Australian Government

Department of Education, Employment and Workplace Relations

ICAA6052B Design an IT security framework

Release: 1

ICAA6052B Design an IT security framework

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to evaluate IT security requirements for a new system and to plan for controls and contingencies. The following unit is linked and forms an appropriate cluster: • ICAA6053B Design system security and controls 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		
	ICAA4041C	Determine and confirm client business expectations and needs

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. Research IT security requirements	1.1. Investigate and assemble relevant statutory, commercial and application ***security requirements*** 1.2. Assess impact on the existing IT system 1.3. Identify additional IT ***security requirements*** 1.4. Document ***security requirements*** and forward to ***appropriate person*** for approval
2. Conduct risk analysis	2.1. Identify ***security threats*** and determine security specifications, taking into consideration the internal and external business environment 2.2. Develop controls and contingencies to alleviate ***security threats*** 2.3. Identify the costs associated with contingencies 2.4. Document and forward recommendations to ***appropriate person*** for approval
3. Develop IT security policy and operational procedures	3.1. Review feedback from ***appropriate person*** to ascertain how to manage ***security threats*** 3.2. Develop ***security policies*** based on the ***security strategy*** 3.3. Create and document work procedures based on the security policies 3.4. Document operating procedures and forward to ***appropriate person*** for approval 3.5. Take action to ensure confidentiality of ***client*** and/or ***user*** information 3.6. Apply statutory requirements to policy and procedures

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE
This section describes the skills and knowledge required for this unit.
Required skills
• Researching skills related to security • Ability to articulate complex security scenarios in a clear concise manner relevant to all levels of the organisation

REQUIRED SKILLS AND KNOWLEDGE
• Skills in relation to analysis, evaluation and presentation of information • Group facilitation and presentation skills in relation to transferring and collecting information
Required knowledge
• Current industry-accepted hardware and software products, including broad knowledge of security features and capabilities • Accurate and in-depth knowledge of the client business domain • Broad general knowledge of privacy issues and legislation (e.g.when integrating legal requirements with IT security) • Risk analysis relating to IT security, including broad knowledge of general security issues incorporating substantial depth in some areas • Detailed knowledge of operating systems, including strengths and weaknesses over lifetime of product • Awareness of legislation relating to IT security

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 sufficient knowledge of the basic elements of legal obligations with respect to privacy and the specific application of security issues. • Assessment must confirm the ability to incorporate common security products and procedures into a security design. To demonstrate competency in this unit the following resources will be needed: • IT business specifications • Information on the security environment including relevant laws/legislation, existing organisational security policies, organisational expertise and knowledge • Possible security environment also includes the threats to security that are, or are held to be, present in the environment • Risk analysis tools/methodologies • IT security assurance specifications
Context of and specific resources for assessment	The breadth, depth and complexity involving analysis, design, planning, execution and evaluation across a range of technical and/or management functions including development of new criteria or applications or knowledge or procedures would be characteristic. Developing an IT security framework requires depth and complexity involving analysis, diagnosis, design, planning, execution and evaluation across a broad range of technical functions, including development of new criteria or applications or knowledge or procedures.

EVIDENCE GUIDE	
	Significant analysis of ISO/IEC/AS and other relevant standards is considered essential as a benchmark for establishing and maintaining a security framework. Significant contribution to the development of security polices, procedures and framework is involved. Assessment must ensure: • application of a significant range of fundamental principles and complex techniques across a wise and often unpredictable variety of contexts in relation to either varied or highly specific functions. Contribution to the development of a broad plan, budget or strategy may be involved and accountability and responsibility for self and others in achieving the outcomes may also be characteristic. • Applications involve significant judgement in planning, design, technical or leadership/guidance functions related to products, services, operations or procedures would be common.
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 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

EVIDENCE GUIDE	
	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 for example: • ICAA6053B Design system security and controls An individual demonstrating this competency would be able to: • Demonstrate clear understanding of security relationships between software, hardware and human interaction • Analyse security solutions and implement objective solutions across a broad range criteria • Produce security design solutions through the analysis of information and concepts at an abstract level • Demonstrate understanding of specialised knowledge with depth in some areas • Analyse, diagnose, design and execute judgement across a broad range of technical or management functions • Generate ideas through the analysis of information and concepts at an abstract level • Demonstrate a command of wide-ranging, highly specialised technical, creative or conceptual skills • Demonstrate accountability for personal outputs within broad parameters • Demonstrate accountability for personal and group outcomes within broad parameters.

Range Statement

RANGE STATEMENT
The range statement relates to the unit of competency as a whole. It allows for different

RANGE STATEMENT	
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.	
Security requirements	• May include laws, organisational security policies, customs, expertise and knowledge. The security environment also includes the threats to security that are, or are held to be, present in the environment, encryption, passwords, hardware, authentication and policies
Security threats may include but are not limited to:	• weaknesses in internet networks • local applications or LAN connections • keyboard logging • eavesdropping • data tampering and manipulation; impersonation, penetration and by-pass actions
Client may include but are not limited to:	• internal departments • external organisations • individual people • employees
Security policies	• To cover theft, viruses, standards (including archival, back-up, network), privacy, audits and alerts. Usually relates directly to the security objectives of the organisation
Security strategy includes:	• privacy • authentication • authorisation and integrity • usually relates directly to the security objectives of the organisation
User may include:	• a person within a department • a department within the organisation • a third party
Appropriate person may include:	• supervisor • teacher • authorised business representative • client

Unit Sector(s)

Unit sector	Analyse and Design

Co-requisite units

Co-requisite units		

Competency field

Competency field	