TECIS60642

Carry out information security incident investigation and management activities

Overview

When information security incidents occur, organisations must respond quickly and effectively to protect themselves from attack and limit the damage and scope of attacks. In order to do this they need to establish incident response teams and define the policies and standards relating to developing, operating, and improving incident management capabilities.

This standard defines the competencies associated with carrying out incident management activities related to identifying, eliminating and preventing potential and current information security threats.

Performance criteria

You must be able to:

1. carry out investigations into information security incidents acting as the primary point of escalation in line with organisational standards
2. coordinate the remediation of information security incidents including incident classification, investigation, resolution, reporting and closure in line with organisational standards
3. correctly implement the standards and procedures relating to information security incident management
4. provide timely and relevant updates on information security incidents to appropriate stakeholders
5. provide lessons learned from incident investigation findings to relevant stakeholders in order to help improve information security resilience within the organisation
6. implement and maintain information security incident response plans and processes to address potential threats in line with organisational requirements
7. facilitate remediation of issues identified during information security incident investigation and management activities
8. communicate the status and results of security incident investigations clearly and effectively to stakeholders in a timely manner

Knowledge and understanding

You need to know and understand:

1. the methods and tools that may be used to respond to information security incidents and how to apply them
2. the differences between information security incident investigation and management
3. the objectives of information security incident management
4. when to escalate information security incidents
5. how to document information security incidents correctly
6. the internal and external policies and standards that exist for information security incident management
7. how to correctly identify, source, gather and collate all relevant sources of information in order to respond to an information security incident
8. the need to act professionally and sensitively with all stakeholders when responding to information security incidents
9. the elements of an information security incident management and escalation plan
10. the key responsibilities when undertaking information security incident management
11. how to correctly identify, gather and document all relevant sources of information related to information security incidents
12. how to conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk
13. the need to maintain own capability to investigate information security incidents

TECIS60642

Carry out information security incident investigation 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	TECIS60642
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, incident investigation, incident management