Australian Government

Department of Education, Employment and Workplace Relations

ICASAS409A Manage risks involving ICT systems and technology

Release: 1

ICASAS409A Manage risks involving ICT systems and technology

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to implement procedures that identify, analyse, evaluate and monitor risks involving information and communications technology (ICT) systems and technology. This includes the development and management of contingency plans.

Application of the Unit

This unit applies to individuals in senior roles in various ICT areas who are required to manage risk in ICT systems.

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
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

1. Establish risk context	1.1 Review and document organisational and technical environment 1.2 Establish and document risk boundaries according to the business operating and strategic environment
2. Identify risk factors	2.1 Develop or acquire a measurement scale for project risk which includes importance, complexity, time and resources required 2.2 Identify project risks based on the measurement scale developed and document according to ***business requirements*** 2.3 Identify the business impact of changes and document according to current and future business directions
3. Implement contingency plans	3.1 Classify each risk and create ***contingency plans*** that address how the risk will be monitored and overcome, if possible 3.2 Identify measurable benchmarks to track the treatment of risks to the new ***system*** 3.3 Identify risk-management intervention points according to benchmarked performance tolerances 3.4 Demonstrate use of phased implementation and piloting to reduce risk factors
4. Monitor, update and report risk profile	4.1 Conduct regular risk updates to add new risks and remove old risks 4.2 Update contingency plans when appropriate to incorporate new information 4.3 Conduct risk reviews at major project milestones and document outcomes 4.4 Establish feedback processes to provide warning of potential new risks according to business requirements

Required Skills and Knowledge

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

Required skills

- analytical skills to analyse the risk associated with ICT systems and technologies
- communication skills to work with project teams on risk reviews
- literacy skills to:
  - disseminate and document technical specifications
  - write policy
- numeracy skills to scale risks
- planning and organisational skills to:
  - manage risk
  - plan for contingencies.

Required knowledge

- detailed knowledge of risk management
- overview knowledge of:
  - Australian Computer Society Code of Ethics
  - business process design
  - how business sites fit into corporate strategy
  - copyright and intellectual property in relation to IT systems and technology
  - privacy legislation relating to IT systems and technology
  - technology updating guidelines
  - business supply chain
  - user analysis and the CRM.

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: • identify where risk occurs • highlight the measures that will mitigate or obviate risk • set up procedures for regular risk reviews.
Context of and specific resources for assessment	Assessment must ensure access to: • analysis software • business website • networks • requirements documentation • risk management plan • site server • site server software • software applications • updated or new technology • user analysis • web servers • appropriate learning and assessment support when required • modified equipment for people with special needs.

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:
	  • risk management
	  • business process design
	• review of candidate's documented outcomes of risk assessment process
	• evaluation of candidate's documented contingency plans
	• direct observation of candidate conducting risk reviews at project milestones.

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.

Business requirements may relate to:	• application • business • network • people in the organisation • system.
Contingency plans may include:	• identifying weaknesses and providing for the implementation of a disaster prevention program • minimising disruption to business operations • providing a coordinated approach to the disaster recovery process.
System may include:	• application service provider • applications • databases • gateways • internet service provider (ISP) • operating systems • servers.

Unit Sector(s)

Systems administration and support