Faculty of Information Technology

Semester 2, 2020

FIT5057 – Project Management

Assignment 1: Individual Critical Literature Review (20%)

Due Date: 1st September

Developed by Asha Padisetti & Chan Cheah, 2020
Technical Contributions: Kim Ko

1.0 Learning Objectives

This is an individual assignment report involving the review of cyber security and project management literature and aims to coach students develop research, critical reading, thinking, and writing skills; these skills are collectively regarded as employability skills and they are intended to help achieve the following Unit Learning Outcomes and meet AQF-9's criteria for critical skills development.

Unit Learning Outcomes	Applicable?	Explanation
1. Analyse and evaluate the role of the modern project manager in the context of IT projects	X	Modern project managers are required to research and apply critical thinking skills to solve their problem problems. Additionally, they are eloquent in communicate their thoughts and use problem-solving logic in their project reports
2. Interpret and critique a variety of project management methodologies offered by various professional bodies including that provided by the Project Management Body of Knowledge (PMBOK)	X	Here project managers are required to understand a breath of knowledge areas and need to be aware of the inherent organisational risks when dealing with software projects and need to be able to integrate a number of knowledge areas such as scope, procurement and risk when in the design phase of the software.
3. Describe and apply the available strategies, techniques and decision tools used by project managers to manage modern IT projects based on PMBOK methodology.	X	Here the main skill that is emphasised are critical reading, thinking and writing skills which project managers require to move from the problem phase to the solution phase.

Table 1: Project Management Unit Learning Outcomes

2.0 Instructions

For this literature review, you are to use the peer reviewed articles provided (see section 3 – Key references) as your main source to critically analyse and evaluate the topic. You MUST also use at least five other additional references (such as a peer-review conference paper, peer-reviewed journal article or textbook) in your writing as a source of evidence for the ideas, arguments, problems and issues raised in your essay.

We have provided you with a list of guiding questions however you are required to write the literature review as one essay.

The completed literature review, including references needs to be at least 12 pages.

Topic: Critically discuss how the digitalisation of supply chains affects the way in which project managers manage cyber security risks when working with large multi-national organisations.

(i) ~~Define cyber supply chains~~ and ~~discuss four types of cyber risks that it brings to organisations. Validate your definition claims with evidence of other research findings and/or appropriate evidence-based case examples.~~

(ii) ~~Discuss how Ghadge et al. 2019, concluded the above common types of cyber supply chain risks.~~

(iii) ~~Given Covid-19 pandemic and geopolitical events, vendor risk management has become important and organisations can be significantly exposed to vendors and their related cyber supply chains. How can organisations address this risk?~~

(iv) ~~Discuss Presley & Landry's, (2016) framework for managing cyber supply chain risk and how the framework relates and impacts the PMBOK (2017) knowledge areas. Present this information in the form of a table~~

(v) ~~Compare and contrast the approach taken by the Australian Cyber Security Centre, (2020) and Presley & Landry's, (2016) in presenting cyber supply chain risk in terms of relevance, efficiency, effectiveness, impact and sustainability.~~

3.0 Key References

Australian Cyber Security Centre (ACSC), (2020). Cyber Supply Chain Risk Management Practitioner Guide. Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management-practitioner-guide

Ghadge, A., Weib, M., Caldwell, N., & Wilding, R., (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management*. p. 1-36. DOI: 10.1108/SCM-10-2018-0357. Retrieved from: https://www.researchgate.net/publication/334736415_Managing_cyber_risk_in_supply_chains_A_review_and_research_agenda

Presley, S.S., Landry, J.P., (2016). A Process Framework for Managing Cybersecurity Risks in Projects: *Proceedings of the Southern Association for Information Systems Conference, St. Augustine, FL, USA March 18th–19th.* Retrieved from: https://pdfs.semanticscholar.org/0d48/72e2e35cbb4f641807385342be7105f35aea.pdf

4.0 Literature Review Template

Literature review template
Cover Page
Abstract
Introduction (State the purpose of report and scope of key discussions)
Body
Cyber Supply Chain Management (CSCM)
Definition
Cyber supply chain risks that affect organisations
An Approach to Vendors Risk Management in CSCM
Importance of Vendors Risk Management in CSCM
Ghadge et al., (2019) Vendors Risk Management Methodology
Framework for managing cyber supply chain risk
Impact of Presley & Landry's, (2016) CSCM risk management framework on PMBOK (2017)
Comparative approaches in presenting cyber supply chain risk management (Australian Cyber Security Centre, (2020) vs Presley & Landry's, (2016))
Conclusion
Reference list
Appendix

5.0 Assessment Criteria

The detailed assessment criteria will be published in Moodle. The high-level mark allocation is presented below:

Literature review - Assessment Rubric	Weightage (%)
Abstract	**5**
Introduction (State the purpose of report and scope of key discussions)	**5**
Cyber Supply Chain Management (CSCM)	
Definition	**5**
Cyber supply chain risks that affect organisations	**5**
An Approach to Vendors Risk Management in CSCM	**10**
Importance of Vendors Risk Management in CSCM	**10**
Ghadge et al., (2019) Vendors Risk Management Methodology	**10**
Framework for managing cyber supply chain risk	**10**
Impact of Presley & Landry's, (2016) CSCM risk management framework on PMBOK (2017)	**10**
Comparative approaches in presenting cyber supply chain risk management (Australian Cyber Security Centre, (2020) vs Presley & Landry's, (2016))	**10**
Conclusion	**5**
Reference quality	**5**
Language / Syntax / Semantics	**10**
Total	**100**