Softwarica COLLEGE OF IT & E-COMMERCE | in collaboration with Coventry University

Student Assignment Brief

CONFIDENTIAL DOCUMENT
This document is intended solely for Softwarica College of IT & E-Commerce students for their own use in completing their assessed work for this module. It must not be passed to third parties or posted on any website.

Contents

Assignment Information

Module Name:	Cyber Security Project
Module Code:	ST6047CEM
Assignment Title:	CW2 – Final Report
Assignment Due:	31 July 2025 [12:00 PM]

Assignment Credit:	5 credits
Word Count:	12000 (+/- 10%)
Assignment Type:	Individual
Grading:	Percentage Grade (Applied Core Assessment)

Assessment Overview

You will be provided with an overall grade between 0% and 100%. You have one opportunity to pass the assignment at or above 40%.

Important Notice

The work you submit for this assignment must be your **own independent work**. More information is available in the 'Assignment Task' section of this assignment brief.

Assessed Module Learning Outcomes

2. Conduct a substantial piece of primary research work (including, but not limited to, an application development, a model or simulation, a business case, or observational or interactional method) to address the initial research question.
3. Conduct such secondary research as to establish the context, need, scope and audience for the project.
4. Reflect and account for the management of the project, showing consideration for the social, legal, professional and ethical dimensions of the work undertaken.
5. Present findings of the research in the form of a project report, utilizing appropriate academic methods of reporting and citation.

Assignment Task

Individual Coursework (100)

In this assignment, you will be required to submit your cyber security project. The project should include the following sections:

Title Page

- Title of the project displaying relevant technology and author's name including CUID.

Conceptual Diagram

- A visual representation of the project's architecture and components

Acknowledgment

- A section to acknowledge the people or organizations who supported the project.

Abstract

- A summary of the research objectives, methodology, and findings (not more than half a page)

Keywords

- List of relevant keywords that describe the topic of the project.

Table of Contents

- Provide a list of the different sections in your project.

List of Figures and Tables

- If any figures, tables, or diagrams are included in the project, list them here.

Introduction

- Background and Context: Provide an overview of the problem area and the context in which it exists.
- Problem Statement: Define the problem and the research question(s) that the project seeks to answer.
- Aim and Objectives: Provide a clear and concise statement of the purpose of the project and the specific goals to be achieved.
- Justification: Explain the significance of the research and how it will contribute to the field of cyber security.

Scope

- Define the boundaries of the project, including any limitations or exclusions.

Research Methodology

- Provide an overview of the research methodology and approach.

Literature Review

- Cyber Security: Provide an overview of the current state of cyber security, including key concepts and frameworks.
- Existing Research: Provide a summary of existing research in the field of cyber security, including at least five case studies or examples of successful cyber security projects.
- Gaps and Areas for Further Research: Identify any gaps or areas for further research in the field of cyber security.

Methodology

- Research Design: Explain the research design, including the research approach, data collection methods, and data analysis techniques.
- Proposed Solution: Describe the proposed solution, including software, hardware, and other tools.
- Project Management: Explain how the project will be managed, including timelines, milestones, and deliverables.
- Risk Management: Identify potential risks to the project and describe how they will be mitigated.
- Ethical Considerations: Identify any ethical considerations related to the project, such as data privacy, security, and confidentiality.
- Legal and Regulatory Issues: Outline any potential legal or regulatory issues that may arise.
- Compliance: Describe how the project will comply with relevant regulations, standards, and best practices, such as ISO 27001, HIPAA, GDPR, or others. Explain how

Task and Mark distribution:

Individual Coursework (100)

In this assignment, you will be required to submit your cyber security project. The project should include the following sections:

Title Page

- Title of the project displaying relevant technology and author's name including CUID.

Conceptual Diagram

- A visual representation of the project's architecture and components

Acknowledgment

- A section to acknowledge the people or organizations who supported the project.

Abstract

- A summary of the research objectives, methodology, and findings (not more than half a page)

Keywords

- List of relevant keywords that describe the topic of the project.

Table of Contents

- Provide a list of the different sections in your project.

List of Figures and Tables

- If any figures, tables, or diagrams are included in the project, list them here.

Introduction

- Background and Context: Provide an overview of the problem area and the context in which it exists.
- Problem Statement: Define the problem and the research question(s) that the project seeks to answer.
- Aim and Objectives: Provide a clear and concise statement of the purpose of the project and the specific goals to be achieved.
- Justification: Explain the significance of the research and how it will contribute to the field of cyber security.

Scope

- Define the boundaries of the project, including any limitations or exclusions.

Research Methodology

- Provide an overview of the research methodology and approach.

Literature Review

- Cyber Security: Provide an overview of the current state of cyber security, including key concepts and frameworks.
- Existing Research: Provide a summary of existing research in the field of cyber security, including at least five case studies or examples of successful cyber security projects.
- Gaps and Areas for Further Research: Identify any gaps or areas for further research in the field of cyber security.

Methodology

- Research Design: Explain the research design, including the research approach, data collection methods, and data analysis techniques.
- Proposed Solution: Describe the proposed solution, including software, hardware, and other tools.
- Project Management: Explain how the project will be managed, including timelines, milestones, and deliverables.
- Risk Management: Identify potential risks to the project and describe how they will be mitigated.
- Ethical Considerations: Identify any ethical considerations related to the project, such as data privacy, security, and confidentiality.
- Legal and Regulatory Issues: Outline any potential legal or regulatory issues that may arise.
- Compliance: Describe how the project will comply with relevant regulations, standards, and best practices, such as ISO 27001, HIPAA, GDPR, or others. Explain how compliance will be ensured throughout the project, including regular assessments, audits, and compliance checks.

Results/ Findings

- Data Collection and Analysis: Describe the data collection and analysis process, including any challenges faced and how they were addressed.
- Findings: Present the findings of the research, including any statistical analyses or data visualizations.

Future Recommendation:

- Evaluate the effectiveness of the solution and identify any additional areas for improvement or refinement.
- Consider integrating the solution with existing cybersecurity tools and systems to enhance their capabilities and effectiveness.

Discussion and Conclusions

- Interpretation of Findings: Provide an interpretation of the findings considering the research questions and objectives.
- Implications for Cyber Security: Discuss the implications of the research for cyber security, including how the proposed solution addresses existing gaps in the field.
- Contributions to the Field: Discuss the contributions of the research to the field of cyber security and any implications for future research.
- Limitations: Discuss any limitations of the research, including any limitations in the proposed solution or methodology.
- Conclusion: Summarize the project and reiterate the importance of the research.

References

- List at least 50 references, including academic journals, books, and other sources.

Appendix

- Technical specifications: Include technical specifications of the hardware and software used in the study.
- Code snippets: Include relevant code snippets that demonstrate the implementation of the proposed solution.
- SWOT analysis: Include a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis that outlines the internal and external factors that may impact the success of the project.
- Glossary: Include a glossary of technical terms used in the project. This can help readers to better understand technical concepts and terminology used in the research.
- Other relevant information: Include any other relevant information that supports the project, such as charts, graphs, diagrams, or other visual aids that help to illustrate key concepts or findings.

Additional Requirements:

- Clear timeline for the project, including milestones and deadlines.
- Definition of roles and responsibilities involved in the project.
- Clear budget and cost estimate for the project.
- Description of how the success of the project will be evaluated and impact measured.

Submission Instructions

Requirement	Details
File Naming	NAME_studentID
File Format	.docx/.pdf format
Submission Method	Campus 4.0 platform (submission link provided 2 weeks before deadline)

Marking and Feedback

How will my assignment be marked?

Your assignment will be marked by the Module Team using standardized criteria.

How will I receive grades and feedback?

Provisional marks will be released once internally moderated. Feedback will be provided alongside grades release within 2 weeks (10 working days).

What will I be marked against?

Details of the marking criteria for this task can be found in the Assessment Marking Criteria section at the end of this brief.

Grade Requirements

You must achieve 40% or above to pass this assessment. Ensure you understand the marking criteria for successful completion.

Assignment Support and Academic Integrity

Getting Help

If you have any questions about this assignment, please meet your respective module leader or teacher for more information.

Language Standards

You are expected to use effective, accurate, and appropriate language within this assessment task.

Academic Integrity

The work you submit must be your own. All sources of information need to be acknowledged and attributed; therefore, you must provide references for all sources of information and acknowledge any tools used in the production of your work, **excluding Artificial Intelligence (AI)**.

We use detection software and make routine checks for evidence of academic misconduct. Definitions of academic misconduct, including plagiarism, self-plagiarism, and collusion can be found in Student handbook in Campus 4.0.

All cases of suspected academic misconduct are referred to for investigation, the outcomes of which can have profound consequences to your studies.

Support for Students with Disabilities

If you have a disability, long-term health condition, specific learning difference, mental health diagnosis or symptoms, contact the Student Support Office for assistance.

Unable to Submit on Time?

If events prevent you from submitting on time, guidance on extenuating circumstances is available in the Student Handbook or from the Student Support Office.

Administration of Assessment

Module Leader Name:	Manoj Shrestha
Module Leader Email:	stw0002@softwarica.edu.np
Assignment Category:	Written
Attempt Type:	Standard
Component Code:	CW

Assessment Criteria

GRADE	CLARITY AND COMPLETENESS OF THE PROJECT	RELEVANCE AND SIGNIFICANCE OF THE RESEARCH QUESTION(S) AND OBJECTIVES	IMPLEMENTATION OF METHODOLOGY	TECHNICAL COMPETENCE AND RELEVANCE	WRITING QUALITY AND PRESENTATION
First **≥70**	The project is clear, comprehensive, and well-organized. It effectively communicates the research question, objectives, and findings.	The research questions and objectives are clearly stated and well-defined. They are directly related to the problem statement and address important gaps in the field of cyber security.	The methodology is clear, appropriate, and well-supported, and the proposed solution is well-described and justified. The project management plan is feasible and well-defined, and risks, ethical considerations, and legal and regulatory issues are identified and addressed appropriately.	The project demonstrates a high level of technical competence and relevance to the field of cybersecurity. The project shows evidence of a deep understanding of the topic, and the prototype is well-designed, functional, and secure. The project makes use of appropriate tools and techniques, and the code is well-documented and commented on. The project is relevant to the student's prior learning and experience in their bachelor's program.	The project is written in clear and concise language, with a logical flow of ideas and well-structured paragraphs. The writing is free of errors in grammar, punctuation, and spelling. The project is presented in a professional manner, with appropriate formatting, citation style, and referencing. The student presents their project in a clear and confident manner during the defense, demonstrating a deep understanding of the research and its implications.
Upper Second **60-69**	The project is mostly clear, comprehensive, and well-organized. It effectively communicates the	The research questions and objectives are stated but could be more clearly defined or	The methodology is generally clear and appropriate, but there may be some gaps in the	The project demonstrates a reasonable level of technical competence	The project is generally well-written, with a coherent structure and logical progression of ideas. There may be some errors in grammar,

	research question, objectives, and findings with minor issues.	lack a direct connection to the problem statement. They address some gaps in the field of cyber security.	data collection or analysis techniques. The proposed solution is described but may not be fully justified. The project management plan is the most feasible and well-defined, but some timelines or milestones may be unclear. Risks, ethical considerations, and legal and regulatory issues are identified but may not be fully addressed.	and relevance to the field of cybersecurity. The project shows evidence of a good understanding of the topic, and the prototype is functional and secure. The project makes use of appropriate tools and techniques, and the code is adequately documented and commented on. The project is somewhat relevant to the student's prior learning and experience in their bachelor's program.	punctuation, or spelling, but they do not significantly detract from the overall quality of the work. The project is presented in an acceptable manner, with mostly correct formatting, citation style, and referencing. The student presents their project in a mostly clear and confident manner during the defense, demonstrating a good understanding of the research and its implications.
Lower Second **50-59**	The project is somewhat clear, comprehensive, and organized. It effectively communicates the research question, objectives, and findings but with some issues.	The research questions and objectives are somewhat unclear or poorly defined. They may not be directly related to the problem statement or may not address important gaps in the field of cyber security.	The methodology is somewhat unclear or not fully appropriate, and the proposed solution is not well-described or justified. The project management plan is not fully feasible or well-defined, and timelines, milestones, or deliverables may be unclear or unrealistic. Risks, ethical considerations, and legal and regulatory issues are identified but not fully addressed.	The project demonstrates some technical competence and relevance to the field of cybersecurity. The project shows evidence of a basic understanding of the topic, and the prototype is functional but may have some security vulnerabilities. The project makes use of some appropriate tools and techniques, and the code is minimally	The project is somewhat difficult to read due to unclear writing or poor organization. There may be several errors in grammar, punctuation, or spelling that detract from the overall quality of the work. The project is presented in an inconsistent manner, with some errors in formatting, citation style, or referencing. The student presents their project in an uncertain manner during the defense, demonstrating some understanding of the research and its implications.

				documented and commented on. The project is loosely relevant to the student's prior learning and experience in their bachelor's program.	
Third **40-49**	The project is unclear, incomplete, or poorly organized. It does not effectively communicate the research question, objectives, and findings.	The research questions and objectives are unclear, poorly defined, or not relevant to the problem statement. They do not address important gaps in the field of cyber security.	The methodology is unclear or inappropriate, and the proposed solution is not described or justified. The project management plan is not feasible or well-defined, and timelines, milestones, or deliverables are unrealistic or missing. Risks, ethical considerations, and legal and regulatory issues are not fully identified or addressed.	The project demonstrates limited technical competence and relevance to the field of cybersecurity. The project shows evidence of a limited understanding of the topic, and the prototype is incomplete or not functional. The project makes use of inappropriate or inadequate tools and techniques, and the code is poorly documented and commented on. The project is not relevant to the student's prior learning and experience in their bachelor's program.	The project is poorly written and difficult to follow, with no clear structure or logical progression of ideas. There are numerous errors in grammar, punctuation, or spelling that significantly detract from the quality of the work. The project is presented in an unprofessional manner, with inconsistent or incorrect formatting, citation style, or referencing. The student presents their project in a confusing and unclear manner during the defense, demonstrating a lack of understanding of the research and its implications.
Fail **<40**	The project is significantly unclear, incomplete, or poorly organized. It does not effectively	The research questions and objectives are missing or not addressed in the	The methodology, proposed solution, project management plan, and/or identification of risks,	The project is incomplete or non-functional, and/or the project demonstrates a	The project is unacceptable in terms of writing quality and presentation, with numerous errors in grammar, punctuation, or spelling that make it

	communicate the research question, objectives, and findings.	proposal.	ethical considerations, and legal and regulatory issues are not present or are seriously deficient.	lack of technical competence and relevance to the field of cybersecurity. The project makes use of inappropriate or inadequate tools and techniques, and the code is poorly documented and commented on. The project is not relevant to the student's prior learning and experience in their bachelor's program.	difficult to read and understand. The structure and organization are unclear, and the project is poorly presented with many formatting, citation style, or referencing errors. The student fails to present their project in a clear and confident manner during the defense, demonstrating a lack of understanding of the research and its implications.
Late submission	0	0	0	0	0