TECIS60341

Carry out information security architecture activities

Overview

The protection of information, services and systems relies on a range of technical and procedural activities, often grouped in an information security architectural framework. The information security framework will contain technical and logical, physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and satisfy compliance obligations.

This standard defines the competencies involved in determining appropriate types of security controls, access management and network security devices and how they work.

Performance criteria

You must be able to:

1. develop information security architecture solutions for network security, infrastructure security, and application security in line with organisational requirements
2. incorporate organisational information security policies and threat/risk profiles into secure architectural solutions that mitigate the risks and conform to legislation in line with business needs
3. select information security products and technologies for use in information security architectures, based upon their strong information security characteristics
4. design robust and fault-tolerant information security mechanisms and components appropriate to the identified information security risks to information systems
5. propose information security architecture solutions which contribute to overall information systems architectures in line with organisational standards
6. develop and implement appropriate methodologies, templates, patterns and frameworks to support information security architecture development
7. apply information security architecture principles to improve the resilience of networks, information systems, control systems, infrastructures and digital products in line with organisational requirements
8. implement identity and access management frameworks into information security architectures in line with organisational standards
9. maintain own awareness of the information security advantages and vulnerabilities of digital products and technologies

Knowledge and understanding

You need to know and understand:

1. that information security controls can be categorised and selected on the basis of that categorisation
2. how technical controls (including cryptography, access management, firewalls, anti-virus software and intrusion prevention systems) work in detail and their associated strengths and weaknesses
3. how the technical information security controls can be deployed in practice
4. the need for information security architecture and its relevance to information systems, service continuity and reliability
5. how information security controls can be selected, deployed and tested to minimise risk and impact
6. how to differentiate between controls to protect systems availability and reliability, controls to protect information and controls to manage human behaviour
7. the trade-offs for functionality, usability and information security for a range of digital technologies and devices
8. the role of information security operations in monitoring, maintaining and evolving controls
9. what is meant by identity and access management within and beyond organisational boundaries
10. that where technical information security controls cannot be used, other forms of controls can be selected
11. how implementing an information security architecture can improve the risk potential for information system design
12. the relationship of information security architecture to IT and enterprise architectures
13. the advantages and disadvantages of implementing a range of commonly used IT components and security products
14. the features and benefits of a range of core information security technologies; e.g. access control models, public and private encryption, authentication techniques, intrusion detection
15. the range of processes, procedures, methods, tools and techniques applicable to secure architecture development activities and their deliverables
16. how to represent security architecture designs and models

TECIS60341

Carry out information security architecture 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	TECHIS60341
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, security architecture, secure solutions development