Reflective Learning

Table of Contents

1.0. Introduction

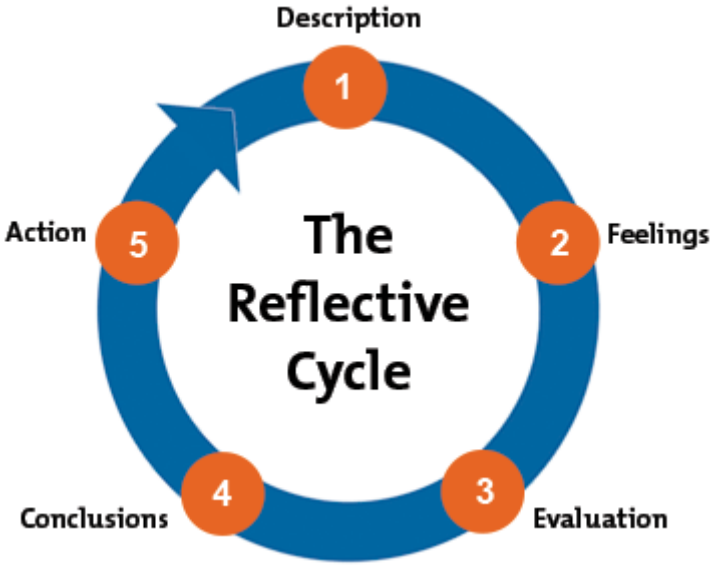
The purpose of this assignment is to present a reflective learning evaluation. In project management, reflective evaluation is key as it contributes to best practice identification. It also helps the individual or the team identify key success areas and challenges which need to be addressed (Divine and Zachry, 2018). Reflective learning also helps revisit project management practices and identifying areas of improvement. It helps the project manager, or the project team-member develop better skills through targeted action plans to improve their own competencies (Turner, 2018). The primary learning outcome of this research is to assess the need for reflective thinking in project management and to engage in a process of continuous learning which can incrementally improve one's skills. This assignment intends to focus on two tasks. The first task is a reflective comparison of the individual and group work to identify key success and challenges as well as identify key learning inputs. The second task involves evaluating assignment 2's project management framework to assess underlying cybersecurity issues.

2.0. Reflective Thinking Model

This report intends to use the reflective learning cycle of Gibbs. The Gibbs reflective cycle is as simple six-stage process which can help one reflect on experiences within the workplace. It helps an individual evaluate what occurred, what were the positive or negative experiences, identify areas of improvement and arrive at key action plans to achieve future growth. The following Figure 1 highlights the reflective learning cycle (Gibbs, 1988). The model is circular in nature and therefore calls for continued learning from experience over time.

The first stage or the description stage sets the context of the event, its experiences and the stakeholders involved. It helps in identifying the role of an individual within a team. The second stage is the feelings stage. This stage helps identify one's feelings during a learning experience (Sekarwinahyu et al., 2019). It helps determine what one felt and what one feels about it now. The third stage is the evaluation step. At this step, the experiences are evaluated to determine the good and bad aspects which contribute to learning. The fourth stage is the analysis stage. At this stage, the goal is to assess what went wrong and what can be done to overcome underlying challenges. The analysis stage builds on the evaluation stage to determine key areas of improvement from other best practice evidences and one's role in improving their own actions in future similar events (Tanaka et al., 2018). The final conclusion and action plan stage helps develop insight into own and other people behaviour and identify key targets for future growth (Gibbs, 1988).

Figure 1: Reflective Learning Cycle



Source: Gibbs (1988)

3.0. Task 1: Reflective Thinking Outcomes

3.1. Introduction

This task will make use of the Gibbs reflective learning cycle to evaluate individual and group work learnings as well as arrive at key implications for future learning.

3.2. Reflection Discussion

What did we do? This section helps identify the first stage of the Gibbs reflective learning model. It identifies the series of events that took place. In Assignment I i conducted an in-depth evaluation of cyber supply chain, their underlying risks, the role of project managers as well as different ways to mitigate the cyber supply chain risks. A total of fourteen sources including books, standards, peer reviewed journal articles and online articles were used to conduct this comprehensive review of literature. In Assignment 2, we intended to develop a project plan for a new addition to the Covid-19 health surveillance and research network. The proposed MOCAS system was developed by the Monash university in conjunction with the Australian government to expand the original CovidSafe application and provide additional data for research or statistical purposes for different branches of the government and other sectors. The report provides a comprehensive project management plan where the goal was to identify the case, the project team, the objectives, the key resource management needs, scope management, schedule management and other important PMBOK knowledge areas.

Practical solutions regarding the implementation of project management principles within the context of a specific project was arrived at.

The approach to completing Assignment 1 differed from that of Assignment 2. This is because, Assignment 2 was a detailed group task where we had to work together to develop a comprehensive framework. Assignment 2 took longer time and required greater collaboration. In assignment 1, my primary learning needs included becoming aware of the concept of cybersupply chain and its risks and attempting to conduct a critical review of available empirical literature. This required focusing on synthesising academic learning and translating this knowledge to arrive at key research outcomes. In contrast, in Assignment 2, the goal was to arrive at a practical project management plan. Though references were made to academic content, the focus was on developing project management knowledge, processes and lifecycle needs.

The three key learning areas which encompass both these assignments include the following. My first learning area was to learn how to translate theoretical knowledge into practical implementation. Therefore, I was able to analyse and evaluate the role of project manager in the context of a specific project. The importance of identifying a relevant project management area was reflected in both assignments. The choice of cybersecurity in supply chains as well as MOCAS, a system which provides Covid-19 support is most relevant to modern security management. My second learning area which is relevant to both assignments is critical analysis. In particular, I believe that I was able to critique knowledge areas and methodologies offered by bodies like PMBOK. For example, In assignment 1, I conducted a systematic search of relevant research literature, compared and contrasted empirical findings and was able to present a conclusion. In assignment 2, I was able to improve my inherent ability to critically apply knowledges gained from prior textbooks and classroom sessions in the context of a single project. The third learning outcome was to apply available strategies in a project. Through Assignment 2, I was able to identify project goals, constraints, deliverables, planning scope, financial assessment, risks and other factors in the context of a single project.

Reflect on your experience in completing Assignment 1 and 2 and answer the following reflective questions?

What worked well and what did not and why?

This analysis reflects the second and third stage of the Gibbs cycle: feeling and evaluation. In completing Assignment 1, I felt overwhelmed with available literature. Though the topic selected was new, I felt that I was overburdened with available literature. This made me feel panicked. I feel that I did not manage my time and selection of articles. On the other hand, I

felt that what worked well was the structure of my critical review and the use of signposting and bullet points which helped me arrive at comprehensive outcomes.

In Assignment 2, what worked well was our team meetings despite the Covid-19 challenge, ability to divide tasks and complete them. I felt proud that as part of a team were able to develop a comprehensive end product. What did not work well was our ability to manage responsibilities. Though we decided on who completed which section of the report, there were some challenges and difficulties in meeting set milestones.

What effect did I have and what I learnt from this situation?

This question helps answer the fourth stage of the Gibbs reflective learning cycle, i.e., the analysis stage. Overall, I feel that across both the first and second assignment being overwhelmed by the nature of task, I have had difficulties in meeting milestones and ensuring that the end product is provided ahead of time. I should use project management tools and techniques to my completion of project. For example, as Tereso et al., (2019) argue, it is important to develop time schedules and Gantt charts to help manage responsibilities. We made the mistake of each individual completing independent sections. For example, while I worked on sections 3.2 and 3.5 there were overlaps with other sections. Lindsjorn et al., (2016) contend that successful projects require support and engagement in the form of team interdependence. We should have had 2 people working together on specific sections so that we would have had the support to achieve end goals and outcomes. I have learnt that I can find it difficult to manage time pressure. As Rzempała and Wisniewski (2020), identified, graduate competencies which can help in future career growth is the use of available tools to plan one's activities. I feel that better planning, communication and time management is required.

3.3. Conclusion and Reflective Evaluation

What are my key learning areas, personal and professional?

This question helps answer the fifth stage of Gibbs learning cycle, i.e., the conclusion stage. Overall, I believe that my learning areas will include three important outcomes. Firstly, I intended to increase my ability to translate knowledge into practice. I found the Assignment 2 task a good step in this direction. However, more work is required to achieve this. Secondly, I want to develop better critical thinking and problem-solving skills. Thirdly, I would like to improve my communication and engagement competencies as a team player. Professional learning areas include better awareness of applying PMBOK knowledge areas into practice, increasing my knowledge of specific scope management, workflow and financial management tools.

What is my personal development action plan?

The following table summarises my action plan for personal development.

Table 1: Improvement Action Plan

	Personal development goals	Steps	Timeline
Short term	Improve knowledge of PMBOK methodology and other project management methodologies	Learn through books, online articles and videos	3 months
Short term	Improve critical thinking and problem-solving capabilities	Apply knowledge gained into practice. Use case studies and questions to evaluate the relevance of knowledge gained.	3 months
Long term	Become project manager for healthcare surveillance project	Increase domain specific knowledge on health care technology needs and project management	5 years
Medium term	Improve team communication and interdependence	Gain leadership and teamwork skills	1 year

4.0. Task 2

4.1. Introduction

The purpose of this task is to evaluate the efficacy of cybersecurity planning within the MOCAS framework and identify key weakness areas. The task also determines the right stakeholder model, stakeholder impacts and learning outcomes.

4.2. Reflection of Framework

The system referred to as the MOCAS was intended to download data from the current CovidSafe warehouse provided by the Federal government and then create a new database containing only covid19 positive test data. This data was then used by relevant departments to conduct analysis and generate trend and location reports. The proposed MOCAS system considered underlying cybersecurity risks and attempted to ensure that security norms were adhered to. The implementation of the MOCAS plan acknowledges underlying cybersecurity risks including information security, legal challenges linked to any cybersecurity threat. It is

expected that an external information security organisation will be hired to address three primary cybersecurity threats. In particular, the key areas of focus with respect to cybersecurity included focus on three elements. Firstly, the security of transmission of information. The security of the transmission was evaluated by expert review. The security system that was selected for the MOCAS system was evaluated based on number of consumers who continue to remain with the security network (i.e., through the churn rate). Additionally, security concerns also target a cyber security system which ensures encryption of user data where the data is converted to an unreadable format and made available only to those who are given access. Finally, security is required at point of upload where privacy concerns regarding the health information of individual users is to be considered.

There are some weaknesses with this approach. This research section intends to evaluate these underlying weaknesses. Prior research has highlighted the vulnerability of public health to cybersecurity threats (Harries and Yellowless, 2013). The rise in funding for health information technology may have come at a cost with more investment in the technology rather than focus on cybersecurity. The healthcare sector could become the future tantalizing opportunity for cyber terrorism.

The choice of info security company being based on simple churn metrics highlights important cybersecurity challenges. It is important that technological challenges are identified. For example, one of the biggest challenges to software platforms like MOCAS is the growing presence of malware. According to Dewar (2014), malware presence within disease surveillance systems can lead to major privacy issues (e.g. misuse of information to stigmatise and discriminate against groups) as well as improper use of data by institutions who have not been approved. Therefore, the ability of the healthcare surveillance and monitoring system to overcome underlying challenges linked to malware identification is important. In particular, there is evidence of ransomware attacks which prevent or restrict users from accessing the system. There is a clear security weakness in the current system as it does not consider underlying challenges of ransomware or malware impact.

Pope (2016) argue that the best approach to overcome issues of ransomware is to educate employees or stakeholders who use the system. Since the MOCAS system is intended to be used by employees across different departments, it becomes essential that education is provided to all users of the system. Apart from this, there should be opportunities to remove systems who are affected immediately. There should also be constant updates of system security by requiring all members to change passwords every month to help uphold the fidelity of the system.

The second weakness identified with the MOCAS system is the lack of security audits. Though the cyber security manager is supposed to manage security compliance, there can be passive attacks which go unnoticed. It is important that as McLean (2013) argues, a thorough audit is conducted to assess physical and software systems.

The third weakness is lack of implementation of controlled system access. The current system is such that data is retrieved from a national database and different users have access to it. It is essential that access is controlled at different levels. This will ensure that there is fidelity within the system and there is controlled access to data. Additionally, improving the degree of control over access it is possible to enhance perimeter defences (Vacca, 2013). The use of firewalls and can be more effective if there is restricted access and limited points through which software-initiated hacks are contained. This can help in overcome inherent security problems including denial of service attacks, phishing and advanced persistent threats.

The fourth weakness that is identified is the potential presence of cloud threats. The use of a data warehouse makes it vulnerable to this security threat. Though the degree of encryption provided by the infosec company is evaluated there can be potential cloud threats where there is hacking of the cloud and loss of data (Jeremiah et al., 2018). According to Bodeau and Graubart (2016), it is important to develop an intrusion detection system which shields the network by gathering information from a spread of framework and network supply. Similarly, the cybersecurity manager should also work with the Infosec company to develop better security patches.

4.3. Proposed Policy

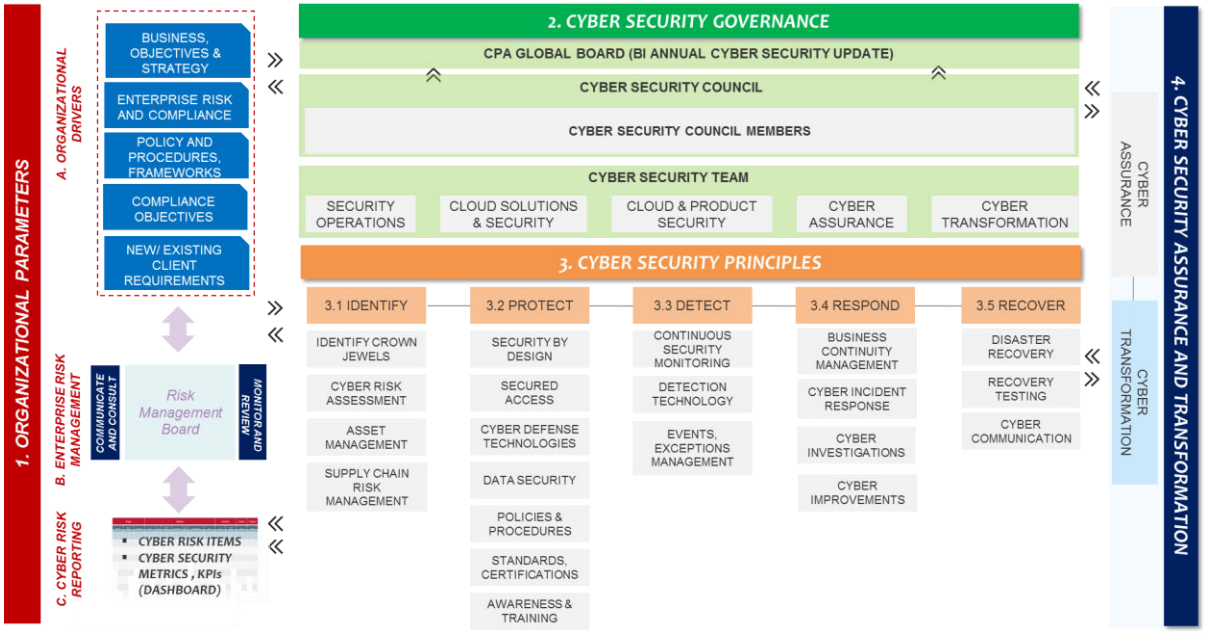
The recent changes implemented in Australian law with respect to cybersecurity requires firms to give notification of authorities where there is breach and holds the organisation responsible to act swiftly. similarly, it is also expected that cybersecurity needs to be developed as a governance mechanism. Therefore, the following governance framework is recommended.

There is a need for governance framework which supports strategic integration (i.e., the integration of cyber security strategy with other organisational strategies), disciplines (i.e., the departments who will be aligned with working with cybersecurity), risk mitigation and evaluation (compliance with standards and constant evaluation) and the nature of decision making (i.e., identifying these responsible for making relevant decisions) (CPA Global, 2016).

As seen in the following figure, the MOCAS application global board will oversee the cybersecurity requirements. There is a cybersecurity council which will need to be implemented including MOCAS cybersecurity managers, MOCAS top management as well as federal government cybersecurity representative. Additionally, there should be clear

guidelines on what the internal cybersecurity team will achieve. For example, it is expected that the cybersecurity team will focus on security and operations, evaluation of risks, cyber transformation as well as product security.

Figure 2: Proposed Cybersecurity Governance Model



Source: Adapted from CPA Global (2018)

Von Solms and Von Solms (2018) argue that successful cybersecurity governance will take into account important cybersecurity principles. This will include identification, protection, detection, response, recovery and resilience. Some of these actions are highlighted in the following figure. Ellis and Mohan (2019) argue that the presence of security governance will need to have a clear charter or mandate for the security programmes, coordinate with other members within and across the network of organisations as well as develop and manage security policy. Therefore, there will be a clear mandate set for the cyber security council including budgeting and resourcing, policy development and control of risks.

Additionally, the following are the list of policy documents that need to be developed as part of the governance model is highlighted below.

- Information security policy
- Incident management plan
- Disaster recovery plans
- Risk management and risk identification plans
- Budgeting for cybersecurity

- Talent identification and resource management plan
- Account and password management plan
- Confidentiality of sensitive data plan
- Security awareness and education plan
- Compliance and audit plan

These documents are developed and distributed to different stakeholder groups as identified in the following table.

Table 2: Documents Needed

List of Documents	Developer of document	Target stakeholder
Information security policy	Cybersecurity council	Entire network which uses the MOCAS system
Incident management plan	Cybersecurity team	Top management, board, cyber security council
Disaster recovery plans	Board of directors	Cybersecurity team, top management
Risk management and risk identification plans	Cybersecurity team	Top management, board, cyber security council
Budgeting for cybersecurity	Cybersecurity team, Finance department	Cybersecurity managers, top management
Talent identification and resource management plan	Cybersecurity team, HR	Cybersecurity team, top management
Account and password management plan	Cybersecurity team, Finance department	Cybersecurity managers, top management
Confidentiality of sensitive data plan	Cybersecurity team, Finance department	Cybersecurity managers, top management
Security awareness and education plan	Cybersecurity team	Top management, board, cyber security council
Compliance and audit plan	Cybersecurity team	Top management, board, cyber security council

4.4. Reflective Evaluation

As observed in Task 1, one of the key challenges and learning gaps that I faced was difficulties in translating knowledge into practice. For example, I need to develop skills on security information management systems, become aware of guidelines of regulations like ISO 27001 and COBIT, improve my security audit skills, learn more about the importance of data analytics and intelligence in cyber security, leverage firewall to filer network traffic. At the moment, while I have theoretical knowledge on these elements this knowledge is limited. Therefore, it becomes imperative that I am able to develop better competencies which help me apply my knowledge of cybersecurity to achieve the right skills.

4.5. Conclusion

The purpose of Task 1 was to conduct an independent assessment of my own work and engagement with my group in assignments 1 and 2. I feel that I was able to pinpoint important challenges and positive outcomes which can help expand to other modules of my learning within this programme. The purpose of the second task was to evaluate the effectiveness of cybersecurity as part of the model proposed in Assignment 2. An evaluation of cybersecurity weakness shows that there is important phishing, denial of service, hacking as well as limited control access issues. The development of an effective cybersecurity governance model can help overcome these challenges.

5.0. References

Bodeau, D. and Graubart, R. (2016). *Cyber prep 2.0: Motivating Organizational Cyber Strategies in Terms of Threat Preparedness*. [Online] Available at: https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-motivating-organizational-cyber-strategies.pdf (Accessed on 25th Oct, 2020).

CPA Global (2016). *Cyber Security Framework*. [Online] Available at: https://www.cpaglobal.com/cyber-security-framework (Accessed on 25th Oct, 2020).

Dewar, R. (2014). *The Triptych of Cyber Security: A Classification of Active Cyber Defense*. 6th International Conference on Cyber Security.

Divine, D. and Zachry, M. (2018). Project management, contradictions, and textualized activity: Supporting reflection in project-based organizations. *Technical Communication*, 65(2), pp.194-209.

Ellis, R. and Mohan, V. (2019). *Rewired: Cybersecurity Governance*. John Wiley & Sons.

Gibbs, G. (1988). *Learning by doing: A guide to teaching and learning methods*. Oxford: Oxford Further Education Unit.

Harries, D. and Yellowlees, P. M. (2013). Cyberterrorism: Is the US healthcare system safe?. *Telemedicine and e-Health*, 19(1), pp.61-66.

Jeremiah, P., Samy, G. N., Shanmugam, B., Ponkoodalingam, K. and Perumal, S. (2018). Potential Measures to Enhance Information Security Compliance in the Healthcare Internet of Things. In *International Conference of Reliable Information and Communication Technology*. Springer, Cham, pp. 726-735.

Lindsjorn, Y., Sjoberg, D. I., Dingsoyr, T., Bergersen, G. R. and Dyba, T. (2016). Teamwork quality and project success in software development: A survey of agile development teams. *Journal of Systems and Software*, 122(1), pp.274-286.

McLean, S. (2013). Beware the Botnets: Cyber Security is a Board Level Issue. *Intellectual Property & Technology Law Journal*, 25(12), pp. 22-27.

Pope, J. (2016). Ransomware: minimizing the risks. *Innovations in Clinical Neuroscience*, 13(11-12), pp.37-40.

Rzempała, J. and Wiśniewski, T. (2020). The Level of Competence of Post-graduate Students in Project Management. Case Study of IPMA Student. *Zeszyty Naukowe. Organizacja i Zarządzanie/ Politechnika Sląska*, 144(1), pp.429-438.

Sekarwinahyu, M., Rustaman, N. Y., Widodo, A. and Riandi, R. (2019, February). Development of problem-based learning for online tutorial program in plant development using Gibbs' reflective cycle and e-portfolio to enhance reflective thinking skills. In *Journal of Physics: Conference Series*. IOP Publishing, 1157(2), pp. 22-99.

Tanaka, M., Okamoto, R. and Koide, K. (2018). Relationship between Reflective Practice Skills and Volume of Writing in a Reflective Journal. *Health*, 10(3), pp.283-288.

Tereso, A., Ribeiro, P., Fernandes, G., Loureiro, I. and Ferreira, M. (2019). Project management practices in private organizations. *Project Management Journal*, 50(1), pp.6-22.

Turner, J. R. (2018). The management of the project-based organization: A personal reflection. *International Journal of Project Management*, 36(1), pp.231-240.

Vacca, J.R. (2013). *Cyber Security and IT Infrastructure Protection*. Waltham: Steven Elliot.

Von Solms, B. and Von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security*, 26(1), pp. 2-9.