



Australian Government

Department of Education, Employment and Workplace Relations

ICASAS505A Review and update disaster recovery and contingency plans

Release: 1

ICASAS505A Review and update disaster recovery and contingency plans

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

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

Application of the Unit

This unit applies to information technology (IT) professionals who are required to prepare contingency plans in case of disaster.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.</i>

Elements and Performance Criteria

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 IT systems 1.4 Identify and evaluate statutory requirements, commercial requirements and contingency possibilities according to specifications and cost constraints
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 that 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

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- communication skills to:
 - gain consensus on concepts when disaster recovery plan is submitted to higher authorities for review and sign-off
 - negotiate with client business area and project team when business critical functions are identified from project documentation
- literacy skills to interpret statutory requirements
- planning and organisational skills to:
 - manage logistics for resources and procedures required for disaster recovery
 - scope project, and plan time, cost, and quality
 - scope communications, risk analysis and management
- research skills to:
 - follow best practice in system development
 - specify, analyse and evaluate broad features of a particular business domain.

Required knowledge

- backup methodologies
- business planning process relevant to the development of IT business solutions
- client business domain
- disaster recovery plan strategies and components, including:
 - physical security
 - system failure, accident or sabotage (hackers)
 - denial of service
 - virus attack
 - cyber attack
 - telecommunications failure
- OHS
- legislative and organisational requirements
- system's current functionality
- systems engineering.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • specify contingencies that minimise down time for business critical functions • clearly specify directions on how to handle serious down time • coordinate, plan and articulate flexible logistics requirements.
Context of and specific resources for assessment	Assessment must ensure access to: • appropriate learning and assessment support when required • modified equipment for people with special needs • vulnerability assessment and general definition of requirements • acceptance test plan • business impact analysis • information technology security assurance specifications • relevant statutory documentation.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • verbal or written questioning to assess candidate's knowledge of the disaster recovery or contingency plan to ensure the following is covered: • defined recovery requirements from the perspective of business functions • impact of an extended loss on operations and key business functions • contingency plan is understandable, and easy to use and maintain • contingency planning considerations may be integrated into ongoing business planning and system development processes • disaster recovery plan is not a one-off activity, but rather an ongoing process • review of disaster recovery plan developed by the candidate.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally

	appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.
--	---

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

<i>Business critical functions</i> may include:	• customer service functions • financial systems • payroll.
<i>Documentation</i> may relate to:	• audit trails • client training • International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Australian Standards (AS) standards • maintaining equipment inventory • naming standards • project management templates and report writing • satisfaction reports • version control.
<i>Project team</i> may include:	• different businesses working in partnership • individual business analysts • solution developers and business clients working together • third-party solution developers working together.
<i>Software</i> may include:	• commercial • in-house • packaged or customised software.
<i>Threats</i> may include:	• accident • cyber attack • denial of service • espionage • information technology failure • sabotage • security • telecommunications network failure • virus attack • weather, such as storms and earthquake.
<i>Systems</i> may include:	• application service provider • applications • databases • gateways

	- internet service provider (ISP) - operating systems - servers.
Statutory requirements may include:	- industry imposed controls and standards - legislation, such as Privacy Act - laws regarding confidentiality and reporting of data in organisations, such as health and banking.
Commercial requirements may include:	- access to internal network - availability - backup - confidentiality - encryption - firewalls - hacking - integrity - passwords and logons - storage and data recovery.
Constraints may include:	- budget - hardware - legal constraints - policy - resource - software - time.
Specifications may include:	- current system functionality - technical requirements - user-problem statement.
Contingency plans will typically:	- identify weaknesses and provide for the implementation of a disaster prevention program - minimise disruption to business operations - provide a coordinated approach to the disaster recovery process - vary in format and content detail.
Appropriate person may include:	- authorised business representative - client - supervisor.
Standards may include:	- ISO, IEC and AS standards - organisational standards - project standards.
Cut-over criteria may include:	- actual system down time - authorisations to cut-over - estimate of business impact, including

	• time before system is operational • cut-over plan refresher.
--	--

Unit Sector(s)

Systems administration and support