TECIS60331

Contribute to 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 covers the competencies required when proactively reacting to new threats and vulnerabilities through implementing the information security architecture. It includes establishing processes for maintaining the security of information throughout its lifespan. Also supporting the implementation of security operating procedures in accordance with security policies and standards.

Performance criteria

You must be able to:

1. contribute to the development of information security systems architectures which include infrastructure applications and cloud based solutions in line with organisation requirements
2. take account of relevant security policies and threat/risk profiles while contributing to the development of secure architectural solutions in order to mitigate risks and conform to legislation
3. advise information system designers on how to incorporate the organisations security architecture and user access management standards into information system design
4. review information systems designs for compliance with the information security architecture in line with organisational standards
5. maintain own awareness of the information security advantages and vulnerabilities of digital technologies and network systems

Knowledge and understanding

You need to know and understand:

1. what is meant by information security architecture
2. what are the main security architectures and frameworks and how to apply them
3. how to interpret organisational information security policies and standards that apply to information security architecture operations
4. the advantages and disadvantages of information system, network components and security products with respect to their vulnerabilities and protection capabilities
5. how to implement appropriate identity and access management requirements into information security architectures
6. the most appropriate information security products and protocols to use in meeting the organisation's security requirements
7. the range of processes, procedures, methods, tools and techniques applicable to information security architecture development
8. the range of core information security technologies including access control models, public and private encryption, authentication techniques, intrusion detection and identity synchronisation

TECIS60331

Contribute to 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	TECIS60331
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