



Australian Government

Department of Education, Employment and Workplace Relations

ICAS5118C Manage system security

Release: 1

ICAS5118C Manage system security

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to implement and manage security on an operational system. 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. Identify threats to system	1.1. Identify and understand the organisation's system 1.2. Conduct risk analysis on system and record outcomes 1.3. Evaluate threats to the system and record findings 1.4. Identify and document human interactions with system
2. Determine risk category	2.1. Conduct a risk assessment on the system and categorise risks 2.2. Conduct a risk assessment on human operations and interactions with the system and categorise risks 2.3. Match risk plans to risk categories 2.4. Determine and plan resources by risk categories
3. Identify appropriate controls	3.1. Identify and put in place effective controls to manage risk 3.2. Design policies and procedures to cover user access s of the system 3.3. Conduct training in the use of system -related policies and procedures 3.4. Monitor high-risk categories at specified periods 3.5. Identify and record system breakdowns
4. Include controls in the system	4.1. Develop security plan and procedures to include in management system 4.2. Develop security recovery plan 4.3. Implement system controls to reduce risks in human interaction with the system
5. Monitor system tools and procedures	5.1. Review and monitor risks and controls using a management review process 5.2. Review risk analysis process based on security benchmarks from vendors, security specialists and organisational reviews 5.3. Plan to re-evaluate system and identify new threats and risks

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Research skills for identifying, analysing and evaluating weaknesses and strengths of security systems
- Best practice in systems security methodologies and technologies
- Problem solving skills for a mixed mode environment of people and systems processes
- Management of unpredictable problems involving participation in group solutions and analysis
- Ability to communicate clear concepts and solutions to complex issues in an unambiguous manner
- Report writing skills requiring depth in some areas, analysis and evaluation of information in a defined range of areas
- Questioning and active listening skills

Required knowledge

- Systems management and process control in relation to security
- Specific knowledge of the client organisation
- Systems technologies, with broad knowledge of general features and capabilities, and substantial depth in some areas
- Risk analysis techniques, with broad knowledge of general features, and depth in security procedures
- Broad knowledge of general features of specific security technology, with substantial depth in some areas

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 knowledge of security risks and options available in the operating environment.
- Assessment must confirm the ability to implement and manage security functions on a system.

To demonstrate competency in this unit the following resources will be needed:

- Live system
- Utility tools

Context of and specific resources for assessment

System security is an increasingly important preoccupation for both ICT and business professionals.

As more organisations expand their operations using the internet and linking their infrastructure to mass communications media, managing systems effectively becomes paramount. Understanding systems is key to managing risk in a cost-effective and secure manner and effective system security is important not only for improving business operations, but in some cases preventing business loss by avoiding security breaches and threats.

Analysis involves participation in development of strategic reviews, determining security outcomes, as well as dependence on organisational information in a complex mixture of people and processes.

The breadth, depth and complexity covering planning and initiation of alternative approaches to skills or knowledge applications across a broad range of technical and/or management requirements, evaluation and

EVIDENCE GUIDE

	coordination would be characteristic. 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. Assessment must ensure: • 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 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 may provide valuable input to the assessment process.

EVIDENCE GUIDE**Guidance information for assessment**

The interdependence of units for assessment purposes may vary with the particular project or scenario. Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

An individual demonstrating this competency would be able to:

- Demonstrate understanding of security in relation to processes and people
- Develop plans and policies and theoretical issues in security, with substantial depth in some key areas
- Analyse and plan to solve technical problems
- Determine management requirements
- Apply theoretical concepts to technical issues
- Demonstrate creative skills in a range of complex situations
- Evaluate information, using it to forecast for planning purposes
- Take key responsibility for the achievement of security outcomes
- Maintain knowledge of industry products and services

Additionally, 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

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.

<i>System</i> may include but is not limited to:	• databases • applications • servers • operating systems • gateways • application service provider • ISP
<i>Threats</i> may include:	• Eavesdropping • manipulation • impersonation • penetration • denial of service and by-pass • hackers • viruses
<i>Security</i> may include but is not limited to:	• IPSec • SSL • PKM • LEAP • WEP • WPA • AAA • Diameter • tokens • smart cards
<i>Security plan</i> may include:	• theft • viruses • standards (including archival, back-up, network) • privacy • audits • alerts and usually relates directly to the security objectives of the organisation

Unit Sector(s)

Unit sector	Support
--------------------	---------

Co-requisite units

Co-requisite units		

Competency field

Competency field	
-------------------------	--