Australian Government
Department of Education, Employment and Workplace Relations

ICAI5250A Develop, implement and evaluate system and application security

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICAI5250A Develop, implement and evaluate system and application security

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to develop, implement and evaluate information security in an IT system or application during the System Development Life Cycle (SDLC) prior to the Operations and Maintenance phase. The practice of these protocols ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. This objective is accomplished through risk assessment; risk mitigation; security control selection, implementation and evaluation; and software security standards compliance. 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		
	ICAB4225B	Automate processes

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. Develop system and application security	1.1. Specify the enterprise and ***IT system or application*** security policies 1.2. Specify the security requirements for the ***IT system or application*** 1.3. Author an IT system or application security plan in accordance with the enterprise and ***IT system or application*** security policies 1.4. Identify the standards against which to engineer the ***IT system or application*** 1.5. Specify the criteria for performing risk-based audits against the IT system or application 1.6. Develop processes and procedures to mitigate the introduction of ***vulnerabilities*** during the engineering process 1.7. Integrate applicable information security requirements, controls, processes, and procedures into ***IT system and application*** design specifications in accordance with ***established requirements***.
2. Implement system and application security	2.1. Execute the enterprise and IT system or application security policies 2.2. Apply and verify compliance with the identified standards against which to engineer ***the IT system or application*** 2.3. Perform the processes and procedures to mitigate the introduction of ***vulnerabilities*** during the engineering process 2.4. Perform secure configuration management practices 2.5. Validate that the engineered ***IT system and application*** security controls meet the specified requirements 2.6. Reengineer security controls to mitigate ***vulnerabilities*** identified during the operations phase 2.7. Ensure the integration of information security practices throughout the SDLC process 2.8. Document ***IT system or application security*** controls addressed within the system 2.9. Practise secure coding practices
3. Evaluate system and application security	3.1. Review new and existing risk management technologies to achieve an optimal enterprise risk posture 3.2. Review new and existing IT security technologies to support secure engineering across the SDLC phases 3.3. Continually assess the effectiveness of the

ELEMENT	PERFORMANCE CRITERIA
	information system's controls based on risk management practices and procedures 3.4. Assess and evaluate system compliance with corporate policies and architectures 3.5. Assess system maturation and readiness for promotion to the production stage 3.6. Collect lessons learned from integration of information security into the SDLC and use to identify improvement actions 3.7. Collect, analyse and report performance measures

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Reading and interpreting program specifications
- Translating requirements from problem space to machine space
- Integrated development environment usage
- Basic programming techniques
- Internal (code) documentation techniques
- Basic debugging techniques
- Testing techniques
- Basic documentation techniques

Required knowledge

- Programming language
- Small size application development
- Data structures
- GUI interfaces
- Best practice in application of language syntax rules

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: • IT system or application security plan • Application and verifying compliance with the identified standards • Practise secure coding practices • Assess and evaluate system compliance
Context of and specific resources for assessment	Assessment must ensure: • Author an IT system or application security plan • Apply and verify compliance with the identified standards • Ensure the integration of information security practices • Re-engineer security controls to mitigate vulnerabilities • Assess and evaluate system compliance • 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 • Application and system scenarios
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

EVIDENCE GUIDE	
	practices in order to accommodate people who may have special needs. Additional guidance on these and related matters is provided in ICA05 Section 1. The following assessment method is appropriate for this unit: • 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. 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. Additionally, 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.	
Established requirements may include:	• standards • policies • regulations • and laws
IT system or application may include:	• program • applications • collection of programs • integrated suite of programs • operating system and system software
Vulnerabilities may include:	• errors in application or system • trapdoors • undefined variables • buffer overflows • undefined or undocumented code • untested code • poor design

Unit Sector(s)

Unit sector	

Co-requisite units

Co-requisite units		

Co-requisite units		

Competency field

Competency field	