TECIS60851

Manage 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 managing information security related business resilience activities, including planning information system recovery strategies, setting policies, standards and guidelines, and maintaining the information systems business resilience capability.

Performance criteria

You must be able to:

1. lead the information security business resilience activities in line with organisational needs
2. define information systems recovery policies in line with organisational requirements
3. lead the creation and testing of information systems recovery and plans
4. make reasoned decisions on the cost and value of information security related business resilience provision, negotiating with sponsors and stakeholders where appropriate
5. coordinate and maintain documentation of information security related business resilience plans, policies, standards and guidelines
6. identify appropriate individuals in leading and/or executing information security related business resilience activities
7. implement training needs analysis and training plans for information security related business resilience staff to meet organisational requirements
8. select information systems recovery strategies consistent with the organisation's information risk appetite and maximum tolerable period of disruption
9. coordinate and communicate status of information systems business recovery activities the in the event of an incident occurring
10. undertake information systems recovery securely and in line with organisational standards
11. negotiate with senior management on the budget for information security related business resilience resourcing and training
12. identify training needs and solutions for information security related business resilience to meet organisational requirements
13. provide an on-going review of information security related business resilience tools, techniques and activities to maintain information system recovery capabilities
14. define information systems recovery testing programmes to assess and improve the information security related business resilience performance

Knowledge and understanding

You need to know and understand:

1. how to develop information security related business resilience policies, standards and plans that meet the needs of the business and are logistically, technically, and financially feasible
2. where to source best practice in business continuity and disaster recovery activities
3. what the best practice approaches for information security related business resilience planning are and how to apply them
4. how to monitor the alignment of information security related business resilience activities and their deliverables with all relevant legislation, regulations and external standards
5. what impact the consequences of an information security incident, crisis or disaster would have on the brand reputation and operational effectiveness of the organisation
6. what are the external factors and their implications that may impact on disaster recovery activities
7. how to analyse information generated by information systems disaster recovery activities in order to determine when and how to return to normal operations
8. how to define and apply triggers and escalation processes in order to establish when to invoke an information systems recovery plan
9. the need to manage relationships with sponsors, stakeholders and external bodies on information security related business resilience activities, and how to do this
10. how to identify information security related business resilience training needs, and where to source training provision
11. what are the priorities for recovering information systems and data assets
12. who are the sponsors and other stakeholders for information security related business resilience activities
13. how to communicate information systems recovery roles, responsibilities, processes and procedures to individuals, sponsors and other stakeholders
14. the importance of advising and guiding others on all aspects of information security related business resilience activities and their deliverables
15. how to negotiate with senior management to secure budget for resourcing, training and software tools for the information security related business resilience function

TECIS60851

Manage 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	TECIS60851
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