TECIS60131

Contribute to 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 standard covers the competencies involved with ensuring that information protection requirements, standards and policies are complied with. This includes understanding the organisational information security governance and management processes, identifying and addressing non-compliance and making recommendations for changes to ensure compliance requirements can be met.

Performance criteria

You must be able to:

1. analyse information security cases within the organisation to identify what threats, vulnerabilities or risks are mitigated and highlight any residual areas of concern
2. document information assets and their owners in an information asset register to help identify and manage the risks associated with them
3. evaluate security threats and hazards to information assets and systems in line with organisational standards
4. identify external sources of threat intelligence and utilise these to create an informed view of threats to the organisation
5. assist in developing an information security case including the security objectives, threats, identified attack techniques and the associated security controls that could be implemented to mitigate these
6. recognise and escalate non-compliances with information security controls, legislation and regulations in line with organisational requirements

Knowledge and understanding

You need to know and understand:

1. what is meant by information security governance and management
2. the difference between information security policies, standards, procedures and guidelines etc.
3. information security governance processes and how to apply them
4. what is meant by an information security case
5. how to develop and analyse an information security case
6. the main information security governance standards and management frameworks available and how to apply them
7. how to maintain an information asset register for assisting in identifying threats to information assets and systems
8. how to identify external sources of threat intelligence to maintain up to date threat awareness
9. the importance of ethical concerns in information security governance and management
10. the main information security concepts including identity, confidentiality, integrity, availability, threat, risk, hazard, trust, and assurance
11. the main features and applicability of law, regulations and standards relevant to information security

Contribute to 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	TECIS60131
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