TECIS60831

Contribute to 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 contributing to the implementation of information security business resilience recovery planning.

Performance criteria

You must be able to:

1. correctly identify the internal and external standards for information security related business resilience planning in line with organisational requirements
2. contribute to the implementation of appropriate information security related business continuity management and disaster recovery processes and plans
3. collate and record, the business requirements for restoration of required information systems, services and assets to support ongoing operation of an organisation
4. undertake business impact analysis for the outage of different information systems within the organisation in line with organisational standards
5. follow policies, and standards to achieve the minimum disruption when recovering from information systems outages
6. gather all relevant information contained within business continuity management plans that have a consequence on information system recovery activities and planning
7. contribute to the estimation of information system recovery time, recovery point and maximum tolerable downtime in line with organisational standards
8. provide accurate and timely information on information system recovery plans, tests and 'dry runs' to others within the organisation

Knowledge and understanding

You need to know and understand:

1. what is meant by information security related business resilience, business continuity planning and disaster recovery
2. the internal and external standards for business resilience including ISO and how to apply them
3. the difference between an information security incident, crisis and disaster and how the recovery process works in recovering from these
4. the components and steps of information systems business continuity and disaster recovery plans and how to apply them
5. how to apply measurements of information systems recovery including recovery time, recovery point and maximum tolerable downtime
6. what the consequences of an information security related disaster are on the brand, reputation and the operational effectiveness of an organisation
7. that information security related business resilience planning is designed to cope with incidents affecting all of the organisation's business-critical information systems, from failure of a single server all the way through to complete loss of a major facility
8. the processes and activities required for the restoration of specific information systems to support ongoing operation of an organisation and how to apply them
9. that information security related business resilience planning must be tested to ensure that it will work effectively when required
10. that changes to information systems need to be reviewed and incorporated within information security related business resilience planning in order to keep plans current, complete and accurate

TECIS60831

Contribute to 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	TECIS60831
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