ASSESSMENT BRIEF 3

Assessment Details

Unit Code Title	ISYS1002: Cybersecurity
Title	Assessment 3: Cyber Risk Assessment and Mitigation for Organisations
Type	Report
Due Date	Monday 18 August 202511:59 pm AEST/AEDT (start of Week 7)
Feedback & Grades Release	Monday 25 August 202511:59 pm AEST/AEDT (start of Week 8)
Weighting	50%
Length	2000 words
Individual / Group	**Individual**
Submission	Word document submitted to Turnitin
GenAI Use Level	Level 2. Purpose-Specific GenAI Use

Learning Outcomes

This assessment evaluates your achievement of the following Unit Learning Outcome:

ULO1: describe and apply the key principles of cyber security.

ULO2: identify and classify different types of cyber security threats and discuss various mitigation strategies through appropriate techniques.

ULO3: differentiate spheres of security.

ULO4. explain and demonstrate cyber security ethics and administration processes.

Assessment Rationale

In this Assessment, you will continue to deepen your understanding of the cybersecurity landscape and management processes, focusing on real-world issues such as BYOD policies, phishing threats, and ethical considerations in cybersecurity. You will learn to assess risks, develop mitigation strategies, and promote ethical behavior, preparing you for practical cybersecurity challenges.

Task Description

As a cybersecurity consultant, you will assess the risks associated with the BYOD policy, develop guidelines to combat phishing, and investigate ethical requirements for a selected organization. You will categorize threats and vulnerabilities across different security domains and recommend appropriate mitigation strategies.

As part of the work, you are required to complete the following tasks:

Task 1:
Assume your selected organisation is currently using a password-based authentication system to control user access to the organisation's information system. However, the Bring Your Own Device (BYOD) and work at home policy recently implemented by the organisation has raised some security concerns. As a security consultant, assess the risk from the BYOD policy and work at home to the organisation's most critical/top five information assets you identified in **Ass Two**.

- Identify and discuss two (2) threats the BYOD and work at home policy may bring to each of the five (5) critical assets identified in Ass 2.
- Identify and discuss potential two (2) weaknesses (vulnerabilities) of each of the top five assets identified in Ass 1 based on three information security components: confidentiality, integrity, and availability.
- Categorize the identified threats and vulnerabilities into different security domains such as system security, network security, and application security and complete TVA sheet.
- Assess and prioritise the risk to the organisation's information system using a qualitative risk assessment approach with the top five information assets against the threats identified above and document the risk assessment process in detail.
- Recommend at least two (2) security measures against each asset to mitigate the risk (with the top threat) identified above. Your recommendation is expected to deal with different security domains such as system security, network security, application security, etc. Justify your recommendation considering feasibility and cost.

You are free to make any assumption about the asset values. Exposure factors (before and after control), and annualised rate of occurrence (before and after control) should be supported by your own and public domain knowledge and references. Cost of controls should be realistic and supported by vendor/provider references.

Task 2:

The organisation you selected has reported a growing volume and sophistication of email-based cyber threats, including spamming, phishing, and social engineering attacks such as spear phishing and business email compromise (BEC). As a cybersecurity strategist, you are tasked with designing a multi-layered, organization-wide defense strategy against these threats. Your report must address both technical and human factors. Support your work with academic research and industry best practices.

Task 3:

Investigate and critically analyse the ethical obligations applicable to your selected organisation operating within a highly regulated industry. The organisation maintains a complex IT infrastructure and handles sensitive user data. Your analysis should focus on the ethical requirements that information system users—both technical and non-technical—must adhere to. Your response should include the following components:

- Discuss how ethical dilemmas impact different security domains within the organization
- Discuss how non-ethical behaviour of the users and IT staff of the selected organisation impacts security positions within the organisation.
- Discuss methods or strategies your selected organisation should take to deter employees from unethical behaviour and promote ethical behavior.

You are free to make any assumption(s) you wish regarding the existing controls, business profile, etc., which will need to be documented in the appropriate sections of your report. However, your analysis should be grounded in industry best practices, relevant regulatory frameworks, and academic literature.

Your report should be well presented with clear headings, subheadings, section numbers etc.; Information should be presented logically, interestingly, easy to follow and well-supported arguments; cite all reference sources. Note that you are not allowed to cut and paste from online resources. Use your own words and figures. Acknowledge all reference sources.

Task Instructions

Make assumptions as needed regarding the organization’s existing controls and profile, ensuring you document these assumptions clearly in your report. Your final document should be well-structured, logically presented, and should cite all reference sources used.

- Include a reference list in APA7 style.

- Copy and paste the appropriate GenAI use acknowledge statement onto the end of after your reference list

Resources

1. Modules 1-6 contents
2. The Report Template provided. This is located in the Assessment 3 folder in the Blackboard unit site.

Referencing Style

You are expected to adhere to APA7 or Harvard referencing style). Please visit to the SCU Library referencing guides for details.

Deliverables & Submissions

A Turnitin link (draft portal) has been set up to provide you with an opportunity to check the originality of your work until your due date. Please make sure you review the report generated by the system and make changes (if necessary!) to minimise the issues of improper citation or potential plagiarism. If you fail to follow this step, your report may not be graded or may incur late feedback.

You can check your Turnitin similarity report as many times as you like (your paper will not be saved) via the draft submission portal. When you have your final report ready, submit to the Turnitin final submission portal (you may only submit to this portal once as your paper will be saved) for marking.
Only Microsoft Word documents submitted via the Turnitin portal on Blackboard will be accepted. The report should be around 1500-2000 words (excluding table of contents, tables, figures, and references)
The first page of the report should have your name, student ID, ISYS1002 Assignment 3, and the date you submit your assignment. You must label your submission with your surname and initials and the assessment task's name, eg.

Gsorwar_ISYS1002_A3_Case study.docx

Generative Artificial Intelligence (GenAI) Guidelines

Conditions of Use

Design Guide: Conditions of Use

Level	Descriptor	Description
2	**Purpose-Specific GenAI Use**	GenAI tools may be used for specific assessment tasks or purposes as identified and scaffolded by the Unit Assessor.

Permitted Uses (Level 2)
Design Guide: Permitted Uses:

Gen AI Use Case	Conditions / Comments
Brainstorming ideas	Use GenAI to refine organisation ICT Scenarios If you don't have access to a real organisation.
Understanding Technical Concepts	Use GenAI to understand specific concepts such as defence-in-depth, definition of TVA, etc.
Planning and structuring the Report format	Use GenAI to refine the structure of the report

Evidence of GenAI Use

You may be required to demonstrate how you have used GenAI to complete this assessment. It is your responsibility to maintain accurate and detailed records of your GenAI use.

For further information see Evidence of GenAI Use Guide. This guide provides information regarding the types of evidence that may be requested.

GenAI use Acknowledgement Statement

The use of GenAI must be acknowledged appropriately. Failure to do so may result in an academic integrity breach, as outlined in the Student Academic and Non-Academic Misconduct Rules, Section 3.

For guidance on proper referencing and citation of GenAI-generated content, please consult the SCU Library Guide on Referencing: SCU Library Guide Referencing.

IMPORTANT:

The following statement **must be** copied and pasted to the last page of your assessment submission. Complete the statement accurately.

Acknowledgement Statement:

- **Option 1 (If GenAI was used):**

"I acknowledge that I have used GenAI to complete this assessment. I used <GenAI tool(s)> to <specific purpose(s) of using GenAI> within the parameters outlined in the Assessment Brief and by the Unit Assessor. I have maintained accurate records of my GenAI use where applicable and acknowledge that I may be required to provide further evidence."

- **Option 2 (If GenAI was NOT used):**

"I acknowledge that I have not used GenAI to complete this assessment."

Marking, Grades & Feedback

Works submitted by the due date will be evaluated against the grading criteria and standards specified in the assessment rubric. For more information regarding SCU grades and standards, visit Final Grades.

Grades and feedback will be posted to the **Grades & Feedback** section on the unit learning site. Please allow up to seven days for marks to be posted.

Rules relating to Assessment and Examination

Please refer to How to apply for Special Consideration and Rules Relating to Awards - Rule 3 - Coursework Awards - Student Assessment and Examinations for information regarding:

- Extensions
- Special Consideration
- Late submissions
- Resubmissions
- SCU Grades
- Appeals
- Academic Integrity

If you have any questions regarding the above, please contact the Unit Assessor as soon as

Academic Integrity Declaration

By submitting this assessment, I declare that I have read and understood SCU's Academic Integrity policies and referencing guidelines, I am aware of the consequences of academic misconduct and confirm that this submission is my own original work, referenced appropriately, and has not been previously submitted. I authorise its reproduction for authentication purposes and understand the implications of a false declaration. I have adhered to guidelines regarding Generative AI.

Assessment Rubric

Marking Criteria and marks allocation	High Distinction (85–100%)	Distinction (75–84%)	Credit (65–74%)	Pass (50–64%)	Fail 0–49%
Identification and Discussion of Threats and Vulnerabilities 12 marks	Identifies and discusses two threats for each asset, offering clear and detailed explanations of their impacts on CIA Triad. Categorizes threats accurately and provides practical examples. Identifies and discusses two vulnerabilities for each asset, offering clear and detailed explanations of their impacts on CIA Triad. Categorizes vulnerabilities accurately and provides practical examples. Completes TVA	Identifies and discusses two threats for each asset with detailed explanations of their impacts on CIA Triad. Categorizes Threats accurately and provides relevant examples. Identifies and discusses two vulnerabilities for each asset with detailed explanations of their impacts on CIA Triad. Categorizes vulnerabilities accurately and provides relevant examples. Completes TVA sheet	Identifies and discusses two threats for each of the five assets, providing adequate explanations of their implications on CIA Triad. Shows competence in explaining threats in practical contexts. Identifies and discusses two vulnerabilities for each asset with adequate explanations. Categorizes vulnerabilities with reasonable accuracy and provides some examples. Brief TVA	Identifies and discusses two threats for each of the five assets with basic explanations. Shows satisfactory ability to relate threats to practical scenarios. Identifies and discusses two vulnerabilities for each asset with basic explanations. Categorizes vulnerabilities satisfactorily and provides minimal examples. No TVA	Fails to identify or discuss threats and vulnerabilities adequately, providing insufficient or unclear explanations.
Risk Assessment Process 10 marks	Conducts a thorough qualitative risk assessment with clear explanations. Prioritizes risks effectively and documents the process with high clarity.	Conducts a well-developed qualitative risk assessment with detailed explanations. Prioritizes risks effectively and documents the process clearly.	Conducts an adequate qualitative risk assessment with satisfactory explanations. Prioritizes risks reasonably well and documents the process adequately.	Conducts a basic qualitative risk assessment with satisfactory explanations. Prioritizes risks minimally and documents the process sufficiently.	Fails to conduct an adequate qualitative risk assessment, providing insufficient explanations and documentation.
Security Measures Recommendation. 10 marks	Recommends at least two (2) measures against each asset with substantial data and realistic	Recommends at least two (2) measures against each asset with substantial data and realistic assumptions but no	Recommends at least two (2) measures against each asset with adequate data and realistic	Recommends at least one measure against each asset with some data and reasonable assumptions but no	Fails to recommends some measures or providing insufficient explanations and justification.

Marking Criteria and marks allocation	High Distinction (85–100%)	Distinction (75–84%)	Credit (65–74%)	Pass (50–64%)	Fail 0–49%
	assumptions and references for a thorough justification	references for a thorough justification	assumptions and some references for a reasonable justification	references for a minimum justification .	
Defense strategy against email-based cyber threats 6 marks	Comprehensive, highly original, and well-integrated strategy. Demonstrates deep insight, strong critical thinking, and excellent use of real-world examples and references.	Well-structured and insightful. Most components are well developed with clear logic and solid supporting evidence.	Develops adequate guidelines with satisfactory instructions, addressing specific security domains reasonably well. Adequate use of references.	Basic coverage of required elements. Limited analysis and weak integration. Minimal supporting evidence.	Incomplete or unclear. Major gaps in understanding, analysis, or structure. Lacks research support.
Discussion of Ethical Requirements 12 marks	Investigates and documents ethical requirements thoroughly, discussing their impact on security domains effectively. Explains consequences of non-compliance clearly, and propose comprehensive strategies (at least four (4) for organisation to deterrent users from unethical behaviours to achieve selected organisation Cyber Security (with examples.	Investigates and documents ethical requirements with detailed explanations, discussing their impact on security domains adequately. Explains consequences of non-compliance reasonably well, propose adequate strategies (at least four (4) for organisation to deterrent users from unethical behaviours to achieve selected organisation Cyber Security (with examples).	Investigates and documents ethical requirements adequately, discussing their impact on security domains satisfactorily. Explains consequences of non-compliance minimally, and propose adequate strategies (at least three (3) for organisation to deterrent users from unethical behaviours to achieve selected organisation Cyber Security (with examples)	Investigates and documents ethical requirements with basic explanations, discussing their impact on security domains sufficiently. Provides minimal explanation of consequences, propose basic level of strategies (at least three (3) for organisation to deterrent users from unethical behaviours to achieve selected organisation Cyber Security. (No examples).	Fails to investigate or document ethical requirements adequately, providing insufficient explanations and insufficient to no details of strategies/measures organization could consider deterring their users from unethical behaviours to achieve Cyber Security.

Description of SCU Grades

High Distinction:

The student’s performance, in addition to satisfying all of the basic learning requirements, demonstrates distinctive insight and ability in researching, analysing and applying relevant skills and concepts, and shows exceptional ability to synthesise, integrate and evaluate knowledge. The student’s performance could be described as outstanding in relation to the learning requirements specified.

Distinction:

The student’s performance, in addition to satisfying all of the basic learning requirements, demonstrates distinctive insight and ability in researching, analysing and applying relevant skills and concepts, and shows a well-developed ability to synthesise, integrate and evaluate knowledge. The student’s performance could be described as distinguished in relation to the learning requirements specified.

Credit:

The student’s performance, in addition to satisfying all of the basic learning requirements specified, demonstrates insight and ability in researching, analysing and applying relevant skills and concepts. The student’s performance could be described as competent in relation to the learning requirements specified.

Pass:

The student’s performance satisfies all of the basic learning requirements specified and provides a sound basis for proceeding to higher-level studies in the subject area. The student’s performance could be described as satisfactory in relation to the learning requirements specified.

Fail:

The student’s performance fails to satisfy the learning requirements specified.