Unit 4 Data Analytics – 2024

Outcome 2 Cybersecurity: data and information 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 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.

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 refer to one organisation, which has data and information security strategies 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. The total number of the marks for the outcome should be out of 100.

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.	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 and the importance of data and information to them. Details regarding the network including the network type, physical and software security controls, hardware and software components used and technical protocols, the collection, storage, communication and disposal of data and information by the organisation and their current security strategies 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.
• 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.	Content should be included in the case study to enable students to identify and evaluate threats. Students will need to consider the types of threats and whether they are accidental, deliberate and events-based or a combination of them. There should be reference to these types of threats and how they impact the organisation. Data integrity is also affected by threats and these need to be identified within the case study to determine the impact on the organisation. The threats should be identified and evaluated as to how they are a threat to the security of data and information.
• 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.	The content above should enable students to evaluate the effectiveness of the organisation's data and information security strategies. The case study could include strategies for each of the following: currency of files, ease of retrieval and the integrity of data and security. The organisation should have some weaknesses in these areas. This will enable students to propose and apply evaluation criteria to measure the effectiveness of the current data and information security strategies.
• 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.	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 Privacy Act 1988, Health Records Act 2001 or Privacy and Data Protection Act 2014. The case study could include 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 whether the organisation is involved in sharing personal data or health data. Details describing how the organisation controls the collection, storage, communication and disposal of their data and information should be included. Students should be able to clearly identify some legal and ethical issues and understand the consequences of ineffective data and information security strategies to the organisation.
• 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.	The content above should enable students to make recommendations and to justify improvements to the current data and information security practices of the organisation.