.  | Correct English usage, but with some lack of precision. Some aspects of the work are not explained clearly and marks limited by the material that the marker can understand. Presentation criteria may not be wholly adhered to. Referencing and bibliography attempted but may lack accuracy.  |
| 30 – 39%  | Evidence of some knowledge of topic under investigation, but with serious omissions. Little understanding of key issues and debates. Evidence of reproduction of material from lectures and introductory material, with no interpretation or deeper understanding.  | Evidence of basic interpretation of the question or assessment task, but answer may address only part of the topic. Evidence of a general, but rudimentary grasp of the question with only limited ability to sustain a response.  | Models are presented, but do not follow modelling rules, are not accurately presented or do not align with the business context. No evidence of research beyond directed reading or lecture notes. Over-reliance on limited range of sources, without analysis or interpretation when designing models.  | Some incorrect use of English and argument is unclear. Some coherency in notes appropriate to question, but further development of prose required. Fails to reference and fails to adhere to required presentation format.  |
| 20 – 29%  | Evidence of some knowledge and reading, but the ideas are largely marginal to the question or the assessment task set. Inadequate understanding of topic under investigation with significant errors or omissions.  | An unbalanced response that omits essential material. Some evidence that assessment task has been understood, but very little development of ideas. Conclusions are not based on evidence presented.  | No models presented, or they are basic, limited and incorrect. Superficial reading of a limited or inappropriate range of sources used for contextualisation. Failure to engage with material in support of modelling.  | Significantly flawed use of English. The answer rambles and has little coherence or structure.  |
| 1 – 19%  | The work contains significant errors and indicates little familiarity with the concepts and language expected of an answer to the topic under investigation.  | Answer of little relevance to the question. Interpretation of the question is seriously flawed with no attempt to construct and argument  | No evidence of modelling skills | Incorrect use of English to such an extent that assignment cannot be understood.  |
| 0  | Cheating (including plagiarism, collusion, duplication and falsification). Submitting other people’s work as your own. Failing to present work.  |

## Feedback and suggestion for future learning

Feedback on your coursework will address the above criteria. Feedback and marks will be returned within 4 working weeks from the submission deadline in line with Cardiff University regulations. Feedback will be returned as follows:

* Individual feedback - in writing via Learning Central – Grade Centre.
* Cohort feedback - summary feedback for the cohort will be provided in writing via Learning Central – Announcements.

Feedback from this assignment will be useful for the Dissertation project*.*

## Submission Instructions

|  |  |  |
| --- | --- | --- |
| Description | Type | Name |
|  | **Compulsory** | One PDF document (.pdf)  | StudentNumber\_Assessment1.pdf |
|  | **Compulsory** | In model/tool specific formats | BPMN, DM models and playbooks included in the report must be provided in the original format produced by the tools used. |

Any code/models submitted will be run on University provided Windows laptop and must be submitted as stipulated in the instructions above.

Any deviation from the submission instructions above (including the number and types of files submitted) may result in a mark of zero for the assessment.

Staff reserve the right to invite students to a meeting to discuss coursework submissions

## Support for assessment

Questions about the assessment could be sent via MS Team channel set for the module, over email to the module lead and in class after the release of the assessment proforma. After the release of the assessment a dedicated session will be organised to discuss the assessment to answer all questions.

1. https://intranet.cardiff.ac.uk/students/study/exams-and-assessment/academic-integrity/cheating-and-academic-misconduct [↑](#footnote-ref-2)
2. <https://support.microsoft.com/en-us/office/create-a-bibliography-citations-and-references-17686589-4824-4940-9c69-342c289fa2a5> [↑](#footnote-ref-3)