Unit 4 Data Analytics – 2024

Outcome 2 Cybersecurity: data and information security – Developing a marking scheme – Sample

Outcome 2

On completion of this unit the student should be able to respond to a teacher-provided case study to investigate the current data and information security strategies of an organisation, examine the threats to the security of data and information, and recommend strategies to improve current practices.

Developing a marking scheme – Marks allocated – 100

Refer to the key skills or the VCAA performance descriptors when developing a marking scheme for the case study. Determine the weighting of the marks out of 100 for each key skill or performance descriptor. When determining weightings for responses consider the time that students will take to complete each component as well as the level of difficulty of each component. Marks should be allocated to ensure students can demonstrate a range of levels of performance in their responses.

Key knowledge	Key skills	VCAA Performance descriptors (Very high)	
• characteristics of wired, wireless and mobile networks • physical and software security controls for preventing unauthorised access to data and information and for minimising the loss of data accessed by authorised and unauthorised users • the role of hardware, software and technical protocols in managing, controlling and securing data in information systems • the advantages and disadvantages of using network attached storage and cloud computing for storing, communicating and disposing of data and information • the importance of data and information to organisations • the importance of data and information security strategies to organisations	• analyse and discuss the current data and information security strategies used by an organisation	• Comprehensive analysis and discussion of the current data and information security strategies used by an organisation.	Students are to analyse and discuss the current data and information security strategies used by the organisation. Possible number of marks – 40 marks
• types and causes of accidental, deliberate and events-based threats to the integrity and security of data and information used by organisations • characteristics of data that has integrity, including accuracy, authenticity, correctness, reasonableness, relevance and timeliness • the impact of diminished data integrity in information systems	• identify and evaluate threats to the security of data and information	• Comprehensive identification and evaluation of the threats to the security of data and information.	Students are to identify and evaluate the threats to the security of the organisation's data and information. Possible number of marks – 20 marks
• criteria for evaluating the effectiveness of data and information security strategies	• propose and apply criteria to evaluate the effectiveness of current data and information security strategies	• Comprehensive set of evaluation criteria to measure effectiveness of the current data and information security strategies are proposed and applied.	Students are to propose and apply evaluation criteria that measure the effectiveness of the organisation's current data and information security strategies. Possible number of marks – 10 marks
• key legislation that affects how organisations control the collection, storage, communication and disposal of their data and information: the *Health Records Act 2001*, the *Privacy Act 1988* and the *Privacy and Data Protection Act 2014* • ethical issues arising from data and information security practices • possible consequences for organisations that fail or violate security measures	• identify and discuss possible legal and ethical consequences of ineffective data and information security strategies	• Comprehensive understanding of the relevant legal and ethical consequences of ineffective data and information security strategies.	Students are to identify and discuss the possible legal and ethical consequences to the organisation for their ineffective data and information security strategies. Possible number of marks – 15 marks
• strategies for resolving legal and ethical issues between stakeholders arising from information security practices • reasons to prepare for disaster and the scope of disaster recovery plans, including backing up, evacuation, restoration and test plans	• recommend and justify strategies to improve current data and information security practices	• Comprehensive recommendations are made and justified to improve the current data and information security practices.	Students are to recommend and justify improvements to the organisation's current data and information security practices. Possible number of marks – 15 marks