TECIS60352

Manage 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 concerning with managing secure software development activities. This includes establishing a culture of designing security aspects into software development. Also defining and implementing secure development policies and standards for embedding preventative security measures into software development practice.

Performance criteria

You must be able to:

1. manage secure software development resources, activities and deliverables in line with organisational requirements
2. define and maintain secure software development policies and standards to minimise exposure to threats and risks
3. design and implement secure development training for software development teams to improve software resilience to information security vulnerabilities
4. develop and maintain the organisation's secure software development architecture in line with organisational requirements
5. review software designs to assess their security resilience in line with organisational standards
6. perform formal security assessments on software products to verify that they meet their security requirements in line with organisational standards
7. clearly communicate to software developers how information security requirements need to be built into particular software solutions or information systems being developed
8. select and implement appropriate software security test strategies to ensure compliance to security requirements
9. develop and implement assessment processes that maintain the required level of security of a software product, or information system through its lifecycle
10. present information on secure software development to a wide range of sponsors, stakeholders and other individuals

Knowledge and understanding

You need to know and understand:

1. how to manage secure software development activities
2. how to develop the policies and standards that relate to secure software development
3. the need to communicate the importance of secure software development and software resilience to a wide range of sponsors and stakeholders
4. the need to review the standard software designs used in secure software development
5. the range tools and techniques available to support secure software development activities and how to apply them
6. how to respond to new threats and vulnerabilities through improved secure software development tools and techniques
7. what is meant by a formal security assessment and how to perform them
8. the potential issues and risks arising from a failure to comply with security requirements in software development
9. what the internal and external factors that may impact on the effectiveness of secure development activities are
10. the importance of ensuring that any secure design and development work undertaken aligns with the security software development and wider security architectures
11. the need to communicate the deliverables produced by secure development activities to others
12. the need for monitoring the alignment of secure software development work with security architecture models and roadmaps

TECIS60352

Manage 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	TECIS60352
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