APPROVED BRITISH UNIVERSITY BUV

27 NOV 2024

BRITISH UNIVERSITY VIETNAM BUV

In collaboration with Staffordshire University

Module Title:	Cyber Security 2
Module Code:	COMP50003
Attempt:	First Sit
Group or Individual:	Group Assignment
Assignment Number:	2 of 2
Assignment valid until:	April 2026
Assignment Title:	Group assignment based on a case study
Weighting:	60%
Assignment set by:	Dr. Donie Jardeleza
Assignment verified by:	Dr. Viju Prakash Maria John
Word Limit:	6000 words

Date Issued to Students:	17 March 2025
Submission Date and Time:	See the Canvas module homepage for the submission date
Method of Submission:	Canvas Submission

Learning Outcomes to be assessed:

1. Demonstrate a critical understanding and be able to evaluate fundamental aspects of cyber security. [Learning, Reflection]
2. Formally identify risks to the security of data, systems, and networks when presented with a given scenario. [Enquiry, Analysis, Problem-solving]
3. Critically analyse the process by which disaster recovery and risk prevention plans are developed and be able to appraise such plans. [Analysis, Communication, Reflection]

AI Level:

The table below shows to what extent you are allowed to use Generative AI (GenAI) tools such as ChatGPT in your assessment. Please refer to the BUV Student AI guidelines for full information on how you can ethically use GenAI tools at BUV.

AI Level	Description	This assessment
1. No AI	The assessment is completed entirely without AI assistance. This level ensures that students rely solely on their knowledge, understanding, and skills. AI must not be used at any point during the assessment.	
2. AI Assisted idea generation and structuring	AI can be used in the assessment for brainstorming, creating structures, and generating ideas for improving work. **No AI content is allowed in the final submission.**	
3. AI Assisted language editing	AI can be used to make improvements to the language of student-created work to improve the quality of the final output, but no new content can be created using AI. **AI can be used, but your original work with no AI content must be provided in an appendix.**	X
4. AI task completion, human evaluation	AI is used to complete certain elements of the task, with students providing discussion or commentary on the AI-generated content. This level requires critical engagement with AI-generated content and evaluating its output. **You will use AI to complete specified tasks in your assessment. Any AI-created content must be cited. You must not use AI to support your commentary or evaluation of the work.**	
5. Full AI	AI should be used as a 'co-pilot' in order to meet the requirements of the assessment, allowing for a collaborative approach with AI and enhancing creativity. **You may use AI throughout your assessment to support your own work and do not have to specify which content is AI-generated.**	

Assessment Brief:

A private organisation, **DigiTech Corporation**, experienced a period of unprecedented growth and urgently relocated to a larger facility to accommodate the expanding company. The facilities are located on the 6th, 7th, and 8th floors of the Hualon Tower. Following the latest penetration testing by a licensed independent contractor, the evaluation of security procedures, policies, and protocols that exist at DigiTech's current facility has not been doing well.

Their systems do not anymore fit for its purpose as they are outdated and are considered obsolete for the new location's network design. Internally, there have been reports of related cyber security breaches. The organisation's network has endured several attacks and DoS outages which in the long run if allowed to continue, will severely harm DigiTech's reputation. So, the company decides to review and secure its systems located on the 6th, 7th, and 8th floors in the Hualon Tower.

As a team of cyber security specialists, you have been asked to undertake a review of the security procedures and protocols within the specified locations of the Hualon Tower. Your team has been tasked with undertaking this review and providing a security recommendation to secure the 6th, 7th, and 8th floors in the Hualon Tower.

In writing this report, you should refer to the security requirements given in the best-known standard/framework (e.g., NIST/ISO27001) while conducting your investigation. You also need to justify appropriate reasons for incorporating further related standard/framework in your security investigation within the 'Scope' section of your group report. After performing your technical analysis, your group is required to make a 15-minute presentation of your findings. This should highlight recommendations concerning upgrading & updating the security model & procedures and protocols at the new location. This will be assessed by the marking team.

The focus of this assignment should be on the application of security methods, techniques, standards, and professional practices, as introduced in the lectures and tutorials, in terms of a real-world case study.

The aims are:

- to develop a more in-depth understanding of the underlying information security concepts.
- to gain hands-on experience in analysing risks and evaluating security requirements.
- to develop skills in formulating these requirements as general security policies and procedures that can be understood by a variety of stakeholders: business managers, security professionals, software engineers, administrators, and users.

Scenario

DigiTech Corporation is progressive and needs to relocate from its current location to a larger facility in a new tower on the edge of town to accommodate a wave of new hires. As the IT group responsible for this relocation, your team needs to take into consideration the security procedures and protocols of the following:

- Cyber Security intelligence lab. There are fifty computers, five printers, four surveillance cameras, two Access Points (AP), two RFID card readers, and one scanner (located on the 8th floor).

- Applications Development lab. There are one hundred computers, ten printers, four surveillance cameras, two Access Points (AP), two RFID card readers, and one scanner (located on the 7th floor)

- Data Centres, Server Rooms, Camera control room, Networking devices (located on the 6th floor)

Case Management

You will need to identify and assign roles to every group member. The **group leader** will be responsible for disseminating responsibilities and managing the group members and the group activities during the investigation. You need to submit all the necessary paperwork as appendices to the report that accompanies your investigation. This may include, interview notes, onsite maps, photographs as well as any contemporaneous notes (as a separate annexure to support the report) that you may develop or find during the investigation.

Presentation Structure

1. Physical Security Assessment (Task-1):

Review the logical (e.g., security policies, procedures, and protocols of the company) and physical infrastructure (i.e., devices and access controls) security that will be needed to secure the new location.

For example: evaluate the new locations' infrastructure security controls against the CIA Triad. Your group may also use the business classification model: highly sensitive, sensitive, internal, and public categories to classify the critical information/resources, infrastructure, and assets.

Outline the logical and physical security measures reviewed. Discuss how the infrastructure meets the requirements of the CIA Triad and business classification model.

2. IT Security and Risk Assessment (Task-2):

Identify critical security vulnerabilities, security models, threats, risks to the reviewed, and IT infrastructure and assets of the organisation. Use the business classification model to prioritize risks and present your risk analysis results.

For example: using the business classification model (highly sensitive, sensitive, internal, public) of the sensitive information and supporting assets within the new location, perform a risk analysis. Create a risk ranking/hierarchy to identify top risks/threats to the security of the new location.

3. Assets and Security Controls Assurance Review (Task-3):

Review and evaluate the assurance level and compliance of security controls implemented to protect assets and business operations of the company. Develop a threat model to assess the effectiveness of these controls.

For example, your group may develop a threat model (best and worst cases) for evaluating the implementation of security controls to maintain assets or business ownership.

4. Mitigation and Security Recommendations (Task-4):

Determine and propose a strategy/model, which can be implemented in the new location to improve the ongoing security process and controls and mitigate top rank risks and threats identified in Task 3.

For example, your group may develop your mitigation model/strategy that should reference international standards such as NIST or ISO27001 and provide clear rationales for each recommendation.

Guidelines:

The 15 Minute Group Presentation will consist of three sections:

A. A brief Introduction of the given assignment (i.e., Tasks 1, 2, 3, or 4) and investigation methods or techniques used in each of the 4 tasks.

B. Presentation of security investigation outcomes and findings from Tasks 1-3.

C. Reasons and justification for the proposed mitigation model or security enhancement recommendations - Task 4.

D. A conclusion summarising your findings and wrapping up your presentation.

E. There will be a 5-Minute Question and Answer session after your presentation. Each group member will be asked a question to check your understanding of the assignment.

F. Each group member will be required to complete a peer assessment in which they will provide feedback on the contribution of other group members. These shall be submitted confidentially to the module leader.

Additional Guidance Notes

a) Your group may want to start Task 1 by outlining the main business functions of the company by describing valuable assets, roles, and relevant operations. Consider hardware, software, and human elements in categorising DigiTech's assets at the new location.

b) Task 2 can involve the identification of the relevant vulnerabilities and threats to the integrity, confidentiality, and availability together with an assessment of the corresponding risks to assets/business at the new location.

c) The critical focus of Task 3 is on security protection. This involves assessing security controls such as authentication, authorisation, encryption, security protocols, and auditing together with the appropriate mechanisms and techniques for achieving these properties.

d) Task 4 involves looking for improvements in the whole security process lifecycle: protection, detection, and reaction, and outlining the measures recommended for each of these stages.

e) All group members are expected to contribute equally to the preparation and delivery of the presentation.

f) Do not include your name anywhere on your assignment.

g) Your assignment should be written in a font size of 12.

h) You must include a correctly formatted Reference List on a separate page at the end of your essay. This must only include references to work that you have directly cited in your essay.

i) You must include your accurate word count at the end of your assignment.

j) Use standard margins for the assignment and 1.15 line spacing.

k) Only **Microsoft PowerPoint** files should be used for Presentation assessments. Please allow time for conversion to these formats if required.

l) Only **Microsoft Word** files should be used for your report assignments. Please allow time for conversion to these formats if required.

m) When you upload your file for submission you must name the file with the following format: **'<Module Code> <Group Number>'**

n) Each presentation must be no longer than 15 minutes. You will be given a warning when you have 5 minutes remaining.

o) After 15 minutes you will be stopped. If you have not completed your presentation at this time, this may mean that certain sections of your presentation may receive a mark of zero. You are strongly encouraged to practice the timing of your presentations on multiple occasions, and you will be given some time in-class time to do this.

p) The presentations will be double marked. You will be allocated a 15-minute slot for your presentation. You must be ready to start your presentation at the exact start time of your slot.

q) The presentation will be recorded.

r) The marking scheme that will be used to mark your work is shown at the end of this document in Appendix 1.

Submission Procedure

You are not required to print and submit a hard copy of your work, as all submissions are carried out electronically through Canvas. Please ensure you do not wait until the last minute to carry out your submission; computer problems can happen at any time, and this will not be accepted as an excuse for a late submission. This includes internet connectivity issues. When you submit your assignment, it is in your best interests to save and/or print a copy of your online submission receipt to prove that you have submitted your assignment on time.

If you feel that you can't submit your assessment on time, you should speak to your module leader who will help you to work out how you can hand it in on time.

If unexpected circumstances which you could not have planned for have happened, you may be able to claim for exceptional circumstances to be taken into account. There is more information here.

If you have no exceptional circumstances and you do not submit you will fail the assessment. If you submit within 1 week of the submission deadline we will mark your work as late, meaning the maximum mark you can achieve is the basic pass mark and this will count as your first attempt. If you are taking a re-sit assessment, late submissions will not be accepted.

Please see the Staffordshire university regulations here for more information

The Maximum word limit is shown on the front cover of the assignment.

You must provide an accurate word count at the end of your assignment. This word count must be placed before your reference list and should include all the written content of your assignment **excluding** the words used in any cover pages, contents pages, titles, sub-titles, reference lists, and appendices.

In the assignment, in addition to the word limit, you may make sensible use of tables, images of academic models, diagrams, figures, and student-created graphics such as Word-Art, etc. without penalty up to a maximum of 30% of the stated word limit of the assignment as shown on the front cover. In no circumstances must your overall use of words in these tables, models, etc. exceed this maximum 30% limit. **If a marker feels that you have used tables simply to avoid the word count, they may count these words as part of your word count.**

A sliding scale of penalties for excess length will be imposed according to the amount by which the limit has been exceeded.

1-10% excess	no penalty
11-20% excess	10% reduction in the mark
21-30% excess	20% reduction in the mark
>30% excess	the work will be capped at a pass i.e. 40%

NB. None of the above penalties will be used to change your mark that is above the pass mark, to one that is below the pass mark. Therefore, the *maximum penalty* for exceeding the word limit will be a reduction to a passing grade.

Please note that students' work is regularly checked to ensure that the stated word count matches what has been submitted.

Academic Misconduct and Plagiarism

BUV follows Staffordshire University policy on academic misconduct and takes suspected cases of academic misconduct, including plagiarism very seriously. The penalties are severe and can in some cases result in a student not being allowed to continue their studies. Plagiarism can happen in any type of assessment where you are given the questions or tasks in advance.

The Staffordshire University policy on Academic misconduct can be found here: and you are strongly encouraged to familiarise yourself with this.

You will have committed academic misconduct if you commit any of the following:

- Plagiarism
- Self-Plagiarism
- Collusion
- False Declaration
- Fabrication or Falsification of Data
- Bribery or Intimidation
- Contract Cheating
- Examination Misconduct

Please see here for a detailed explanation of these terms or click the individual links above.

All work submitted at BUV must be composed in English by the students themselves. Using online software to translate work originally written in a language other than English is not permitted, as it misrepresents the level of effort you have put into completing the assessment. You are reminded to refer to BUV's Artificial Intelligence (AI) guidelines for a full understanding of the permissible use of AI technologies, including Generative Artificial Intelligence (GenAI) tools. The use of online paraphrasing tools and other AI-powered writing aids is governed by these guidelines. Any violations of these guidelines may be treated as academic misconduct, or you may receive significant mark penalties.

If Academic Misconduct is proven by the university, then typical punishments include:

- The grade for your assessment, is reduced to zero with the right to resubmit.
- The grade for the whole module or super module being reduced to zero with the right to resubmit.
- Failure of the entire level of which you are currently studying with a requirement to re-start the level at the next opportunity
- Failure of the award and/or termination of your studies at the University. Your ability to reapply and enrol again at the university may also be restricted, normally for two whole academic years.

BUV encourages you to refer to appropriate academic sources, as long as you reference these correctly, and do not use too much material from the source.
You must use the Harvard referencing system for all your assignments unless you are told otherwise by your Module Leader. If you do not know how to do this, please follow the guidelines given at this website address: http://www.staffs.ac.uk/support_depts/infoservices/learning_support/refzone/harvard/

BUV employs Turnitin to assess all submissions for potential academic misconduct. This software highlights to the examiners in detail where material may have either been copied directly or paraphrased from a source with correct citation.

Appendix 1: Marking Rubric for Group Assignment

Criteria	% Weight	0%-39%	40%-49%	50%-59%	60%-69%	70% - 79%	80% - 89%	90% - 100%
Introduction	5%	No introduction or fails to introduce.	Vague introduction with little relevance.	Basic introduction with some relevance.	Adequate introduction, covers essentials.	Comprehensive introduction.	Detailed and engaging introduction.	Exceptional, insightful introduction.
Task 1 - Physical Security Assessment	15%	No assessment or irrelevant content.	Minimal relevant content.	Basic assessment using some relevant models.	Adequate use of CIA Triad and models.	Good review with proper use of models.	Very good, insightful review of models.	Exceptional, thorough use of all models.
Task 2 - IT Security and Risk Assessment	15%	No assessment or fails basic criteria.	Minimal risk analysis.	Basic risk analysis, some criteria met.	Adequate risk analysis, most criteria met.	Good risk analysis, solid criteria usage.	Very good analysis, nearly all criteria met.	Exceptional analysis, exceeds criteria.
Task 3 - Assets and Security Controls Assurance Review	15%	No review or irrelevant content.	Minimal use of threat models.	Basic use of threat models, some criteria met.	Adequate use of models, good evaluation.	Good review and evaluation of controls.	Very good review, thorough evaluation.	Exceptional review, outstanding evaluation.
Task 4 - Mitigation and Security Recommendations	20%	No recommendations, lacks understanding.	Minimal recommendations, some relevance.	Basic recommendations, meets some standards.	Adequate recommendations, meets standards.	Good recommendations, solid understanding.	Very good recommendations, high standards.	Exceptional recommendations, best practices.
Conclusion	5%	No conclusion or fails to summarize.	Minimal conclusion, lacks clarity.	Basic conclusion, some clarity.	Adequate conclusion, summarizes well.	Good conclusion, clear and concise.	Very good conclusion, detailed.	Exceptional conclusion, insightful.
Questions and Answers	5%	No responses or irrelevant.	Minimal responses, some relevance.	Basic responses, generally relevant.	Adequate responses, answers questions.	Good responses, clear and helpful.	Very good responses, insightful.	Exceptional responses, highly informative.
Peer Assessment Marks	5%	Refer to the Peer Assessment Form	Refer to the Peer Assessment Form	Refer to the Peer Assessment Form	Refer to the Peer Assessment Form	Refer to the Peer Assessment Form	Refer to the Peer Assessment Form	Refer to the Peer Assessment Form
Time Management - Each Member	5%	Major timing issues, lacks cohesion	Some timing issues, minimal cohesion	Minor timing issues, basic cohesion	Minor timing issues, generally cohesive	On time, good cohesion	On time, very cohesive	Perfect timing, exceptional cohesion

Presented Equally Cohesive and Coherent								
AI Usage	10%	No AI used or irrelevant application.	Minimal AI usage, not impactful.	Basic AI integration, low impact.	Adequate AI usage, noticeable impact.	Good AI integration, beneficial impact.	Very good AI application, high impact.	Exceptional AI use, highly innovative.

Peer Assessment Form

Name of student: ______________________________

Write the name of each group member in each corresponding column. For each person, indicate the extent to which you agree with the statement on the left, using a scale of 1 – 4 (1 - **strongly disagree; 2 – disagree; 3 – agree; 4 – strongly agree**). Sum up the numbers in each column.

Evaluation Criteria	**Group member:**	**Group member:**	**Group member:**	**Group member:**
Attends group meetings regularly and arrives on time.				
Contributes meaningfully to group discussions.				
Completes group assignments on time.				
Prepares work in a quality manner.				
Demonstrates a cooperative and supportive attitude.				
Contributes significantly to the success of the project.				
TOTAL				