Unit 4 Software Development – 2024 Outcome 2 Cybersecurity: software security – Template for developing an assessment task – Plan			
Outcome 2 On completion of this unit the student should be able to respond to a teacher-provided case study to examine the current software development security strategies of an organisation, identify the risks and the consequences of ineffective strategies and recommend a risk management plan to improve current security practices.			**Assessment task development – Planning for the case study** Create a fictitious organisation that is a real-world example with a reasonable level of complexity. Media articles can assist with this. A case study for this task needs to involve an organisation that develops software and has some security strategies in place that can be analysed and discussed. The information system must not be a manual system and must be an existing system, not proposed. Have issues in what the organisation is doing. Write the case study for the organisation. Key content within the case study should be based on the targeted key knowledge and key skills.
Key knowledge	**Key skills**	**VCAA Performance descriptors (Very high)**	
• reasons why individuals and organisations develop software, including meeting the goals and objectives of the organisation • physical and software security controls used to protect software development practices and to protect software and data, including version control, user authentication, encryption and software updates • software auditing and testing strategies to identify and minimise potential risks	• analyse and discuss the current security controls to protect software development practices and to protect software and data	• Comprehensive analysis and discussion of the current security controls used to protect software development practices and to protect software and data.	Content to be included in the case study should introduce students to the background of the organisation. This could include the setting of the organisation, what they do in terms of software development and their goals and objectives. Details regarding the physical and software security controls used to protect their software development practices and how they protect their software and data including any software auditing and testing strategies to minimise risks should be included. Issues should be included within the case study for students to pick up on and write about in their analysis and discussion. These could include a lack of security controls and strategies.
• types of software security and data security vulnerabilities, including data breaches, man-in-the-middle attacks and social engineering, and the strategies to protect against these • types of web application risks, including cross-site scripting and SQL injections • managing risks posed by software acquired from third parties • characteristics of data that has integrity, including accuracy, authenticity, correctness, reasonableness, relevance and timeliness • the impact of ineffective security strategies on data integrity	• identify and discuss the potential risks to software and data security with the current security strategies	• Comprehensive identification and discussion of the potential risks to software and data security.	Content should be included in the case study to enable students to identify and discuss the potential risks to software and data security. Students will need to consider the types of vulnerabilities in the key knowledge for this outcome: data breaches, lack of version control, poor user authentication practices, irregular software updates, man-in-the-middle attacks, social engineering, or lack of encryption, the types of web application risks and managing risks with software acquired from third parties. While there is no requirement for teachers to include all of these vulnerabilities within the case study, there should be some reference to the types of vulnerabilities selected by the teacher. Data integrity is also affected by vulnerabilities and risks and these need to be identified within the case study to determine the impact on the organisation.
• criteria for evaluating the effectiveness of software development security strategies	• propose and apply criteria to evaluate the effectiveness of the current security practices	• Comprehensive set of relevant evaluation criteria to measure the effectiveness of the current security practices are proposed and applied.	The content above should enable students to evaluate the effectiveness of the organisation's current security practices by considering how vulnerabilities may pose a security risk to their development practices, and how they reduce the effectiveness of their development practices. The case study could include strategies that they follow. The organisation should have some weaknesses in these practices and strategies. This will enable students to propose and apply evaluation criteria to measure the effectiveness of the current security practices.
• key legislation that affects how organisations control the collection, storage (including cloud storage) and communication of data: the *Copyright Act 1968*, the *Health Records Act 2001*, the *Privacy Act 1988* and the *Privacy and Data Protection Act 2014* • ethical issues arising during the software development process and the use of a software solution	• identify and discuss the possible legal and ethical consequences to an organisation for ineffective security practices	• Comprehensive understanding of the possible legal and ethical consequences of ineffective security practices.	Content should be included in the case study for students to be able to clearly identify the relevant legislation impacting the organisation. This could be the Copyright Act 1968, the Privacy Act 1988, the Health Records Act 2001 or the Privacy and Data Protection Act 2014. Therefore, students could be given information on the type of organisation, the amount the organisation earns each year, the location of the organisation, whether it is a government or private organisation, and how the ineffective security practices may be impacted by the relevant legislation. Details describing how the organisation controls the collection, storage and communication of their data should be included. Students should be able to clearly identify some legal and ethical issues involving the software development process and the use of the software solution.
• risk management strategies to minimise security vulnerabilities to software development practices.	• recommend and justify an effective risk management plan to improve current security practices	• Comprehensive recommendations are made and justified to improve the current security practices as part of an effective risk management plan.	The content above should enable students to make recommendations and to justify improvements to the organisation's security practices through an effective risk management plan.