TECIS60241

Carry out 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 following the steps in the information risk assessment and management process. Ensuring that information risks are identified and assessed, that an impact assessment is undertaken, that risk treatment options are specified, appropriate controls selected and that there is ongoing monitoring and review.

Performance criteria

You must be able to:

1. perform information security risk assessments that identify and assess potential risks in terms of their probability of occurrence
2. analyse the identified risks to assess their potential impact on information assets and to determine whether they are within specified organisational information security risk tolerance levels
3. correctly identify the range of response actions that may be used to mitigate or control information security risks and apply these to high risk scenarios in line with organisational standards
4. contribute to the development and maintenance of information security risk management plans used to mitigate risks in accordance with relevant internal and external standards
5. regularly review the current and potential threats to the organisations information security, analysing trends and highlighting information security issues that need to be addressed
6. prepare and disseminate information security threat intelligence reports providing threat indicators and warnings in line with organisational standards
7. objectively analyse and clearly present the findings from information security risk assessment and management activities to sponsors and stakeholders

Knowledge and understanding

You need to know and understand:

1. that information security risk assessment and management refers to the processes of documenting what information is at risk, the type and level of that risk, and the impact of the risk being realised
2. how to undertake an information security risk assessment
3. that information is an organisational asset that has a value, which may be relative, and therefore can be classified to reflect its importance to the organisation
4. that information is vulnerable to threats to information systems
5. that information has attributes relating to confidentiality, possession or control, integrity, authenticity, availability, and utility, any of which can make it vulnerable to attack
6. that information may need to be protected and some of the reasons why that protection must occur, including legal and regulatory drivers, customer rights or organisational objectives
7. that information has a lifecycle, from creation through to deletion, and protection may be required and may change throughout that lifecycle
8. how to develop and maintain an information security risk management plan
9. the range of approaches that can be taken to information security risk assessment and management activities and their appropriateness in a range of business contexts
10. the internal and external factors that may impact on information security risk management activities
11. the regulations, legislation, internal and external standards that may apply to information security risk assessment and management activities
12. that risk management activities should be planned as ongoing/cyclical activity

Carry out 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	TECIS60241
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