TECIS60161

Direct information security governance activities

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 role involves directing information security governance and management activities and setting the information security policy and strategies.

Performance criteria

You must be able to:

1. be fully accountable for all aspects of information security governance and management
2. create and maintain an information security strategy and governance framework in line with organisational requirements
3. assign information security governance responsibilities to relevant members of the information security management team
4. define measures for the outcomes of information security investments and information security improvements, and monitor and report on information security programme effectiveness
5. direct, develop and maintain organisational security policies, standards and processes using recognised standards
6. secure management commitment and resources to support information security governance and management activities in line with organisational requirements
7. monitor the alignment of information security management with all relevant legislation, regulation, internal and external standards, in line with organisational strategy, policies and standards
8. provide timely and objective advice and guidance to others on all aspects of information governance including best practice and the application of lessons learned
9. provide thought leadership on the discipline of information security governance and management, contributing to internal best practice and to externally recognised publications

Knowledge and understanding

You need to know and understand:

1. that effective information security requires co-ordinated and integrated action from the top down
2. what the multi-disciplinary information security structures, policies, procedures, processes and controls are and how they relate to each other
3. that cultural and organisational factors are fundamentally important to information security governance
4. how to create and maintain an information security strategy and governance framework
5. standards, and the Security Policy Framework and how to apply them
6. how to identify and incorporate areas best practice in relation to information security governance and management
7. that rules and priorities need to be established and enforced through information security policies and programmes
8. the need to provide a positive security influence across the organisation
9. the key factors to consider when creating an awareness or user education programme
10. that reputational damage can be considerable if information governance does not remain effective

Direct 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	TECIS60161
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