MIS761 – Cyber Security Strategies

Trimester 2, 2024

Assessment Task 2 – Group Assignment: Cyber Resilience Review

DUE DATE AND TIME: **20th Sept. 2024, 8 PM (AEST)**
PERCENTAGE OF FINAL GRADE: Weighting = 35 **%**
HURDLE DETAILS: **No Assignment Hurdle**

Learning Outcome Details

Unit Learning Outcome (ULO)	**Graduate Learning Outcome (GLO)**
ULO3: Apply relevant security policies and technologies in the creation of cybersecurity solutions that align with an organisation's business goals and aspirations.	**GLO1**: Discipline-specific knowledge and capabilities. **GLO5**: Problem solving.
ULO4: Develop adaptive solutions for authentic and real-world security issues within an organisation's cybersecurity service management.	**GLO1**: Discipline-specific knowledge and capabilities. **GLO4**: Critical thinking. **GLO5**: Problem solving.

Assessment Feedback:

Students who submit their work by the due date will receive their Marks and Feedback within 15 Working Days on CloudDeakin.

Assignment Description/Requirements

This is a **group assignment** and you must be a member of and contribute to the group effort in order to submit your assignment and receive a mark.

You are required to work in groups of three (3) students. Your overall task is to conduct a comprehensive cybersecurity review of a real-life business entity, which you will source yourselves. This involves using a structured questionnaire derived from the NIST Cybersecurity Framework 2.0. Your task will be to assess the current cybersecurity posture of the business, develop a target profile that aligns with its business needs and regulatory environment, and propose a detailed action plan to address identified gaps. You should present your review in the form of a Business Report in the format provided in *Report Structure and Layout Format* below.

The maximum word count for the report is **3500 +/- 10% words**. (Note that Reference List, Appendices and Tables are not included in the word count)

Team Meetings

Your team is required to meet (virtually or physically) regularly. You must conduct the meetings at a mutually agreed upon time.

Each team member is expected to attend and contribute to each meeting or offer a valid apology if absent.

NOTE: It is strongly advised that you use Microsoft Teams for all communications (Deakin University's Office 365 subscription provides Teams to all students).

IMPORTANT: You are required to document (i.e., record meeting minutes) your meeting discussions and decisions. This includes meeting details (e.g. date, time, who was present for the meeting, absentees/apologies, action items and deadlines, allocated team members etc.) including regular inter-team communications.

The topics that should be covered in these Meetings are as follows:

- List who is Chairing the meeting, attendees, apologies and non-attendees (why?).
- Each member is to report back on action items, progress and deliverable outcomes completed.
- Describe what tasks are you currently working on?
- Discuss what you plan to do the next?
- Identify any roadblocks are you facing as a group and as individuals?
- Discuss and develop possible resolutions, noting assigned/reassigned personnel resources.

Remember the essence of these meetings is that they are short and sharp and let the team know what everyone is working on at any given time, what the potential roadblocks are and if there are any major issues that need to be addressed.
In addition to your team meetings, time will be allocated in some of our seminars for you to work on the assignment.

You need to provide evidence of your team meetings in the final project report documenting team attendance and 2 key outcomes from each meeting. The meeting minutes are be presented in the report Appendix.

Selecting a Business Organisation to Investigate

If you are in doubt about the suitability of the organisation which you have chosen, please check with your Tutor as early as possible. The business owner or a manager from the organisation must also approve your review and will need to sign the Letter of Consent (please refer to Report Structure and Layout Format below).

Some suggested types of businesses/organisations for this review are:

- A local family business or other small business;
- A local community library, sporting association or other NGO/NPO;
- A department within a larger business;
- A small overseas business (this option may suit some Cloud and International students).

Data Collection

For this assessment, you will evaluate the business's cybersecurity practices using a detailed questionnaire that aligns with the NIST Cybersecurity Framework. The questionnaire covers 22 categories across the six functions of the framework. You are required to:

- **Rate Each Category**: Assess and score each category on a scale from 0-4, based on the degree to which the business has implemented the corresponding cybersecurity measures.
- **Document Findings**: For each statement in the questionnaire, provide not only a score but also a description of how the business demonstrates compliance or falls short of the framework's criteria. Use NIST's Implementation Examples as a reference to understand potential ways of meeting each criterion. Remember, these examples are not exhaustive, and deviation from them does not automatically imply a failure to meet the standard.
- **Customize the Questionnaire**: Consider tailoring the questionnaire to include additional questions on specific subcategories that are particularly relevant to your target profile analysis. This customization will allow for deeper investigation into areas of keen interest or concern.

Data collection can be conducted through various methods, including face-to-face, email, or phone interviews with key personnel such as the managing director, business owner, or IT manager. This flexibility allows you to engage with businesses remotely if necessary, such as those located in different countries. Real-time interviews are highly recommended as they allow for immediate follow-up questions, providing deeper insights into the business's cybersecurity practices and the rationale behind them. Additionally, consider exploring the business organization’s website and any policy documents provided by the organization to supplement your findings. This approach ensures a comprehensive understanding of the business’s cybersecurity practices and the contextual factors influencing them.

Assignment Business Report

Audience

Your business report is intended for your group's client business owner/manager. Therefore, the style and tone of the report should take this into consideration. You should write the report in a professional business style, selecting appropriate fonts and styles and writing in a constructive (non-critical) manner appropriate to be read by the business owner or manager.

We suggest you review this resource at the outset:
https://www.deakin.edu.au/students/studying/study-support/academic-skills/report-writing

Report Structure and Layout Format

Your business report should consist of the following sections.

Title Page

Disclaimer

You MUST include the following disclaimer on a separate page (see below).

IMPORTANT NOTICE: DISCLAIMER

This report, including any recommendations contained therein, was prepared for the purposes of academic assessment in Deakin University's unit:

- MIS761 – Cyber Security Strategies.

It should not be relied upon, or used in any way as a basis for making any "real-life" commercial decisions.

The assistance of (insert name of organisation) in providing us with access to its staff and records in the course of researching the report is gratefully acknowledged.

Letter of Consent

You MUST include the following letter of consent on a separate page:

Dept. of Information Systems and Business Analytics
Deakin Business School, Faculty of Business and Law
Deakin University

LETTER OF CONSENT
MIS761 – Assignment – CYBER RESILIENCE REVIEW REPORT

Dr. Wilson Li
Dept. of Information Systems and Business Analytics
Deakin University
221 Burwood Hwy
Burwood 3125
Phone: (03) 9244 6370
Email: wilson.li@deakin.edu.au
..... / ..... / 2024

Dear Wilson,

I/we hereby give permission for the following students:

.....
.....
.....
.....

to review the cybersecurity aspects of our business organisation:

.....

In order to fulfill the Assignment requirements for MIS761.

I/we have read the Assignment requirements, and understand that the students will behave responsibly and professionally in this review at all times.

I/we expect to receive a copy of the final assignment report, containing the results of the review, during the week beginning 18th October 2024.

Yours sincerely,

..... (signed)

..... (Please Print Name)

..... (Work email address)

Executive Summary (approximately 150 words)

Provide an overview of key findings from the review, intended for the business owner.

Table of Contents (separate page)

Introduction (approximately 100 words)

Provide an overview of the following:

- Introduction to the cyber security resilience review.
- The organisation name, industry, location and brief business background.
- Scope, aims and constraints for the review.

Report Body: Business Background and Context (approximately 400 words)

Provide a description of the organisational context in terms of potential organisational influences on cyber security strategy, including:

- **Business Profile and Core Ideals**: Describe the business, including the products and services it offers, along with its mission and vision statements. This combination will illustrate what the business aims to achieve and how it positions itself in the market, providing a backdrop for aligning cyber security strategies with business goals.
- **Strategic Objectives and Regulatory Influences:** Detail the strategic objectives of the business, focusing on how these objectives are shaped by business needs and regulatory requirements. Explain how compliance obligations, industry-specific regulations and requirements/expectations from different stakeholders (e.g., customers, business partners) are integral to shaping the business's strategic planning and cybersecurity needs.
- **Organizational Resources**: Discuss the resources available to the business that may influence its cybersecurity strategy. This includes financial, personnel, and technological resources. Note any limitations or strengths that could impact cybersecurity planning and execution. General description of the threat landscape the business faces (consider the industry, region, size)
- **Threat Landscape**: Provide a general description of the threat landscape the business faces, considering factors such as the industry, region, and size of the business. Highlight specific threats that are more prevalent or damaging given the business's operational context.

Report Body: **Review of Current and Target Profile of Cyber Security Posture** (approximately 1600 words)

Current Profile:

- Summarize the business's existing cybersecurity postures across all six NIST functions (Govern, Identify, Protect, Detect, Respond, Recover). For each function, provide the rating given from the questionnaire and explain the rationale behind these scores.
- Describe how the business currently achieves or falls short in each function, detailing specific practices, technologies, and policies in place. You may summarize or directly quote from the questionnaire responses, citing these appropriately with footnotes.
- Highlight both strengths and weaknesses, providing a comprehensive view of the

cybersecurity landscape of the business.
- Additionally, discuss the underlying reasons why the firm is succeeding or failing in these areas, examining factors like resource allocation, employee training, and technology adoption.

Target Profile:
- Focus on three selected NIST functions, including Govern. This analysis should reflect the business's unique context, including its threat environment, regulatory requirements, and strategic business objectives.
- In developing the target profile, consider the organization's risk tolerance and anticipate changes to its cybersecurity posture that may arise from new business requirements (e.g., demands from current clients, prospective customers, and/or business partners), regulatory changes, adoption of new technologies, and evolving trends in cybersecurity threat intelligence. Define clear cybersecurity goals that are responsive to these dynamic factors, ensuring the proposed measures are robust yet adaptable to anticipated changes.
- This profile should articulate a vision for enhanced cybersecurity practices that align with both immediate needs and future challenges, emphasizing a proactive approach to security planning.

Report Body: Gap Analysis and Action Plan (approximately 1000 words)
- Identify and discuss the most significant gaps between the current and target profiles. Offer a holistic perspective on these gaps (i.e., evaluating how identified gaps are interconnected and might affect various aspects of the organization), considering potential risks and the impact of not addressing these issues.
- Develop a detailed action plan to bridge these gaps, including specific initiatives, technologies to be adopted, policy changes, or training programs. Refer to the NIST CSF 2.0 Informative References and Implementation Examples to gain deeper insights and practical examples that can guide your development of effective strategies.
- When proposing realistic timelines and budgets, include actual figures provided during interviews with the business or, if not available, base your estimates on a well-informed understanding of the business's resources, including leadership support, financial capacity, and talent/personnel availability.
- Define clear metrics for evaluating the effectiveness of the proposed improvements and ensure that the action plan is actionable within 18 months.

Conclusion (approximately 100 words)

Conclude the report, highlighting your main findings and immediate prioritised recommendations.

Reflection (approximately 150 words)

Reflect upon your review undertaken. Discuss any problems encountered during the review and lessons learned regarding conducting a cyber security resilience assessment.

Appendix A: Reference List
Referencing any documents or frameworks used during or applied in the report.

Appendix B: Questionnaire Results, Team Meeting Minutes

Appendix C: Provide a statement of the contribution made by each group member. This statement

should be agreed upon and considered by all respective group members.

Student Name	Student ID	Contribution (%)

Other Appendices may be attached as needed.

Submission Instructions

You must submit your assignment in the Assignment Dropbox in the unit CloudDeakin site on or before the due date (**8pm on 20th September 2024**). When uploading your assignment, name your document using the following syntax: <GroupNum_MIS761_Assignment2.doc (or '.docx'). For example, 'Group1_MIS761_Assignment2.doc'.

Submitting a hard copy of this assignment is not required. You must keep a backup copy of every assignment you submit until the marked assignment has been returned to you. In the unlikely event that one of your assignments is misplaced you will need to submit your backup copy.

Any work you submit may be checked by electronic or other means for the purposes of detecting collusion and/or plagiarism and for authenticating work.

When you submit an assignment through your CloudDeakin unit site, you will receive an email to your Deakin email address confirming that it has been submitted. You should check that you can see your assignment in the Submissions view of the Assignment Dropbox folder after upload and check for, and keep, the email receipt for the submission.

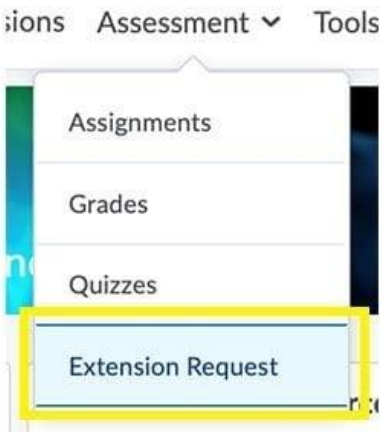
Marking and feedback

The marking rubric indicates the assessment criteria for this task. It is available in the CloudDeakin unit site in the Assessment folder, under Assessment Resources. Criteria act as a boundary around the task and help specify what assessors are looking for in your submission. The criteria are drawn from the ULOs and align with the GLOs. You should familiarise yourself with the assessment criteria before completing and submitting this task.

Students who submit their work by the due date will receive their marks and feedback on CloudDeakin 15 working days after the submission date.

Extensions

Extensions can only be granted for exceptional and/or unavoidable circumstances outside of your control. Requests for extensions must be made by 12 noon on the submission date using the online Extension Request form under the Assessment tab on the unit CloudDeakin site. All requests for extensions should be supported by appropriate evidence (e.g., a medical certificate in the case of ill health).



Applications for extensions after 12 noon on the submission date require University level special consideration and these applications must be must be submitted via StudentConnect in your DeakinSync site.

Late submission penalties

If you submit an assessment task after the due date without an approved extension or special consideration, 5% will be deducted from the available marks for each day after the due date up to seven days*. Work submitted more than seven days after the due date will not be marked and will receive 0% for the task. The Unit Chair may refuse to accept a late submission where it is unreasonable or impracticable to assess the task after the due date. *'Day' means calendar day for electronic submissions.

An example of how the calculation of the late penalty based on an assignment being due on a Thursday at 8:00pm is as follows:

- 1 day late: submitted after Friday 11:59pm and before Saturday 11:59pm– 5% penalty.
- 2 days late: submitted after Saturday 11:59pm and before Sunday 11:59pm – 10% penalty.
- 3 days late: submitted after Sunday 11:59pm and before Monday 11:59pm – 15% penalty.
- 4 days late: submitted after Monday 11:59pm and before Tuesday 11:59pm – 20% penalty.
- 5 days late: submitted after Tuesday 11:59pm and before Wednesday 11:59pm – 25% penalty.
- 6 days late: submitted after Wednesday 11:59pm and before Thursday 11:59pm – 30% penalty.
- 7 days late: submitted after Thursday 11:59pm and before Friday 11:59pm – 35% penalty.

The Dropbox closes the Friday after 11:59pm AEST/AEDT time.

Support

The Division of Student Life provides a range of **Study Support** resources and services, available throughout the academic year, including **Writing Mentor** and **Maths Mentor** online drop ins and the SmartThinking 24 hour writing feedback service at **this link**. If you would prefer some more in depth and tailored support, **make an appointment online with a Language and Learning Adviser**.

Referencing and Academic Integrity

Deakin takes academic integrity very seriously. It is important that you (and if a group task, your group) complete your own work in every assessment task Any material used in this assignment that is not your original work must be acknowledged as such and appropriately referenced. You can find information about referencing (and avoiding breaching academic integrity) and other study support resources at the following website: http://www.deakin.edu.au/students/study-support

Your rights and responsibilities as a student

As a student you have both rights and responsibilities. Please refer to the document ***Your rights and responsibilities as a student*** in the Unit Guide & Information section in the Content area in the CloudDeakin unit site.