TECIS60231

Contribute to information security risk assessment and management activities

Overview

Information in all its forms is a vital component of the digital environment in which we live and work. Information risk is concerned with assessing the importance of information to the organisation and the harm that can be caused from the failure to manage, use or protect information. Risk management allows an organisation to prioritise risks, deploy resources efficiently and to treat risks using a consistent and documented approach taking into account potential threats, vulnerabilities, and harm. Information system risk needs to be understood and actively planned for and managed within this context.

This standard defines the competencies for applying defined organisational processes for risk assessment and risk management, including risk treatment options. It also includes the knowledge and understanding for the concepts of information risk and business impact assessment.

Performance criteria

You must be able to:

1. assist in undertaking information security risk assessments and proposing remediation advice in line with organisational standards
2. identify potential vulnerabilities to specified information assets taking account of known threats
3. review and assess potential threats and vulnerabilities in terms of their risk potential, probability and potential impact on information assets
4. review internal and external policies, standards and other sources of information to ensure that newly emerging threats and risks are identified in a timely manner
5. follow an appropriate information security risk assessment methodology to assess and manage risks
6. identify the range of information security risk management controls that are used to mitigate information security risks
7. review information security risks against the stated risk tolerance levels and act in a timely manner to mitigate/control or escalate risks that exceed tolerance levels

Knowledge and understanding

You need to know and understand:

1. what is meant by information security risk assessment, risk management, risk mitigation and risk control and what these involve
2. the causes of information security risk to information assets and how to identify information assets at risk
3. how to classify threats and risk with respect to information assets and systems
4. the concepts of risk appetite and risk tolerance
5. the concept of residual risk and what it means for an organisation
6. that criteria can be used to assess the suitability of information security risk management approaches for an organisation
7. the fact that some information assets may be more valuable than others and as such require increased levels of protection/assurance
8. how risks to information assets can be caused by both accidental/negligent behaviour and also malicious activity
9. the importance of identifying and assessing risks in terms of both their potential impact and their probability to occur
10. where to source information on the threats and vulnerabilities on information assets
11. the policies, processes, and standards that exist for risk assessment and management and how to apply them
12. how to use and apply appropriate risk assessment and management methodologies and tools
13. how to establish the prioritisation, probability and likely impact of risks

TECIS60231

Contribute to information security risk assessment and management 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	TECIS60231
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, risk assessment, risk management