
Overview

Operational security management is a collection of associated security activities that help to maintain the ongoing security posture of an organisation. It consists of the monitoring, maintenance and management of the security aspects of the IT estate, its people, and its processes.

This standard defines the competencies required to manage all aspects of secure operations and service delivery. This include developing and maintaining operational security policies and standards and co-ordinate information security operations activities across the organisation.

Manage operational information security management activities

Performance criteria

You must be able to:

1. lead teams managing secure operations and service delivery activities in line with organisational requirements
2. develop and maintain operational information security management policies and procedures used across multiple information systems in line with organisational procedures
3. identify the need for, and implement new operational security management controls, and practices to meet changing organisational requirements
4. manage the alignment of IT operations and service delivery activities with relevant organisational information security strategy, policy and standards
5. routinely monitor operational security management provision, taking action to address potential vulnerabilities
6. develop and implement the necessary information security operations management plans to maintain effective resilience during ongoing operations and shutdown/closure of information systems
7. manage the review cycle for security operations, taking into account information from incidents, vulnerability assessments, penetration tests, threat assessments and changes to relevant legislation and regulations
8. routinely evaluate compliance to legal, regulatory, contractual and organisational requirements for the security of information assets
9. report the metrics on the performance of operational security management activities to sponsors, stakeholders and other internal/external individuals and bodies
10. provide advice regarding operational information security management activities to others

Knowledge and understanding

You need to know and understand:

1. how to write and maintain procedures required to ensure security of the organisation's information infrastructure
2. the specific requirements for the protection and security of customer/business information assets
3. how to interpret the results from any security issues, vulnerability assessments, security tests and threat assessments
4. what actions to take to mitigate security issues through information system operations management, problem tickets and help desk analysis
5. the user identity lifecycle within an organisation
6. how to ensure alignment of information system security operating processes and procedures to ensure that they provide cost effective security provision
7. how to influence sponsors and stakeholders to resource security operation management activities to ensure ongoing compliance with security requirements
8. the importance of ensuring that operational environments apply and maintain appropriate levels of security in line with standards and procedures
9. the fact that information security requirements may form part of specific service level and operational level agreements for information systems
10. the detailed content and relevance of organisational policies and standards for security operations management
11. the importance of reviewing and updating operating procedures for information security operations management
12. the need to maintain up to date security records and documentation
13. the need to manage the review cycle for information system

Manage operational information security 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	TECIS60551
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, operational security management