

---

## 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 required for assisting with auditing information systems security robustness. This includes checking for and verifying compliance with security policies and standards as well as external legal and regulatory requirements. It also includes verifying that information systems meet the organisations security criteria, including policy, standards and procedures through undertaking security compliance audits in accordance with an appropriate methodology.

## Performance criteria

You must be able to:

1. record information systems and data assets in an asset management and tracking system in line with organisational standards
2. assist with conducting information security audits to verify that information systems and processes meet the organisations security policies and regulatory requirements
3. assist with compliance monitoring reviews to verify on-going organisational conformance to security polices and regulatory requirements
4. accurately gather and collate the findings from information security audit activities in line with organisational standards
5. clearly and objectively report the results and findings from information security audit activities
6. assist with the review and communication of the audit results and findings from with accountable owners and other stakeholders
7. assist with action planning to remediate any issues resulting from any particular information security audit

## Knowledge and understanding

You need to know and understand:

1. what is meant by an information security audit and compliance monitoring review
2. the objectives and benefits of conducting information security audits for the organisation
3. how to conduct an information security audit including planning, fieldwork, reporting and monitoring
4. the importance of operating with integrity, objectivity, confidentiality and competency
5. the different types of information security audit that can be undertaken including compliance-based, threat-based and combined
6. the common audit methodologies in use and how to apply these
7. the difference between a compliance monitoring review, an assessment and an audit
8. the organisational policies, processes, and standards together with legislation and regulatory requirements that exist for information security audit
9. who needs to be communicated with as part of any particular information security audit and/or compliance monitoring review
10. which processes and documents need to be assessed as part of an information security audit
11. that information security audits may be required as part of the regulatory and legal governance framework of the organisation
12. how to accurately identify and prioritise issues and risks arising from information security audits
13. the importance of information security audits in maintaining appropriate levels of compliance to internal policies and/or external standards
14. the importance of information security reviews in ensuring that compliance to internal policies and/or external standards is built into information systems and solutions
15. the importance of ensuring that information security policies, and the associated audit processes, procedures and approaches are maintained in line with emerging information security threats

Contribute to information security audit, compliance and assurance activities

<b>Developed by</b>	e-skills
<b>Version Number</b>	1
<b>Date Approved</b>	March 2016
<b>Indicative Review Date</b>	April 2019
<b>Validity</b>	Current
<b>Status</b>	Original
<b>Originating Organisation</b>	The Tech Partnership
<b>Original URN</b>	TECIS60731
<b>Relevant Occupations</b>	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
<b>Suite</b>	Information Security
<b>Keywords</b>	Information security, cyber security, audit, compliance, assurance