TECIS60342

Carry out secure software development activities

Overview

Information security breaches can lead to critical situations such as disclosure of customer information, denial of service, and threats to the continuity of business operations. These can have significant financial consequences, but the real cost to the organisation could be the loss of customer trust and confidence. This may be irreparable and impossible to quantify in monetary terms.

Software can be designed, developed, and deployed with information security considerations 'built in'. This includes factoring in necessary information security controls that minimise the risk exposure and the impact to the organisation if exploited. The information security features used to support secure software development can include: defining and implementing secure development standards; following the information security architecture for software development; implementing appropriate test strategies; verifying that developed software meets its security criteria (requirements and/or policy, standards & procedures); specifying processes to maintain the required level of security of software through its lifecycle and managing a system or component through a formal information security assessment.

This standard covers the competencies concerned with conducting secure software development. This includes implementing secure development standards and practices, translating information security requirements into secure software. Also to recommend and implement a range of standard technical security controls to make software solutions more resilient. And reducing the through the use of "standard" security architectures which support secure software development activities.

Performance criteria

You must be able to:

1. apply the organisation's secure software development architecture to software development projects in line with organisational requirements
2. accurately identify information security requirements for software solution development
3. clearly communicate how security requirements can be built into software solutions to relevant stakeholders
4. select and implement appropriate secure software development test strategies in line with organisational requirements
5. conduct rigorous testing of all aspects of software solutions to identify information security issues or risks
6. verify that a software product or system meets its security criteria (requirements, policy, standards & procedures) through software testing
7. critically review software solutions to ensure that they comply with any necessary internal and external information security standards and the information security architecture
8. review secure software development techniques and implement any identified improvements

Knowledge and understanding

You need to know and understand:

1. the range of information security architectures that can be applied to secure information system development
2. the internal and external security standards that need to be applied during secure software development
3. how to implement secure software controls into secure software development using an appropriate methodology
4. how information security testing that can be used to validate that information system security requirements are met
5. the approaches used to conduct a formal security assessment on a new software product or information system
6. the benefits of "designing in security into software applications and information systems
7. the potential threats and vulnerabilities that may need to be considered within any software design
8. how to use and apply information security standards, architectures and frameworks
9. the importance of minimising the risk to information assets or systems through the use of standard security architectures and models in secure software development
10. the potential issues and risks arising from a failure to comply with secure software development requirements
11. the importance of ensuring that any secure software design and development work undertaken aligns with the specified information security architecture
12. the importance of analysing potential threats associated with the software development approach being taken prior to design work being undertaken
13. the internal and external factors that may impact on the effectiveness of secure software development activities
14. how to apply secure software development for authentication mechanisms, protective monitoring, malware defences, secure protocols and cryptographic algorithms

Carry out secure software development activities

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60342
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, secure software development