TECIS60841

Carry out information security related business resilience activities

Overview

Business resilience encompasses the activities needed to recover from information security related incidents, crisis and disaster. It responds to all types of risk that an organisation may face from information security threats. As well as addressing the consequences of a major information security incident, crisis or disaster, information security related business resilience concerns the ability of an organisation to adapt to a dynamic changing environment of information security threats and conditions. Business resilience planning enables organisations to survive and succeed in an increasingly hostile risk, vulnerability and threat conscious environment knowing it can recover its critical business information systems processes and minimise business disruption.

This standard defines the competencies associated with undertaking information security related business resilience activities, including disaster recovery and business continuity. It includes implementing and testing information systems disaster recovery and business continuity plans in order to ensure that the organisation's business-critical information systems can be protected, and any serious incidents or disasters survived and recovered from as quickly as possible.

Performance criteria

You must be able to:

1. implement information security related business continuity management and disaster recovery processes and plans in line with organisational requirements
2. develop recovery strategies so that the organisation can resume normal operations as soon as possible following n information security incident in line with organisational requirements
3. correctly apply the processes, tools and techniques relating to information security business continuity and disaster recovery operations
4. implement routine information back up schedules so that all critical company data is frequently backed up and held in both on and off site storage
5. create and execute test scenarios to validate information systems business continuity and disaster recovery plans
6. analyse business processes to help determine the impact that information systems disaster scenarios might have on the organisation and how to mitigate these
7. collate and document the criteria for the secure restoration of specific information systems following an information security disruption, incident or disaster
8. follow the organisational escalation procedures when implementing information systems disaster recovery plans
9. communicate information on information systems business continuity and disaster recovery plans and tests to others within the organisation

Knowledge and understanding

You need to know and understand:

1. the principles of business continuity and disaster recovery
2. how to identify the processes, tools and techniques relating to disaster recovery activities
3. how to develop business continuity management plans that have a consequence on disaster recovery
4. what the consequences of disaster on the brand, reputation and the operational effectiveness of an organisation
5. how to interpret the results from disaster recovery tests and 'dry runs'
6. what constitutes an information security incident, crisis or disaster for an organisation and how to invoke the escalation process
7. how to restore specific information systems following an incident, crisis or disaster
8. the value in having current and effective disaster recovery and business continuity plans
9. what the potential implications of disaster recovery activities being incorrect, incomplete, inadequate and/or inappropriate
10. that disaster recovery plans must be tested to ensure that they will work effectively
11. the importance of advising and guiding others on disaster recovery options to meet the business needs to restore information systems
12. the importance of complying with the requirements for disaster recovery contained within the business continuity management plans
13. the importance of ensuring that there is relevant education and training provided to all individuals within the organisation on disaster recovery plans and activities
14. the need for monitoring of disaster recovery activities during tests and dry runs
15. what are the legislation, regulations and external standards that may impact on disaster recovery activities
16. the alignment of disaster recovery work and its deliverables with all relevant legislation regulations and external standards needs to be monitor
17. how to protect information during the recovery phase

TECIS60841

Carry out information security related business resilience 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	TECIS60841
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, business resilience, disaster recovery, business continuity