|  |
| --- |
| **DATA ANALYTICS UNIT 4 OUTCOME 2****SCHOOL-ASSESSED COURSEWORK** |
| **Performance descriptors** |
|  |  |
| **Unit 4****Outcome 2**On completion of this unit the student should be able to respond to a teacher-provided case study to analyse the impact of a data breach on an organisation, identify and evaluate threats, evaluate current security strategies and make recommendations to improve security strategies. | **DESCRIPTOR: typical performance in each range** |
| **Key skill** | **Very low** | **Low** | **Medium** | **High** | **Very high** |
| **An analysis of the breach** |
| analyse a data breach and describe its impact on an organisation | Identifies the goals of the organisation.Identifies the data breach. | Outlines the goals and objectives of the organisation.Outlines the data breach. | Explains the importance of data security to the organisation and their goals. | Analyses the impact of the data breach on the organisation’s data and their goals. | Discusses the consequences of diminished data integrity to the organisation resulting from the data breach. |
| examine and describe an organisation’s current data and information security strategies | Identifies the current security controls used by the organisation to prevent unauthorised access to data and information. | Outlines the key features of the current security controls used by the organisation to prevent unauthorised access to data and information. | Explains the purpose of the current security controls used by the organisation to prevent unauthorised access to data and information, and to minimise data loss. | Examines the current use of the security controls used by the organisation to prevent unauthorised access to data and information, and to minimise data loss, highlighting weaknesses or lack of required security controls. | Describes the issues that led to the data breach, based on the organisation’s current data and information security strategies. |
| **An evaluation of the threats** |
| identify and evaluate the threats to the security of data and information | Identifies the threats to the integrity and security of data and information used by the organisation. | Outlines the threats to the integrity and security of data and information used by the organisation.Outlines the threats to data integrity. | Explains the importance of data integrity to the organisation. | Examines the effect of the threats to the data integrity of the data and information used by the organisation related to the characteristics of data integrity. | Evaluates the effect of the threats to the integrity and security of data and information to the organisation related to the consequences of diminished data integrity. |
| evaluate the disaster recovery plan for an organisation | Identifies the components of the organisation’s current disaster recovery plan. | Outlines the key features of the organisation’s current disaster recovery plan. | Explains the importance of each component of the disaster recovery plan to the organisation. | Analyses the impact of an ineffective disaster recovery plan on the organisation. | Evaluates the strengths and weaknesses of the organisation’s current disaster recovery plan.Proposes relevant improvements or additions to the disaster recovery plan. |
| propose and apply criteria to evaluate the effectiveness of current data and information security strategies | Identifies effectiveness measures that can be used to evaluate current data and information security strategies. | Outlines criteria to evaluate the effectiveness of the current data and information security strategies. | Proposes relevant criteria to evaluate the effectiveness of the current data and information security strategies.Describes how relevant criteria can be measured to evaluate the effectiveness of the current data and information security strategies. | Applies appropriate criteria to evaluate the effectiveness of the current data and information security strategies. | Applies a set of criteria to accurately evaluate and measure the effectiveness of the current data and information security strategies.Documents the findings clearly. |
| identify and discuss possible legal and ethical consequences of ineffective data and information security strategies | Identifies legal issues related to the data breach. | Outlines the relevant legal issues and consequences arising from the data breach.Outlines the key legislation relevant to the data breach. | Discusses the relevance of the key legislation to the organisation, including notifying impacted individuals and organisations of the data breach.Identifies ethical issues arising from the actions of the organisation. | Explains the possible legal and ethical consequences of ineffective data and information security strategies of the organisation. | Discusses the specific issues, resulting from the data breach, that should have been met by adhering to key legislation and the ethical issues arising from the organisation’s current data and information security strategies. |
| **Recommendations to improve security practices** |
| recommend and justify improvements to current data and information security strategies | Identifies security controls to improve the current data and information security strategies. | Outlines security controls and emerging trends to improve the current data and information security strategies. | Recommends new security controls and improvements to the current data and information security strategies.Recommendations are feasible. | Analyses the impact of the security controls and improvements to the current data and information security strategies.Recommendations have been prioritised in order of impact to the organisation. | Justifies the use of new security controls and improvements to the current data and information security strategies of the organisation. |

KEY to marking scale based on the Outcome contributing 100 marks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Very Low 1–20 | Low 21–40 | Medium 41–60 | High 61–80 | Very High 81–100 |