



Australian Government

Department of Education, Employment and Workplace Relations

ICASAS419A Support system software

Release: 1

ICASAS419A Support system software

Modification History

Version	Comments
ICASAS419A	This version first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to operate and support system software.

Application of the Unit

This unit applies to individuals working in the support area who are required to provide technical assistance to users with operating system problems.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>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.</i>

Elements and 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 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 system for viruses and remove detected viruses 2.6 Test 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 according to 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 backup and to restore services in the event of a disaster 3.5 Document disaster recovery procedures
4. Carry out system	4.1 Confirm backup schedule meets organisational

backup	requirements 4.2 Ensure system backups are completed according to organisational, scheduling and system requirements 4.3 Ensure that a secure off-site location for the storage of backup media is provided and used 4.4 Ensure system backups 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

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

Required skills

- analytical skills to analyse routine and non-routine work processes
- communications skills to liaise with users and peers
- literacy skills to write business reports
- problem-solving skills to address a range of unpredictable operating system problems
- technical skills to update operating systems.

Required knowledge

- detailed knowledge of system software and system tools
- overview knowledge of:
 - change-management systems
 - client business domain
 - OHS requirements related to work safety, environmental factors and ergonomic considerations
 - quality assurance practices with regard to supporting system software
 - vendor products and trends in product development.

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 ability to: • monitor system software performance according to vendor and organisational benchmarks • maintain system performance to these benchmarks • use a wide range of features and system tools.
Context of and specific resources for assessment	Assessment must ensure access to: • organisational performance benchmarks • live system • client user requirements • appropriate learning and assessment support when required • modified equipment for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • verbal or written questioning to assess knowledge of: • system software • benchmark performance • system software tools • direct observation of candidate: • liaising with client • upgrading system software • review of candidate's call documentation • evaluation of client feedback from candidate's communications.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.

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.

Organisational requirements may relate to:	• preventative maintenance and diagnostic policy • problem solution processes • roles and technical responsibilities in the IT department • vendor and product service level support agreements • work environment.
Disk may include:	• CD • CD-RW • diskettes (floppy disks) • DVD RW • solid state hard drive • zip disk.
System may include:	• application service provider • applications • databases • gateways • hardware and software components that run a computer • ISP • operating systems • servers.
System requirements may include:	• client or user • cost constraints • environment • geography • system functionality.
Policies may include:	• awareness raising strategies • forensic procedures • incident response procedures • network intrusion detection systems • training.
User may include:	• department within the organisation • person within a department • third party.
Organisational	• communication methods

guidelines may include:	• content of emails • dispute resolution • document procedures and templates • downloading information and accessing particular websites • financial control mechanisms • opening mail with attachments • personal use of emails and internet access • virus risk.
Security requirements may include:	• encryption • privacy • security levels • secure socket layer (SSL) • trusted sites.
Network may include:	• data • large and small LANs • private lines • internet • use of the public switched telephone network (PSTN) for dial-up modems only • voice • virtual private networks (VPNs) • wide area networks (WANs).

Unit Sector(s)

Systems administration and support