TECIS60461

Direct information security testing activities

Overview

Information security testing is the activity of assessing a system for the presence of security weaknesses or vulnerabilities. Network or infrastructure security testing, involves assessing network devices, servers, and other network infrastructure services such as Domain Name Service (DNS) for security vulnerabilities. Application security testing generally refers to testing custom or commercial software applications for security vulnerabilities. Web application security testing is specifically focused on testing web applications and mobile application security testing is specifically focused on testing mobile applications.

There are a few common types of security testing used. A vulnerability assessment typically involves scanning for security issues using some combination of automated tools and manual assessment techniques to confirm the presence of a vulnerability without actually exploiting it. Penetration testing identifies and exploits vulnerabilities. The goal is to emulate a real attacker who can break into a system and steal or modify data or impact the systems availability. Runtime testing involves assessing the system for security issues from the perspective of an end user. Code review involves assessing an application by reviewing its source code. Not performing a code review leaves a system open to greater risk from malicious insider threats.

This standard involves planning and setting of the overall strategy for information security testing within the organisation to maintain business information systems resilience. It also involves ensuring that the information security testing strategy is underpinned by effective policies, procedures and processes and that the resources are in place to deliver the strategy.

Performance criteria

You must be able to:

1. direct all aspects of information security testing activities to ensure effective testing operations to maintain high levels of information security resilience in line with organisational requirements
2. develop the strategy and policies for information security testing to meet organisational requirements
3. define the business case for investment in the information security testing function to maintain an effective information security testing capability of the appropriate capacity
4. represent, internally and externally, the interests of the organisation on matters relating to information security testing
5. drive innovation in information security testing across the organisation to improve organisational information system resilience
6. implement a research led continuous quality improvement programme for maintaining the effectiveness of information security testing activities
7. champion a culture of continuous improvement in information security testing activities in line with the changing threat and vulnerability landscape
8. provide thought leadership on the discipline of information security testing, contributing to internal best practice and to externally recognised forums

Knowledge and understanding

You need to know and understand:

1. the information security testing strategies that are required to meet organisational information security resilience requirements
2. how to develop strategy, policies, plans, processes, procedures and standards relating to information security testing
3. how to improve business information system resilience through information security testing
4. the internal and external threats and vulnerabilities driving information security testing and how to address them
5. the external factors that may impact on information security testing activities and how to identify them
6. how to manage the relationships with internal stakeholders and external bodies involved in information security testing
7. how to coordinate resources for information security testing operations
8. how to implement standards relating to information security testing and management
9. the risks to the organisation which can arise from poor quality information security testing and how to mitigate them
10. contemporary information security testing best practice
11. how to apply continuous improvement to information security testing activities to maintain their effectiveness

TECIS60461

Direct information security testing 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	TECIS60461
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, information security testing, penetration testing