Australian Government

Department of Education, Employment and Workplace Relations

ICAS4127B Support system software

Release: 1

ICAS4127B Support system software

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to operate and support system software. The following units are linked and form an appropriate cluster: • ICAS4107B Rectify system faults on a live system • ICAS4119B Monitor and administer systems security 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		
	ICAI3020B	Install and optimise operating system software

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. Maintain system software	1.1. Evaluate system effectiveness against *organisational requirements* and benchmarks, to determine if maintenance activities should be commenced
	1.2. Use system utilisation, file and *disk* structure, performance reports and files to identify peak periods and possible performance problems
	1.3. Monitor *system* data levels to determine whether *system* performance is consistent with predetermined standards
	1.4. Troubleshoot the *system*, if required, with appropriate *system* tools
	1.5. Monitor and retune the *system*, where applicable, to improve performance
2. Set up and manage the system files	2.1. Evaluate *system requirements* and monitor the appropriateness of file and folder structures
	2.2. Use the appropriate administration and tools to create file and folder structures
	2.3. Set security, access and sharing of file system to meet *requirements*
	2.4. Identify the virus protection requirements of the network in line with *policies* and *organisational requirements*
	2.5. Scan the *system* for viruses and remove detected viruses
	2.6. Test the file *system* to ensure that appropriate access is available to the *user* groups
	2.7. Ensure log-on scripts and custom written utilities and programs conform to *organisational guidelines* for simple programming constructs
	2.8. Document the file *system* created in accordance with *organisational guidelines*
3. Monitor and manage system usage and security	3.1. Monitor *user* access against *user* access levels
	3.2. Review *security requirements* for *user* and data to be stored on *network*
	3.3. Determine risks that data is exposed to, and formulate appropriate prevention and recovery processes
	3.4. Implement a *system* to provide back-up and to restore services in the event of a disaster
	3.5. Document disaster recovery procedures

ELEMENT	PERFORMANCE CRITERIA
4. Carry out system backup	4.1. Confirm the back-up schedule meets *organisational requirements*
	4.2. Ensure *system* back-ups are completed according to organisational, scheduling and *system requirements*
	4.3. Ensure that a secure off-site location for the storage of back-up media is provided and used
	4.4. Ensure *system* back-ups are recorded according to *organisational requirements*
5. Restore system backup	5.1. Ensure *system* restores are completed when required for *system* recovery or testing according to *organisational guidelines*
	5.2. Optimise the restored *system* according to *organisational requirements*
	5.3. Ensure *system* restores are documented according to *organisational requirements*

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE
This section describes the skills and knowledge required for this unit.
Required skills
• Managing system support • Analysis skills in relation to routine and non-routine work processes • Report writing skills for business requiring depth in some areas, analysis, and evaluation of information in a defined range of areas • Problem solving skills in non-routine work processes • Plain English literacy and communication skills in relation to dealing with users and team members
Required knowledge
• Detailed understanding of using system software and system tools • Broad knowledge of vendor products and trends in product development • Broad general knowledge of the client business domain • Broad knowledge of quality assurance practices • Broad general knowledge of change management systems • Broad knowledge of OH&S requirements in relation to work safety, environmental factors and ergonomic considerations

Innovation and Business Skills Australia

Innovation and Business Skills Australia

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 monitor and maintain system software performance according to vendor and organisational benchmarks utilising a wide range of features and system tools. To demonstrate competency in this unit the learner will require access to: • Organisational performance benchmarks • Live system • Client user requirements
Context of and specific resources for assessment	Breadth, depth and complexity of knowledge and skills would prepare a person to perform a range of tasks necessary in supporting systems software. Operations must be undertaken in accordance with organisational polices and procedures. Managing the system software should be done under competent supervision where there is a clearly defined range of contexts for ensuring minimal disruption of services to the organisation. The breadth, depth and complexity of knowledge and skills in this competency would cover a broad range of varied activities or application in a wider variety of contexts most of which are complex and non-routine. Leadership and guidance would be involved when organising activities of self and others as well as contributing to technical solutions of a non-routine or contingency nature.

EVIDENCE GUIDE	
	Assessment must ensure:
	• Performance of a broad range of skilled applications including the requirement to evaluate and analyse current practices, develop new criteria and procedures for performing current practices and provision of some leadership and guidance to others in the application and planning of the skills would be characteristic.
	• Applications may involve responsibility for, and limited organisation of, others.
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 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:

EVIDENCE GUIDE

	• ICAS4107B Rectify system faults on a live system • ICAS4119B Monitor and administer systems security An individual demonstrating this competency would be able to: • Demonstrate relevant understanding of policies and procedures related to support system software, with theoretical knowledge of implementation issues in the system context • Apply known solutions to a variety of predictable software problems and perform processes that require some discretion • Interpret available website for managing systems software information using discretion and judgement • 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 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, analyse and evaluate information from a variety of sources • Take responsibility for own outputs in relation to specified quality standards • Take limited responsibility for the quantity and quality of the output of others

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

RANGE STATEMENT

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.

Organisational requirements may be in relation to:	• work environment • problem solution processes • preventative maintenance and diagnostic policy • roles and technical responsibilities in the IT department • vendor and product service-level support agreements
System may include but is not limited to:	• hardware and software components that run a computer, databases, applications, servers, operating systems, gateways, application service provider and ISP
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 and templates • communication methods • financial control mechanisms
Network may include but is not limited to:	• large and small LANs • VPNs • WANs • the internet • the use of the PSTN for dial-up modems only • private lines • data • voice
Security requirements may include but are not limited to:	• security levels • trusted sites • privacy • SSL • encryption
User may include:	• a person within a department • a department within the organisation

RANGE STATEMENT	
	• a third party
Policies may include:	• incident response procedures • network intrusion detection systems • forensic procedures • training • awareness raising strategies
System requirements may include but are not limited to:	• system functionality • geography • environment • client user • cost constraints
Disk may include but are not limited to:	• diskettes (floppy disks) • CD • CD-RW • DVD RW • zip disk • solid state hard drive

Unit Sector(s)

Unit sector	Support

Co-requisite units

Co-requisite units		

Competency field

Competency field	