



FIT5129 Assignment 1

Enterprise IT security - planning, operations and management

COPYRIGHT WARNING

Commonwealth of Australia Copyright Act 1968

Warning

This material has been reproduced and communicated to you by or on behalf of Monash University
in accordance with section 113P of the *Copyright Act 1968* (the *Act*).

The material in this communication may be subject to copyright under the Act. Any further
reproduction or communication of this material by you may be the subject of copyright protection
under the Act.

Do not remove this notice.

Assignment Objectives

AQF-9 Unit Learning Outcomes

Assessing this assignment translates to showing how well students are able to demonstrate the following basic cybersecurity capabilities (unit learning outcomes) at the Australian Quality Framework Level 9 or AQF-9.

Unit Learning Outcomes	Applied Contexts
<input checked="" type="checkbox"/> 1. Explain critical factors of enterprise security planning, operations and management;	To keep in line with practice developments, we are modernising the term “enterprise security planning, operations and management” to reference today’s rename of this domain as “cybersecurity”.
<input checked="" type="checkbox"/> 2. Perform risk analysis and assessment;	This Assignment will pick a main peer reviewed literature article that illustrates knowledge application of the critical factors of cybersecurity; the specifics of cyber risk detection, analysis and assessment, and response actioning; and the implications of cybersecurity policy making and deployment-strategy planning in today’s enterprises.
<input checked="" type="checkbox"/> 3. Provide practical security policies, strategies and implementation plan for enterprise systems.	Additionally, the Assignment will require each student to apply literature research, critical thinking and literacy techniques. The given assessment marks indicates the levels of a student’s scholarly and employability skills as an evidence based critical thinker and problem solver.

AQF-9 means that graduates can demonstrate they (via their unit grades):

1. Have acquired mastery in cybersecurity knowledge and scholarly and employability skills
2. Are able to apply these acquired capabilities in individual work in future research or workplace settings.

Understanding the Real-world Playout of the Unit’s Learning Outcomes:

The 2019 peer-reviewed article is titled “**Ethics of AI and Cybersecurity When Sovereignty is at Stake**”. It addresses complex ethical (hence governance) issues in executing cybersecurity operational work; as well as implications in cybersecurity policy and strategy planning, from both government and enterprise perspectives. These discussions inform you about the clear and present real-world perspectives of how the unit’s 3 learning outcomes are played out and implicated in the currently unresolved and growing ethical issues arising from 21st century cybersecurity’s risk management operations, policy and implementation-strategy management. Globally, every one of us are witnessing

the implications of these ethical challenges, posing as new wicked problems that potentially create [existential risks](#)¹.

Assignment Brief

Cybersecurity is [cyber risk management](#). As in any management work, one needs to appreciate the underpinning operational work involved in [detecting, analysing and responding](#) to cyber risks; and [planning and managing](#) the execution of such work. In senior management roles, one also needs to plan cybersecurity related [policies](#) and [implementation-strategies](#), as well as [governing compliance](#) to these policies and other corporate governance requirements. Additionally, there is a new need to collaborate with [others outside](#) the organisation, to ensure one's organisational cybersecurity plans and operations are aligned to those of [government agencies](#), in order to protect [homeland infrastructure systems and resources](#); and [citizens](#) against cyber hackers.



Work Instructions

1. Please [read](#) the given peer-reviewed article, "[Ethics of AI and Cybersecurity When Sovereignty is at Stake](#)" with a critical eye.
2. Apply the [critical reading techniques](#) (see Appendix 2) to [summarise the key points](#) of the whole paper. You can work with one or more students to discuss and clarify each other's understanding and use the discussions to outline the key highlights of the paper in one to two pages without integrating your own opinions or ideas. However, make sure the writing is

¹ If you do not have access to The Australian news article, refer to an extracted copy in the Appendix 1 of this brief.

originally yours. The aim here is to interpret the authors' information correctly and precisely in a summary.

3. Examine the following inquiry questions and determine which key points of your earlier reading-summary can help you frame each answer and what additional research topics you need to explore to give you more ideas, deeper insights or real-world case examples for detailing your answers.

- 1) Identify and discuss the ethical challenges in AI enabled cyber risk management that the author had raised. Discuss two additional and different ethical or other governance issues you can find in cybersecurity literature.
- 2) The author explained residual risks, from both financial and non-financial perspectives. Research another case study that is different from the one used by the author and use it to explain your own understanding of the residual risks of AI enabled cyber threats.
- 3) The author discusses three solution options for addressing the ethical challenges in cybersecurity: taking a national, preferably a government lead risk management approach; adopting a strategic partnership approach that involves regional commitment of business and government stakeholders from countries; and considering a global “common good” approach that depends on setting up an international governance body, such as the United Nations, in managing cyber risks. Summarise these 3 approaches in your own words and supported by a consolidating visual diagram of your explanations. For each of the approaches, you need to include at least 1 citation to strengthen the insights of each summary.
- 4) The author highlights that cybersecurity and ethics conflict because of the differences of nations' rights to sovereignty (in terms of countries wanting to assert their sovereign power and values on each other through cyber activities). This conflict affects the protection of human rights, nations' societal values and ways of life and sometimes territorial boundaries. Research 2 case studies and use them as illustrating examples to explain the non-financial costs of sovereignty conflicts prevailing in cyber activities among countries.
- 5) What additional insights can you abstract and conclude from your answers to the implied questions that underpin the above inquiry instructions?

4. Start researching to get more information and select the relevant ideas of other researchers and practitioners to detail your answers in convincing manners. Make sure you also include APA styled citations of researching findings used in your answers. At least 9 references (including the given article) is to be included.

5. Rewrite and restructure your answers to read logically and clearly. Some of you may take 2-3, or more iterations. If some ideas are too abstract to write clearly, use visual graphics and diagrams to communicate the complex ideas, supported by short descriptions of the visuals you created or copied for writing illustration. This is where you need to apply much more critical thinking and writing techniques to result in a writing structure that succinctly communicates the answers to all the questions and in a logically connecting and easy reading flow.

6. Proofread and when ready, submit into the Moodle assignment box.

No more than 6 pages, inclusive of all contents.

Good Turnitin scores should be in the vicinity of 1 to 10, average ones about between 11 and 20.

Recommended Report Structure (up to 6 pages)

Executive summary (½ up to 1 page)

Introduction (up to ½ page)

The Ethical Challenges of AI enabled Risk Management

Residual Risks of AI enabled Cyber Threats

Three Approaches for Addressing Ethical Challenges in Cybersecurity

Sovereignty Costs of Unethical Cyber Attacks

Summary of Discussions

Conclusion

APA Reference List

Marking Scheme Weightings

<u>Report Section</u>	<u>Weighting</u>
Executive summary (½ up to 1 page)	2.5%
Introduction (up to ½ page)	2.5%
The Ethical Challenges of AI enabled Risk Management	12.5%
Residual Risks of AI enabled Cyber Threats	12.5%

Three Approaches for Addressing Ethical Challenges in Cybersecurity	20%
Sovereignty Costs of Unethical Cyber Attacks	10%
Summary of Discussions	5%
Conclusion	5%
Referencing	5%
Language	10%
Turnitin Score	10%

Appendix 1: The Referred Australian's News Article

Copy of the Australian article that explains the existential risks of cyber-attacks ([The Australian 25 Feb 2020](#))

Existential threat of cybercrime

Renaud Deraison

12:00AM February 25, 2020

With another edition of the World Economic Forum (WEF) in Davos now concluded, global leaders have returned to their organisations with a fresh understanding of the macro existential threats that could impact their business or government.

As always, there's plenty of food for thought. While the WEF's annual Global Risks Perception Survey understandably highlighted environmental concerns and geopolitical risks as key priorities, cybersecurity was also high on the agenda.

From the recent ransomware attack on the local logistics sector to the hack last year that crippled a Melbourne heart clinic, organisations are starting to appreciate the danger posed by cyberthreats.

The WEF survey showed 76 per cent of respondents expected attacks against infrastructure to increase this year. In addition, 75 per cent of forum leaders expected cybertheft of money and data to increase in 2020, placing it as the eighth major risk to business on the list.

Concern about cyberattacks in 2020 now outranks the perceived risk from water crises, global government failures and asset bubbles in the World Economic Forum's lead report.

It's encouraging to see organisations being urged to approach cyber risk with the same degree of analysis and consideration they apply to other existential threats.

In case business leaders needed a reminder of the immediate and real-world threat of cyberattacks, the Global Risk Report was released days after the NSA alerted Microsoft to a vulnerability in its operating system which, if exploited, could've had serious consequences. The Australian government estimated cybersecurity incidents cost Australian businesses \$29bn in 2019.

As the world seeks continued economic growth and competitiveness, infrastructure from automated factories to smart motorways are becoming ever more interconnected and efficient. A serious cyberattack against critical infrastructure is not unrealistic in the digital world we operate in today.

Cyber-driven interference in Australia's power or water services would have obvious consequences for human life and the environment. We also need to consider how malicious tampering of systems in public and private organisations within the health, food and transport sectors could impact our everyday lives. Cybersecurity underpins today's digital economy and, without it, our very way of life is at risk.

Tackling cyberattacks requires collaboration between the public and private sectors.

New & improved business newsletter. Get the edge with AM and PM briefings, plus breaking news alerts in your inbox.

Thankfully, the federal government has been working in consultation with the private sector to refresh its national cyber security strategy, backed by \$230m, to protect the country's digital interests.

To help organisations proactively reduce their cyber exposure, the Australian Signals Directorate has published the "Essential Eight" a prioritised list of initiatives to enhance computer security. It includes mitigation strategies such as using the latest operating systems and patching vulnerabilities when possible. It should be an essential read for business leaders everywhere.

Renaud Deraison is co-founder and CTO of cybersecurity company Tenable.

Appendix 2 – Research, Critical Literacy & Thinking Techniques

RESEARCH

Use APA standard to cite and list your references - <https://guides.lib.monash.edu/citing-referencing/apa>. Whichever proprietary version you use (e.g. Monash APA, Microsoft APA Reference Style, One Note, etc), make sure you follow the chosen proprietary version's citation and reference-listing formats.

Some tips on where to focus your literature research:

Apply the [CRAP analysis](#) on the 4 given articles. Using information from the article/s with the lowest score should be supported with more additional references.

When you search for other articles, also apply this test to find high quality references and avoid uncredible ones.

Currency
<ul style="list-style-type: none">• How recent is the information?• How recently has the website been updated?• Is it current enough for your topic?
Reliability
<ul style="list-style-type: none">• What kind of information is included in the resource?• Is content of the resource primarily opinion? Is it balanced?• Does the creator provide references or sources for data or quotations?
Authority
<ul style="list-style-type: none">• Who is the creator or author?• What are the credentials? Can you find any information about the author's background?• Who is the published or sponsor?• Are they reputable?• What is the publisher's interest (if any) in this information?• Are there advertisements on the website? If so, are they clearly marked?
Purpose/Point of View
<ul style="list-style-type: none">• Is this fact or opinion? Does the author list sources or cite references?• Is it biased? Does the author seem to be trying to push an agenda or particular side?• Is the creator/author trying to sell you something? If so, is it clearly stated?

READING

1. How do you read effectively ?

- a. Monash's list of effective reading techniques - <https://www.monash.edu/rlo/study-skills/reading-and-note-taking/effective-reading-strategies>
- b. https://flexiblelearning.auckland.ac.nz/reading-effectively/13_2.html

2. How do you read critically?

<https://www.monash.edu/rlo/study-skills/reading-and-note-taking/developing-your-critical-reading-skills>

3. How do you read difficult papers?

<https://www.monash.edu/rlo/study-skills/reading-and-note-taking/reading-difficult-material>

WRITING

How to write for assignments?

<https://www.monash.edu/rlo/research-writing-assignments/writing>

How to write Body Paragraphs?

<https://www.monash.edu/rlo/research-writing-assignments/assignment-types/writing-an-essay/writing-body-paragraphs>

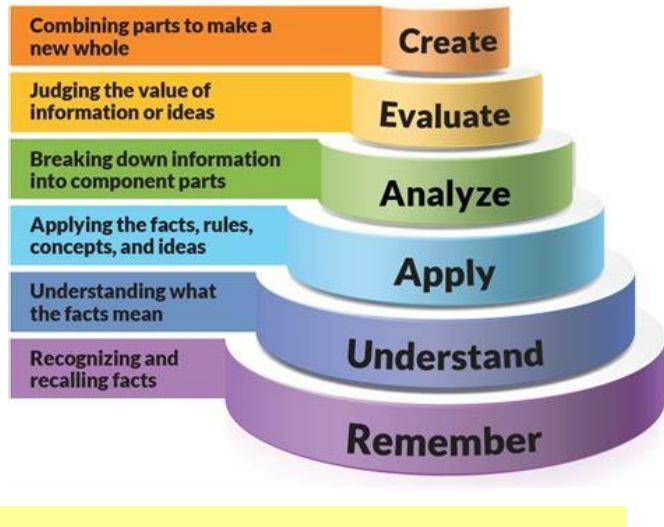
How to write an essay? (these essay writing techniques can still apply to report writing)

<https://www.monash.edu/rlo/research-writing-assignments/assignment-types/writing-an-essay>

CRITICAL THINKING TECHNIQUES

Using [Bloom's Taxonomy](#) framework, there are 6 techniques of critical thinking:

1. You **remember** what you are reading or have read.
2. You **understand** what you read.
3. You **analyse** what you read, ie break into parts the key ideas or concepts or claims that make up your answers to the 3 inquiry Qs.
4. You research and **evaluate** the parts. ie decide how relevant are they to answer the 3 inquiry Qs.
5. You **apply** the parts and research evidence to synthesis your answers.



Color Legend: Showing where literacy techniques integrate with critical thinking processes.

	Apply reading techniques
	Use notes taking and visualisation techniques
	Apply writing and proof-reading techniques