Australian Government
Department of Education, Employment and Workplace Relations

ICAA5056B Prepare disaster recovery and contingency plans

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICAA5056B Prepare disaster recovery and contingency plans

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to analyse the impact of the system on the organisation and carry out risk analysis, disaster recovery and contingency planning for the project. No licensing, legislative, regulatory or certification requirements apply to this unit at the time of publication.

Application of the Unit

Application of the unit	

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Prerequisite units		

Employability Skills Information

Employability skills	This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	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.

Elements and Performance Criteria

ELEMENT	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***, with consideration of 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

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Logistic management skills for identified resources and procedures skills (e.g. when IT hardware, software and resources required for disaster recovery are identified and documented according to project specifications and cost constraints)
- Negotiation skills in relation to self and other team members and applied to a defined range of predictable problems (e.g. when business-critical functions are identified from project documentation and discussion with client business area and project team)
- Project planning skills in relation to scope, time, cost, quality, communications, risk analysis and management (e.g. when business-critical functions are identified from project documentation and discussion with client business area and project team, and when contingency possibilities are identified and evaluated according to project specifications and cost constraints)
- Research skills for specifying, analysing and evaluating broad features of a particular business domain and best practice in system development (e.g. when threats to the system are identified, taking into consideration security analysis and internal and external business environment)
- Facilitation and presentation skills in relation to transferring and collecting information and gaining consensus on concepts (e.g. when business-critical functions are identified from project documentation and discussion with client business area and project team, and when disaster recovery plan is documented and submitted to higher authorities for review and sign-off

Required knowledge

- Broad knowledge of basic engineering (e.g. when evaluating threats)
- Broad knowledge of fire/safety knowledge (e.g. when formulating prevention and recovery strategy)
- Detailed knowledge of back-up methodologies (e.g. when formulating prevention and recovery strategy)
- Broad knowledge of systems engineering (e.g. when evaluating threats)
- Specific components of the business planning process relevant to the development of IT business solutions (e.g. when evaluating impact of system on business continuity)
- Broad knowledge of the client business domain (e.g. when evaluating impact of system on business continuity)
- Detailed knowledge of the system's current functionality (e.g. when evaluating impact of system on business continuity)

Evidence Guide

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 following is essential: • Assessment must confirm the ability to specify contingencies that minimise down time for business-critical functions. • Assessment must confirm the ability to clearly specify directions on how to handle serious down time. • Assessment must confirm the ability to coordinate, plan and articulate flexible logistics requirements. To demonstrate competency in this unit the learner will require access to: • A vulnerability assessment and general definition of requirements • Business impact analysis • Acceptance test plan • Information technology security assurance specifications
Context of and specific resources for assessment	Assessment of this unit of competency could include review of the disaster recovery/contingency plan developed by the learner to ensure the following is covered: • Defined recovery requirements from the perspective of business functions • The impact of an extended loss on operations and key business functions • The contingency plan is understandable, easy to use and easy to maintain • Contingency planning considerations may be integrated into ongoing business planning and system development processes • The disaster recovery plan is not a one-off activity, but rather an ongoing process

EVIDENCE GUIDE	
	The plan should cover: • Physical security • System failure, accident, sabotage (hackers) • Denial of service • Virus attack • Telecommunications failure Disaster recover plans are critical for organisations that rely on IT for business operations. The breadth, depth and complexity covering planning and initiation of alternative approaches to skills or knowledge applications across a broad range of technical and/or management requirements, evaluation and coordination would be characteristic. Assessment must ensure: • The demonstration of competency may also require self-directed application of knowledge and skills, with substantial depth in some areas where judgement is required in planning and selecting appropriate equipment, services and techniques for self and others. • Applications involve participation in development of strategic initiatives as well as personal responsibility and autonomy in performing complex technical operations or organising others. It may include participation in teams including teams concerned with planning and evaluation functions. Group or team coordination may also be involved.
Method of assessment	The purpose of this unit is to define the standard of performance to be achieved in the workplace. In undertaking training and assessment activities related to this unit, consideration should be given to the implementation of appropriate diversity and accessibility practices in order to accommodate people who may have special needs. Additional guidance on these and related

EVIDENCE GUIDE	
	matters is provided in ICA05 Section 1. - Competency in this unit should to be assessed using summative assessment to ensure consistency of performance in a range of contexts. This unit can be assessed either in the workplace or in a simulated environment. However, simulated activities must closely reflect the workplace to enable full demonstration of competency. - Assessment will usually include observation of real or simulated work processes and procedures and/or performance in a project context as well as questioning on underpinning knowledge and skills. The questioning of team members, supervisors, subordinates, peers and clients where appropriate may provide valuable input to the assessment process. The interdependence of units for assessment purposes may vary with the particular project or scenario.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended. An individual demonstrating this competency would be able to: - Demonstrate understanding of a broad knowledge base incorporating theoretical concepts, with substantial depth in some areas - Analyse and plan approaches to technical problems or management requirements - Transfer and apply theoretical concepts and/or technical or creative skills to a range of situations - Evaluate information, using it to forecast for planning or research purposes - Take responsibility for own outputs in relation to broad quantity and quality parameters - Take some responsibility for the achievement of group outcomes - Maintain knowledge of industry products and services

Range Statement

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.	
Business-critical functions may include but are not limited to:	• financial systems • customer service functions • payroll
Documentation may follow:	• ISO/IEC/AS standards • audit trails • naming standards • version control • project management templates and report writing • maintaining equipment inventory • client training • satisfaction reports
Project team may include:	• solution developers and business clients working together • individual business analysts • a number of third-party solution developers working together • a number of different businesses working in partnership
Software may include but are not limited to:	• commercial • in-house • packaged or customised software
Specifications may include but are not limited to:	• technical requirements • user problem statement • current system functionality
Constraints may include but are not limited to:	• time • budget • resource • hardware • software

RANGE STATEMENT	
	• policy • legal constraints
System may include but are not limited to:	• databases • applications • servers • operating systems • gateways • application service provider • ISP
Appropriate person may include:	• supervisor • teacher • authorised business representative • client
Threats may include:	• Weather (storms, earthquake) • Security • Information technology failure (hardware, software) • Accident • Espionage • Sabotage (hackers) • Telecommunications network failure • Denial of service • Virus attack Supplementary questioning of the client may be used during the assessment phase, where necessary, to ensure that all issues relating to threats to the system are considered and appropriate choices made given the need to prevent, limit, recover, respond and recover from disasters
Back-up strategy may include:	• hot standby site • warm standby site • cold standby site • mobile van • supplier • bureau • contacts through user group • third parties

RANGE STATEMENT	
Contingency plans will vary in format and content detail, but 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
Cut-over criteria may include:	• estimate of time before system is operational • estimate of business impact • authorisations to cut-over • actual system down time • refresher of cut-over plan
Security environment	• Includes legislation, organisational security policies, customs, expertise and knowledge that are, or may be, relevant. The security environment also includes the threats to security that are, or are held to be, present in the environment
Statutory requirements	• May include legislation (e.g. Privacy Act), industry-imposed controls and standards. In certain organisations (e.g. health and banking), there may be strict laws regarding confidentiality and reporting of data
Commercial requirements	• Back-up • Storage and recovery of data • Access to internal network • Passwords/logons • Encryption • Firewalls • Hacking • Confidentiality • Integrity • Availability
Standards may include:	• ISO/IEC/AS standards • organisational standards • project standards (for further information refer to the Standards Australia website at: www.standards.com.au)

Unit Sector(s)

Unit sector	Analyse and Design

Co-requisite units

Co-requisite units		

Competency field

Competency field	