Unit 4 Software Development – 2024

Outcome 2 Cybersecurity: software security – Template for developing an assessment task – Blank

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**
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.	
• 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.	
• 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.	
• 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.	
• 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.	