|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **SOFTWARE DEVELOPMENT 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 an organisation’s software development practices, identify and evaluate current security controls and threats to software development practices, and make recommendations to improve practices. | | **DESCRIPTOR: typical performance in each range** | | | | | |
| **Key skill** | **Very low** | **Low** | **Medium** | **High** | **Very high** |
| **An analysis of the organisation’s software development practices** | | | | | |
| analyse and describe an organisation’s software development practices | Identifies the goals of the organisation.  Identifies the current security controls used to protect software development practices. | Outlines the goals and objectives of the organisation.  Outlines the current security controls used to protect software development practices and data stored within the applications. | Explains the advantages and disadvantages of developing software in-house or externally.  Describes how the current security controls and threat modelling principles are used to protect software development practices and the data stored within the applications. | Explains the organisation’s current software development practices, including the use of security controls and threat modelling principles. | Analyses how the organisation’s current software development practices, including the use of security controls and threat modelling principles, support goals and objectives. |
| identify and describe vulnerabilities and risks based on current practices | Identifies vulnerabilities based on current practices. | Outlines vulnerabilities and risks based on current practices. | Discusses how the identified vulnerabilities and risks compromise software development and the data stored within applications. | Explains the nature of the vulnerabilities and risks and how they compromise software development practices. | Describes how the identified vulnerabilities and risks could impact/have impacted the organisation as a result of compromised software development practices. |
| **An evaluation of the current security controls and threats** | | | | | |
| propose and apply criteria to evaluate the effectiveness of the current software development practices | Identifies effectiveness measures that can be used to evaluate current software development practices. | Outlines criteria to evaluate the effectiveness of the current software development practices. | Proposes relevant criteria to evaluate the effectiveness of the current software development practices.  Describes how relevant criteria can be measured to evaluate the effectiveness of the current software development practices. | Applies appropriate criteria to evaluate the effectiveness of the current software development practices. | Applies a set of criteria to accurately evaluate and measure the effectiveness of the current software development practices.  Documents the findings clearly. |
| identify and discuss the possible legal and ethical consequences to an organisation for ineffective software development practices, and how these could be resolved | Identifies legal issues relating to ineffective software development practices. | Outlines the relevant legal issues and consequences arising from ineffective software development practices.  Outlines the key legislation and industry frameworks relevant to the organisation. | Discusses the relevance of the key legislation and industry frameworks to the organisation.  Identifies ethical issues arising due to the actions of the organisation.  Identifies possible resolutions to the identified legal and ethical consequences. | Discusses possible legal and ethical consequences that have arisen due to the actions of the organisation.  Proposes resolutions to the identified legal and ethical consequences. | Discusses viable resolutions to identified legal and ethical consequences, with reference to relevant key legislation and industry frameworks. |
| **Recommendations to improve practices** | | | | | |
| recommend and justify improvements to organisations and their development environments to enhance secure software development practices. | Identifies mitigation methods, including security controls, to reduce or eliminate threats, vulnerabilities and risks to the organisation and their development environment to improve software development practices. | Outlines mitigation methods, including security controls, to reduce or eliminate threats, vulnerabilities and risks to the organisation and their development environment to improve software development practices. | Recommends and describes feasible mitigation methods to enhance secure software development practices, including:   * security controls * threat modelling principles * improvement strategies.   References how the enhanced practices enable the organisation to meet legal obligations. | Analyses the impact of new mitigation methods to enhance secure software development practices, including:   * security controls * threat modelling principles * improvement strategies.   References how the enhanced practices enable the organisation to meet its goals and objectives. | Justifies the use of new mitigation methods to enhance secure software development practices, including:   * security controls * threat modelling principles * improvement strategies.   References how the enhanced practices enable the organisation to meet relevant industry frameworks. |

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 |