Australian Government
Department of Education, Employment and Workplace Relations

ICAA6053B Design system security and controls

Release: 1

INDUSTRY
SKILLS
COUNCILS
Creating Australia's Future

ICAA6053B Design system security and controls

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to design the controls that ensure the organisational system is secure from both a legal and business perspective. The following unit is linked and forms an appropriate cluster: • ICAA6052B Design an IT security framework 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. Review organisational security polices and procedures	1.1. Review business environment to identify existing ***requirements*** 1.2. Determine organisational goals for legal and security ***requirements*** 1.3. Verify security needs in a policy document 1.4. Determine legislative impact on business domain 1.5. Gather and document objective evidence on current ***security threats*** 1.6. Identify options for utilising internal and/or external expertise 1.7. Establish and document a standard methodology for performing security tests
2. Develop security plan	2.1. Investigate theoretical attacks and threats on the business 2.2. Evaluate risks and threats associated with the investigation 2.3. Prioritise assessment results and write ***security policy*** 2.4. Document information related to attacks, threats, risks and controls in a ***security plan*** 2.5. Review the ***security strategy*** with security-approved key ***stakeholders*** 2.6. Integrate approved changes into business plan and ensure compliance with statutory ***requirements***
3. Design controls to be incorporated in system	3.1. Implement controls in a procedurally organised manner to ensure minimum risk of security breach in line with ***organisational guidelines*** 3.2. Monitor each phase of the implementation to determine the impact on the business 3.3. Take corrective action on system implementation breakdown 3.4. Record implementation process 3.5. Evaluate corrective actions for risk 3.6. Plan ***risk assessment*** review process 3.7. Take action to ensure confidentiality throughout all phases of design

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Analysis and risk assessment data gathering techniques
- Problem solving skills for an evolving complex scenario of security threats
- Ability to provide accurate and concise insights to possible security threats for all levels of staff, both technical and managerial
- Ability to manage group facilitation and presentation skills in relation to transferring and collecting information (e.g. when senior management and auditor approval is obtained for the design of the controls)

Required knowledge

- Security testing methodology for performing security tests
- Information security risk assessment
- Process security for policies and procedures
- Internet technology security, including firewalls
- Communications security, including human organisational interactions
- Wireless security
- Physical security
- Current industry-accepted security processes, including general features and capabilities of software and hardware solutions
- Broad general knowledge of privacy issues and legislation (e.g. when specifying appropriate controls)
- Broad general knowledge of ethics in IT (e.g. when reviewing audit needs)
- Risk analysis, including broad knowledge of general features incorporating substantial depth in some areas (e.g. when designing controls to be incorporated in system)
- Broad knowledge of general features of specific security technology incorporating substantial depth in some areas (e.g. when specifying appropriate controls and for designing controls to be incorporated in system)
- Privacy (e.g. when designing controls to be incorporated in system)

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 security products and organisational security policy. • Assessment must confirm the ability to establish realistic ground rules for security product procedures. To demonstrate competency in this unit the following resources will be needed: • Risks to the mission/business resulting from IT-related risks • Probability, frequency and severity of direct and indirect harm, loss or misuse of the IT system • Security environment relating to relevant laws/legislation, existing organisational security policies, organisational expertise and knowledge that may be relevant • 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	Design covers: • Resilience of the system to security breaches • Layered security • Risk management in relation to overall system • Levels of security across system • Upgrade/scalability of system and security controls • Ease of implementation of security controls This unit involves organisational polices and procedures for information security, process security, internet technology security, communications security, wireless security and physical security.

EVIDENCE GUIDE	
	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. Competency in this unit will include observation of real or simulated procedures and polices, security plans and risk assessment strategies. Breadth, depth and complexity of knowledge and competencies would cover a broad range of varied activities in a wider variety of contexts, most of which are complex, evolving and critical in nature. Performance of a broad range of skilled applications, including requirements to evaluate and analyse current security practices and developing new criteria in a risk environment. 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

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 with specific emphasis on due process of policy creation assessment. 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, for example: • ICAA6052B Design an IT security framework An individual demonstrating this competency would be able to: • 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 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 environment	• Includes legislative requirements, organisational security policies, internal and external expertise and threat assessment plans • The security environment also includes the threats to security that are, or are held to be, present in the environment and in human social and organisational interaction
Stakeholders may include:	• sponsor • user • development team • project team
Organisational guidelines may include but are not limited to:	• personal use of emails and internet access • content of emails • downloading information and accessing particular websites • opening mail with attachments • virus risk • dispute resolution • document procedures • templates • communication methods • financial control mechanisms
Requirements may be in reference to:	• business • system • application • network • people in the organisation
Security plan	• A systematic process of controls identified by the organisation to be enforced. May contain social, physical and logical controls to safeguard organisational integrity

RANGE STATEMENT	
Security policy may be in relation to:	• theft • viruses • standards (including archival, back-up, network) • privacy • audits and alerts; usually relates directly to the security objectives of the organisation
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
Security strategy includes:	• privacy • authentication • authorisation and integrity • usually forms part of the overall objectives of the organisation
Risk assessment includes:	• developing risk plans • gathering information • identifying threats • evaluating threats • developing scenarios • ranking risk • identifying counter measures • reporting • following up

Unit Sector(s)

Unit sector	Analyse and Design

Co-requisite units

Co-requisite units		

Co-requisite units		

Competency field

Competency field	