Assignment Brief and Front Sheet PG

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate ‘your’ section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

**To be completed by the student(s) prior to final submission:**

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

|  |  |
| --- | --- |
| **Student ID or IDs for group work** | **e.g. 1234567** |

**To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:**

|  |  |
| --- | --- |
| **Date set** | October 2024 |
| **Submission date (excluding extensions)** | Monday 07th April 2024 by 12:00pm (UK Time) |
| **Submission guidance** | To be submitted electronically via Tabula. |
| **Marks return date (excluding extensions)** | Latest date that marks can be returned to the students (i.e. the 20 day turnaround) |
| **Late submission policy** | If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). “Late” means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.  For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5. |
| **Resit policy** | If you fail this module and/or component, the University allows students to remedy failure (within certain limits). Decisions to authorise resits are made by Exam Boards. These will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.  If this is **already a resit** attempt, this means you will not be eligible for an additional attempt. The University allows as standard a maximum of two attempts on any assessment (i.e. only one resit). Students can only have a third attempt under exceptional circumstances via a Mitigating Circumstances Panel decision. |

**To be completed by the module owner/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:**

|  |  |
| --- | --- |
| **Module title & code** | WM9P1-15 Cyber Security Research Methods (CSRM) - **Coursework 1,** |
| **Module leader** | Dr Elzbieta Titis |
| **Module tutor** | Dr Elzbieta Titis |
| **Assessment type** | Report on undertaking a research project |
| **Weighting of mark** | 80% |

|  |
| --- |
| **Assignment brief** |
| At the end of this document. |

|  |  |
| --- | --- |
| **Word count** | The word count is 3200 words.  +10% will be allowed on this word count without penalty. If you exceed this word count by more than 10% to 30%, a penalty of 10% on the original mark awarded will be applied. If you exceed this word count by more than 30%, the final mark will be capped at the pass mark.  The word count does not include tables, however, you must use tables carefully. Improper use of tables, e.g. as an opportunity to consume more words will be penalised.    The word count does not include references, or appendices. Although appendices are allowed, these will not be marked and only referred to add context, please do not place into the appendices anything which you materially rely upon in your submission. |
| **Module learning outcomes (numbered)** | 1. Develop a research proposal within the field of cyber security, aligning the problem, research objectives, research questions, and research design. 2. Critically investigate and analyse sources of information appropriate to a given research problem. 3. Identify and evaluate specific issues and challenges for doing research in the cyber security domain and propose suitable mitigations/controls to conduct research safely and effectively. 4. Report findings with clarity and an appropriate degree of confidence, referring to both wider scholarship and own proposed investigations. 5. Critically understand key aspects of research methods and ethics in cyber security for generating impactful knowledge, validating theories, adding critical rigour, and promoting moral and social values. |
| **Learning outcomes assessed in this assessment (numbered)** | LO1, LO2, LO3, LO4 |

**Marking guidelines**

|  |  |
| --- | --- |
| **Criteria** | **Total marks available** |
| 1. Understanding of the central concerns of the task, including comprehension, focus and relevance. | 10% |
| 1. Analysis of the task, including the use of techniques and concepts in relation to the adopted approach.   Broken down as follows:   * Propose a research question and associated objectives for the research. * Develop a referenced literature review. * Develop and justify appropriate research method(s) to suit the requirements of your specific research question. * Anticipate and address ethical and safety constraints in the conduct of research. * Manage project risks by applying suitable mitigations. | 50%  10%  10%  10%  10%  10% |
| 1. Evaluation with respect to the task, including critical evaluation of the corpus of the research, and reliability and validity in planning the research. | 30% |
| 1. Presentation and style, including visual presentation, clarity and cohesiveness, and referencing. | 10% |
| Total | 100% |

Analysis is “the study of structure, content of something, or data in order to interpret them… used to further explain a subject matter.” The purpose is to “explain the nature and meaning of something”.

Evaluation is “a judgement of the quality of something… [that] can be conducted to test one’s skills.” “The main objective of the evaluation is concluding the existing level, quality, or standards of something. The results can be used for further development or in decision making.”

Evaluation is therefore supported by analysis.

Visual presentation includes the use of headings, bullet points, diagrams, and other formatting tools to enhance readability.

Clarity and cohesiveness include clarity of the writing and logical flow; use of clear language, logical organization of content, and effective use of transitions to guide the reader.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria** | **91-100** | **81-90** | **71-80** | **61-70** | **51-60** | **41-50** | **31-40** | **0-30** |
| **Criteria 1**  **Comprehension.**  **Focus.**  **Relevance.** | Sophisticated understanding of the central concerns of the task provided. A full and relevant exploration with sustained consideration of the implications of the questions. Extensive use of evidence to support an argument which is clearly focused on the demands of the question. | Comprehensive understanding of the central concerns of the task provided.  A relevant exploration which demonstrates secure consideration of the implications of the question.  Extensive use of evidence which clearly supports the demands of the question. | Sound understanding of the central concerns of the task provided.  A relevant and thoughtful approach to the question.  Use of evidence which is relevant to the demands of the question. | Broad understanding of the central concerns of the task provided.  A relevant approach to the question.  Use of evidence to address the demands of the question. | Adequate understanding of the central concerns of the task provided.  Mostly relevant approach to the question.  Some use of evidence to address the demands of the question. | Little understanding of the central concerns of the task provided.  A limited approach to the question.  Limited evidence to support demands of the question. | Very little understanding of the central concerns of the task provided.  Very little attempt to answer the question.  Very little evidence to support demands of the question. | Lack of understanding of the central concerns of the task provided.  No attempt to answer the question.  No evidence to support demands of the question. |
| **Criteria 2**  **Propose question/objectives.**  **Scoping lit rev.**  **Propose suitable methods.**  **Anticipate risks.**  **Propose mitigations.** | Relevant analysis of a task -appropriate range of techniques and concepts skilfully strengthening the approach adopted. | Relevant analysis of a task -appropriate range of techniques and concepts strengthening the approach adopted. | Relevant analysis of a task - range of appropriate techniques and concepts strengthening the approach adopted. | Relevant analysis of a task - range of techniques and concepts largely supporting the approach adopted. | Adequate analysis of a task - range of techniques and concepts supporting the approach adopted. | Little analysis of a task - some techniques and/or concepts. | Very little analysis of a task - limited techniques and/or concepts. | Lack of analysis of a task - no techniques and/or concepts. |
| **Criteria 3**  **Critical evaluation of the corpus of the research.**  **Reliability and validity in planning the research.** | A committed, clear, evaluative stance with respect to the task that is skilfully based on precise evidence discussed within the response. | A clearly identifiable evaluative stance with respect to the task that is securely based on evidence discussed within the response. | A discernible and relevant evaluative stance with respect to the task based on evidence discussed within the response. | Relevant evaluative stance with respect to the task based on evidence discussed within the response. | Adequate evaluative stance with respect to the task based on evidence discussed within the response. | Little evaluation with respect to the task provided and/or lack of relevance to the question and/or evidence. | Very little evidence of evaluation and/or supporting evidence. | Lack of evidence of evaluation and/or supporting evidence. |
| **Criteria 4**  **Visual presentation.**  **Clarity and cohesiveness.**  **References.** | Exceptional presentation and style requiring no amendments. | Excellent presentation and style requiring no amendments | Very good presentation and style requiring very little minor amendments. | Good presentation and style requiring mostly minor amendments. | Adequate presentation and style requiring amendments. | Inadequate presentation and style requiring major amendments. | Poor presentation and style requiring many major amendments. | Very poor presentation and style requiring many major amendments. |

|  |  |
| --- | --- |
| **Academic guidance resources** | You will have an opportunity to ask questions and get support on the assessment after it has been handed to you. You will be supported in this assessment through:   1. Specialist assessment support session. 2. One to one session during scheduled class time (please arrange meeting with the module leader). 3. Dedicated Moodle forum.   **Notes to students:**  If support is provided on a Teams Channel or a Moodle forum, please ensure you check previous questions posted on the channel. The Teams/Moodle channel will typically be closed one week before the submission date and no new questions will be addressed, please organise your time accordingly. Please be patient with module tutors. Please turn on your Teams Channel/Moodle notifications. If a tutor has not responded to a query within 5 working days, please email the module leader. |
| **Where to get help:**   1. Talk to your module tutor if you don’t understand the question or are unsure as to exactly what is required. 2. There are also numerous online courses provided by the University library to help in academic referencing, writing, avoiding plagiarism and a number of other useful resources. <https://warwick.ac.uk/services/library/students/your-library-online/> 3. If you have a problem with your wellbeing, it is important that you contact your personal tutor or wellbeing support services <https://warwick.ac.uk/services/wss> | |

# Assessment Detail

**Overall Context**

The Department for Information and Cyber Security (DICS) has recently advertised a lucrative early researcher post. The post sits within a team of governmental researchers who will conduct high quality research into cyber security issues – ultimately influencing government policy.

You have had a successful interview and have been shortlisted as one of ten candidates for the final round. The final step requires you to produce a research proposal. The final selection decision will be made purely on the basis of the research proposal.

You may select one of the following areas of research:

* The investigation of IoMT (Internet of medical things) devices.
* Influencing good cyber behaviour in UK SMEs.
* Developing effective inter-state cyber security policy issues.
* The investigation of the characteristics of people prone to cyber security failure, the types of scenarios they fail in and the factors that influence this failure.
* AI-based threats identification in financial institutions using machine learning approach.
* Protecting SMEs against third party cyber-attacks.
* Protecting SMEs against supply chain cyber-attacks.
* Impact of Big Data Analytics and ChatGPT on cyber security.
* Vulnerability of cyber security in cloud computing environment.
* AI enabled cyber security defence for smart cities.
* Applying blockchain and AI for securing AVs.
* Raising cyber security awareness to reduce SEAs through social media.
* Enhancing cyber security awareness towards phishing using gamification.
* Incorporating VPNs for cyber security to facilitate remote working.
* Implementation and detection of keyloggers in a system for defending against cyber threats.

Your task begins by performing a literature review into your selected domain.

In your analysis, you will address the following criteria:

1. Propose a fundamental research question and the associated objectives for the work documented.
2. Formulate relevant ideas into a referenced literature review.
3. Select appropriate research method(s) to suit the requirements of your specific research question, including justification.
4. Anticipate and address ethical and safety constraints in the conduct of research.
5. Manage project risks by applying suitable mitigations.

You will also need to evaluate the confidence that should be placed in any findings, for example, critically evaluate the corpus of research; address issues of reliability vs validity in research, including internal and external validity, etc.

It is therefore appropriate to discuss reliability and validity in various sections of your analysis. Showing that you have taken them into account in planning your research so that anticipated results make your work more credible and trustworthy. For example, in your literature review section, consider what have other researchers done to devise and improve methods that are reliable and valid? In your method section, explain how did you plan your research to ensure reliability and validity of the measures used? This includes the chosen sample set and size, sample preparation, external conditions, and measuring techniques.

You will present your findings with clarity and cohesiveness, providing clear and cohesive narrative, facilitating easy comprehension through skilful use of range of formatting tools, and demonstrating proficiency with regards to referencing.

# Special instructions

Do not include the Assignment Guidance and Front Sheet in the submission.

**Spelling/grammar.** Ensure that you spell check the submission, use a grammar checker and ensure that you proofread your work prior to submission. Spell/grammar checkers must be set to UK English, do not use ‘Americanised’ spellings.

**References.** References are to be included at the end of the report using the Harvard referencing system. You may also include a bibliography. Each reference must be connected to a citation within the main body of the report.

Do not attempt to hide text within JPEGs, this will be construed as an attempt to mislead the assessor.

**Coherence**. A poorly worded report will hide excellent content. The narrative should be easy to read, and arguments should be presented coherently and convincingly.

**Formatting**. All figures and tables must be properly labelled and captioned. All pages must be numbered. Formatting must be consistently applied throughout the submission. Submissions that stray from this guidance may be penalised.