TECIS60251

Manage 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 concerned with conducting risk management activities on information systems, information assets and digital process control systems. It includes following the processes for managing, communicating and responding to risks on information systems, information assets and digital process control systems..

Performance criteria

You must be able to:

1. manage information security risk assessment activities for protecting information systems in line with organisational standards
2. review and maintain the strategy, policies, tools and techniques relating to information security risk assessment and management activities in line with organisational standards
3. develop information security risk business-impact tables to quantity risks to the organisations information assets and systems
4. correctly develop information security risk contingency plans, based upon analysis of the probability and impact of potential risks to information systems
5. manage the resourcing and training needs for information security risk assessment and management activities to meet organisational requirements
6. analyse threat evaluations and vulnerability testing results to produce accurate information security risk assessments
7. develop and maintain of information security risk assessment processes in accordance with relevant internal and external standards
8. evaluate information security risks associated with third party products and services as part of risk assessment activities
9. identify and document the range of approved response actions that may be used to mitigate information security risks
10. communicate risk assessment and management capability and performance measures to a wide range of sponsors, stakeholders and other individuals

Knowledge and understanding

You need to know and understand:

1. what are the available best practice methods, tools and techniques used to conduct information security risk assessment activities
2. how to undertake detailed risk assessments for complex information systems, conducting business impact analysis on the risks identified
3. how to develop information security risk business-impact tables
4. how to use and apply information from threat analysis, IT health checks and vulnerability testing tools to information security risk assessments
5. the importance of providing advice and guidance to less experienced staff
6. how to analyse, document and present risk assessment activities and outcomes
7. how to analyse threat assessments and evaluations
8. what are the range of methods for performing information security risk assessments in terms of usability, flexibility, and their outputs
9. how to plan training to meet the needs of the information security risk assessment and management function
10. the importance of monitoring the quality and effectiveness of information security risk assessment activities
11. the importance of communicating information security risk assessment and management status and performance measures with stakeholders

TECIS60251

Manage 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	TECIS60251
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