TECIS60751

Manage information security audit, compliance and assurance activities

Overview

An information security audit verifies that information systems and processes meet the organisations security policies, standards and procedures, and can also help to assess the business benefits of security controls. Compliance monitoring defines and implements processes to verify on-going conformance to security and/or regulatory requirements. This is accomplished through undertaking security compliance checks against technical, physical, procedural and personnel controls using an appropriate methodology.

This standard defines the competencies concerning with managing information security audit activities. Including managing resources activities and deliverables. This also includes verifying compliance with security policies and standards as well as external legal and regulatory requirements. Planning, conducting and reporting on comprehensive security audit approaches, as well as designing and implementing organisational policies, standards and processes.

Performance criteria

You must be able to:

1. be fully accountable for undertaking complex, accurate information security audits on all types of information systems
2. develop, implement and maintain audit plans, processes, procedures, methods, tools and techniques for information security activities and their deliverables
3. lead and manage an audit team to execute technical audit projects in line with organisational requirements
4. evaluate the effectiveness of information security governance, tools and operations
5. evaluate the design, effectiveness and efficiency of information technology and security processes, procedures, and technical controls in line with organisational standards
6. use the results from risk and vulnerability assessments to inform audit activities
7. implement organisational logging and documentation standards to comply with audit requirements
8. clearly and accurately define the scope of information security audit activities
9. advise and guide others on all aspects of information security audit activities and their deliverables
10. clearly and effectively communicate information security audit results to a wide range of sponsors, stakeholders and other individuals

Knowledge and understanding

You need to know and understand:

1. what are the available methods, tools and techniques used to conduct information security audit activities
2. how to use and apply information and data from risk, threat and vulnerability assessments, into information security audit activities
3. how to set the levels of resources allocated to information security audit activities and prioritises their work
4. how to conduct peer reviews of information security audit policies and procedures
5. the range of information security audit methodologies that may be in terms of usability, flexibility, and the outputs they produce
6. how to analyse, document and present surety audit outcomes
7. the importance of monitoring the quality and effectiveness of information security audit activities
8. how to identify and implement improvements to information security audit processes and procedures
9. the need to ensure that information security audits are undertaken professionally
10. the relevance of existing and new methods, tools and techniques used to support information security audit activities

TECIS60751

Manage information security audit, compliance and assurance 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	TECIS60751
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, audit, compliance, assurance