Australian Government

Department of Education, Employment and Workplace Relations

ICASAD503A Minimise risk of new technologies to business solutions

Release: 1

ICASAD503A Minimise risk of new technologies to business solutions

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 identify and plan to minimise the financial and technological risks facing business solutions using new technologies.

Application of the Unit

This unit applies to individuals in senior information and communications technology (ICT) roles in a variety of areas who are required to assess potential implications of new technologies, both monetary and technical.

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 the risk context	1.1 Review organisational and technical environment and proposed business solution 1.2 Identify scale, importance and complexity of project risks 1.3 Establish acceptable and unacceptable levels of risk and consequences for the ***solution*** 1.4 Identify the impact of risks against the business environment 1.5 Determine and document proposed actions to insure against identified generic risks
2. Conduct risk analysis	2.1 Conduct a risk analysis to determine the likelihood of risks identified 2.2 Rank risk factors according to the impact and likelihood of occurrence 2.3 Develop ***contingency plans*** to mitigate identified risks 2.4 Document risk analysis and contingencies in a ***risk-management plan*** 2.5 Implement risk management plans and undertake awareness training to inform ***stakeholders***
3. Monitor risks	3.1 Establish feedback channels to warn of unforeseen and identified risks 3.2 Conduct regular reviews to identify new risks and update established risks 3.3 Document changes to risk management plans as appropriate

Required Skills and Knowledge

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

Required skills

- analytical skills to review organisational and technical business solutions
- communication skills to liaise with stakeholders and provide training
- literacy skills to:
  - write and dissemination policy
  - write technical documents
- numeracy skills to assess financial risk
- planning and organisational skills to:
- develop mitigation strategies
  - manage a project
  - manage risk and implement contingency plans
- technical skills to:
  - maintain and administer a site
  - transfer files
  - use site design software and hardware.

Required knowledge

- business process design
- business supply chain
- copyright and intellectual property relating to new technologies
- how business sites fit into corporate strategy
- 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: • develop procedures that identify where risk occurs • identify measures to be taken to treat the risk.
Context of and specific resources for assessment	Assessment must ensure access to: • analysis software • business website • customer relationship model (CRM) • requirements documentation • site server • site server software • 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
	  • financial calculations of risk
	• review of candidate's documented risk management plan
	• evaluation of candidate's risk review procedures.

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.

Solution may include:	• implementing a new system • new hardware and hardware upgrades • new software and software upgrades • user training.
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.
Risk-management plan may include:	• insuring against risk may include transferring risk to external technicians or ensuring that indemnity insurance is valid and appropriate to the situation • potential risk events, preferred and alternative risk management strategies and actions, formal arrangements, responsibility assignment, contingency plans and assigned risk responsibilities.
Stakeholders may include:	• development team • project team • sponsor • user.

Unit Sector(s)

Systems analysis and design