

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 information security governance and includes managing the implementation of information security policies and strategies within the organisation.

Manage information security governance activities

Performance criteria

You must be able to:

1. develop and maintain information security strategy, policies, standards and processes in line with organisational requirements
2. identify information security awareness and training needs in line with the information security governance strategy
3. negotiate management commitment and financial resources to support information security training needs in line with organisational requirements
4. define and communicate individual roles, responsibilities and authority to the information security management team
5. manage the implementation of information security programmes in line with organisational requirements
6. manage all aspects of a security programme, including reacting to new threats and vulnerabilities consistent with organisational security policies, standards and procedures
7. manage the development and/or delivery of information security awareness and training programmes in line with organisational requirements
8. identify and advise on the information security risks associated with third party relationships
9. assess the quality and effectiveness of information security management processes against relevant internal and external policies and standards

Manage information security governance activities

Knowledge and understanding

You need to know and understand:

1. the legal and regulatory environment within which the business operates
2. the information security policies and standards required for effective information security management
3. the importance of securing financial support to maintain effective skills through training
4. that a successful information security strategy is made up of a number of phases including business awareness, strategy definition, strategy development, metrics, benchmarking and implementation and operation
5. the importance of aligning information security governance with the ethos, culture and business governance processes
6. the internal and external factors that may impact upon the effectiveness of information governance models and standards
7. the need to define roles and responsibilities in relation to information security governance activities
8. the fact that information security governance standards will only be effective if there is sufficient board level sponsorship for them
9. that information governance policies and standards will only be effective if they can be effectively communicated and enforced
10. the need to have both corporate information governance standards and lower level policies, procedures and standards relating to specific areas of information activities
11. how to assess the quality and effectiveness of information security management processes

Manage 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	TECIS60151
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