Australian Government

Department of Education, Employment and Workplace Relations

ICAI5152B Implement risk management processes

Release: 1

ICAI5152B Implement risk management processes

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to implement procedures that identify, analyse, evaluate and monitor risks involving ICT systems and technology. This includes the development and management of contingency plans. The following unit is linked and forms an appropriate cluster: • ICAA5156B Review and plan to minimise risk to business solutions

Application of the Unit

Application of the unit	

Licensing/Regulatory Information

Not Applicable

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. Establish risk context	1.1. Review and document the 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

REQUIRED SKILLS AND KNOWLEDGE
This section describes the skills and knowledge required for this unit.

REQUIRED SKILLS AND KNOWLEDGE
Required skills
• Capacity planning • Technology transfer • Information architecture • Use of site design software and hardware • Project management
Required knowledge
• Technology updating guidelines • Business process design • Maintaining and administering a site • Understanding how business sites fit into corporate strategy • Policy writing and dissemination • Documenting technical specifications • Understanding the business supply chain • Understanding user analysis and the CRM • Copyright and intellectual property • Relevant privacy legislation • Australian Computer Society Code of Ethics

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 implement procedures that identify where risk occurs and what measures need to be taken to handle the risk. Contingency planning is an integral part of demonstrating competency. • Effective implementation procedures include preventative considerations, such as establishing warning systems and establishing an ongoing process that includes regular or programmed reviews to the risk profile. • Risk management must include managing those factors that may have an adverse effect on an external party, such as an business website customer or supplier. Consequently, risk management may need to be a collaborative process that involves users and commercial partners. To demonstrate competency in this unit the person will require access to: • Web servers • Business website • Site server • Site server software • Analysis software • Requirements documentation • Risk management plan • User analysis • Updated or new technology • Software applications • Networks
Context of and specific resources for assessment	The breadth, depth and complexity covering planning and initiation of alternative approaches to skills or knowledge applications across a broad range of technical

EVIDENCE GUIDE	
	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 matters is provided in ICA05 Section 1. • Competency in this unit should 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

EVIDENCE GUIDE	
	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, for example: • ICAA5156B Review and plan to minimise risk to business solutions 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 Additionally, an individual demonstrating this competency would be able to: • Demonstrate knowledge of risk management processes, incorporating some theoretical concepts • Apply solutions to a defined range of unpredictable problems • Identify and apply skill and knowledge areas to a wide variety of contexts, with depth in some areas • Identify and evaluate information • Take responsibility for the quality of risk assessment and contingency planning

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 requirements may be in reference to:	• business • system • application • network • people in the organisation
System may include but is not limited to:	• databases • applications • servers • operating systems • gateways • application service provider • ISP
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

Unit Sector(s)

Unit sector	Implement

Co-requisite units

Co-requisite units		

Co-requisite units		

Competency field

Competency field	