



Australian Government

ICTSAS505 Review and update disaster recovery and contingency plans

Release: 1

ICTSAS505 Review and update disaster recovery and contingency plans

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Application

This unit describes the skills and knowledge required to analyse the impact of the system on the organisation and carry out risk analysis, disaster recovery and contingency planning.

It applies to individuals who apply a wide range of higher level technical skills and systematic problem solving approaches in information and communications technology (ICT) related areas.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Systems administration and support

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Evaluate impact of system on business continuity	1.1 Identify business critical functions and the security environment from documentation and from discussion with business area and project team 1.2 Identify critical data and software from documentation 1.3 Assess potential impact of business risk and threats on ICT systems 1.4 Identify and evaluate statutory requirements, commercial requirements and contingency possibilities according to specifications and cost constraints

ELEMENT	PERFORMANCE CRITERIA
2. Evaluate threats to system	2.1 Identify threats to the system, considering security analysis and internal and external business environment 2.2 Evaluate risk minimisation alternatives against specifications and cost constraints
3. Formulate prevention and recovery strategy	3.1 Evaluate prevention and recovery options to support critical business functions against business specifications and cost constraints 3.2 Review current operational procedures to ensure adequate risk safeguards and contingency plans are in place 3.3 Submit disaster recovery and prevention strategy to appropriate person for approval
4. Develop disaster recovery plan to support strategy	4.1 Identify and document resources required for disaster recovery according to specifications and cost constraints 4.2 Identify and document processes required for disaster strategy according to project standards 4.3 Identify cut-over criteria before initiating disaster plan 4.4 Document disaster recovery plan and submit to appropriate person for review and sign-off

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Performance Criteria	Description
Reading	1.1, 1.2, 1.4, 3.2, 4.1, 4.3	Researches and analyses textual information and technical data/specifications from a range of documentation and sources to inform the development of contingency plans
Writing	3.3, 4.1, 4.2, 4.4	Uses clear and accurate language and formats appropriate to the task to convey explicit technical information, systems data requirements and recommendations
Oral Communication	1.1	Participates in a verbal exchange of ideas and elicits the view and opinions of others by listening and questioning

Numeracy	1.2, 1.4, 4.4	Accurately interprets, analyses and documents numerical, financial and technical system data
Navigate the world of work	1.4, 2.1, 3.2, 4.2	- Develops and implements strategies to ensure organisational policies, procedures and regulatory requirements are met - Monitors and reviews the organisations policies, procedures and adherence to legislative requirements to implement and manage change
Interact with others	1.1, 3.3, 4.4	- Uses relevant communication tools and strategies in building and maintaining effective working relationships - Influences and fosters a collaborative culture that facilitates a sense of commitment and workplace cohesion
Get the work done	1.1, 1.3, 1.4, 2.1, 2.2, 3.1, 3.2	- Plans strategic priorities and outcomes within a flexible, efficient and effective context in a diverse environment exposed to competing demands - Gathers and analyses data and seeks feedback to improve plans and processes - Addresses complex problems involving multiple variables, using formal analytical, lateral thinking techniques, experience and knowledge to focus in on the root cause

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTSAS505 Review and update disaster recovery and contingency plans	ICASAS505A Review and update disaster recovery and contingency plans	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTSAS505 Review and update disaster recovery and contingency plans

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the ability to:

- develop a contingency plan that identifies threats and minimises down time for business critical functions
- develop clear and specific directions on how to handle serious down time
- coordinate, plan and articulate flexible logistics requirements.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- compare and contrast backup methodologies
- explain the business planning process relevant to the development of information and communication technology (ICT) business solutions
- analyse the client business domain
- evaluate disaster recovery plan strategies and components, including:
 - physical security
 - system failure, accident or sabotage (hackers)
 - denial of service
 - virus attack
 - cyber attack
 - telecommunications failure
 - contingency arrangements
- interpret and analyse key workplace health and safety, legislative and organisational requirements relevant to the task
- evaluate the organisation's current systems functionality and systems engineering.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the systems administration and support field of work, and include access to:

- vulnerability assessment and general definition of requirements
- acceptance test plan
- business impact analysis
- information technology security assurance specifications
- relevant statutory documentation.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>