
Overview

The protection of information is closely tied to the organisation and its requirements, the legal and regulatory environments in which the organisation operates and the need for all employees to handle information correctly. Information security governance and management is concerned with designing, implementing and operating the set of policies, procedures, processes and controls required to manage information security at an enterprise level. This is aimed at ensuring that an organisation's immediate and future regulatory, legal, environmental and operational information security requirements are complied with.

This standard covers the competencies involved with ensuring that information governance standards and the organisations information security policy are implemented within the organisation.

Carry out information security governance activities

Performance criteria

You must be able to:

1. implement information security governance and management processes within the organisation
2. undertake regular conformance checks of information security controls with organisational information security policies
3. maintain compliance with relevant legal and regulatory standards
4. identify, analyse and monitor threats and vulnerabilities to information systems and recommend updates to security controls
5. develop an information security policy or process to address an identified risk in line with organisational standards
6. promote the ethics of information security to peers and others within the organisation

Carry out information security governance activities

Knowledge and understanding

You need to know and understand:

1. why information security needs to be governed
2. how to develop information security policies, standards and guidelines
3. how to verify conformance of information security controls to information security policies
4. the common methodologies that are used for checking information security compliance
5. how to identify and analyse threats and vulnerabilities
6. the relevant legal, regulatory and information security standards
7. how to apply a structured approach to managing information security risks, business continuity, and IT operations within the context of an organisation's objectives

Carry out information security governance 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	TECIS60141
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 governance, information security management