Australian Government

Department of Education, Employment and Workplace Relations

ICASAS501A Develop, implement and evaluate an incident response plan

Release: 1

ICASAS501A Develop, implement and evaluate an incident response plan

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to develop and implement an incident response plan. The results of the incident response plan must be evaluated if they affect the mission of the organisation.

Application of the Unit

This unit applies to network managers who are responsible for maintaining network service.

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
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

1. Develop the incident response program	1.1 Develop the ***incident*** management policy 1.2 Identify the services the incident response team should provide 1.3 Create incident response plans according to security policy and organisational goals 1.4 Develop procedures for incident handling and reporting 1.5 Create incident response exercises and red-teaming activities 1.6 Develop specific processes for collecting and protecting forensic evidence during incident response 1.7 Specify incident response staffing and training requirements 1.8 Establish the response program
2. Implement the incident response program	2.1 Apply response actions in reaction to security incidents according to established policy, plans and procedures 2.2 Respond to and report incidents 2.3 Assist in collecting, processing and preserving evidence ***according to requirements*** 2.4 Execute incident response plans 2.5 Execute red-teaming activities and incident response exercises 2.6 Ensure lessons learned from incidents are collected in a timely manner and are incorporated into review plans 2.7 Collect, analyse and report incident management measures
3. Evaluate the incident response program	3.1 Assess efficiency and effectiveness of incident response program activities and implement changes as required 3.2 Examine effectiveness of red teaming and incident response tests, training and exercises 3.3 Assess effectiveness of communication between incident response team and related internal and external organisations, implementing changes where appropriate 3.4 Identify and implement improvements based on assessments of effectiveness

Required Skills and Knowledge

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

Required skills

- communication skills to:
  - liaise with clients and team members
  - present technical information
- initiative and enterprise skills to develop incident response policies
- learning skills to build organisational knowledge
- literacy skills to prepare reports
- planning and organisational skills to:
  - manage a project
  - manage logistics for identified resources and procedures to ensure on-time availability of required equipment
- problem-solving skills to evaluate:
  - broad features of a particular business domain
  - best practice in system development.

Required knowledge

- broad knowledge of:
  - client business domain
  - OHS procedures when formulating prevention and recovery strategy
  - systems engineering when evaluating threats
- detailed knowledge of:
  - backup methodologies
  - specific components of the business planning process relevant to the development of information technology (IT) business solutions
  - current system functionality.

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: • develop an incident response program • manage an incident response activation and operation • evaluate the incident response.
Context of and specific resources for assessment	Assessment must ensure access to: • appropriate learning and assessment support when required • modified equipment for people with special needs • IT business specifications • information on the security environment, including relevant laws and legislation, existing organisational security policies, organisational expertise and knowledge • possible security environment, including threats to security that are, or are held to be, present in the environment • risk analysis tools and methodologies • IT security assurance specifications • incident scenarios.
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 candidate's knowledge of security environment and risk analysis • review of incident response plan and associated documentation.
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.

Incident may include:	• fire • misuse or improper access • other physical damage • theft of data or property • unauthorised publication.
According to requirements may include:	• directives • laws • policies • procedures • regulations • standards.

Unit Sector(s)

Systems administration and support