Australian Government

Department of Education, Employment and Workplace Relations

ICAI5252A Develop, implement and evaluate an incident response plan

Release: 1

ICAI5252A Develop, implement and evaluate an incident response plan

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required for the application of the knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate, and recover, and apply lessons learned from incidents impacting the mission of an organisation. 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		
	ICAP4037B	Contribute to the development of a strategy plan
	ICAI5152B	Implement risk management 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 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 in accordance with security policy and organisational goals 1.4. Develop procedures for performing 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 the incident response staffing and training requirements 1.8. Establish incident management measurement program
2. Implement the incident response program	2.1. Apply response actions in reaction to security incidents in accordance with 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 plan reviews 2.7. Collect, analyse, and report ***incident*** management measures
3. Evaluate the incident response program	3.1. Assess the efficiency and effectiveness of the incident response program activities and implement changes as required 3.2. Examine the effectiveness of red teaming and ***incident*** response tests, training, and exercises 3.3. Assess the effectiveness of communications between ***incident*** response team and related internal and external organisations and implement changes where appropriate 3.4. Identify incident management improvement actions

ELEMENT	PERFORMANCE CRITERIA
	based on assessments of effectiveness

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE
This section describes the skills and knowledge required for this unit.
Required skills
• Logistic management skills for identified resources and procedures skills • Negotiation skills in relation to self and other team members and applied to a defined range of predictable problems • Project planning skills in relation to scope, time, cost, quality, communications, risk analysis and management • Research skills for specifying, analysing and evaluating broad features of a particular business domain and best practice in system development • Facilitation and presentation skills in relation to transferring and collecting information and gaining consensus on concepts
Required knowledge
• Broad knowledge of basic engineering (e.g. when evaluating threats) • Broad knowledge of fire/safety knowledge (e.g. when formulating prevention and recovery strategy) • Detailed knowledge of back-up methodologies (e.g. when formulating prevention and recovery strategy) • Broad knowledge of systems engineering (e.g. when evaluating threats) • Specific components of the business planning process relevant to the development of IT business solutions (e.g. when evaluating impact of system on business continuity) • Broad knowledge of the client business domain (e.g. when evaluating impact of system on business continuity) • Detailed knowledge of the system's current functionality (e.g. when evaluating impact of system on business continuity)

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: • Develop the Incident response program • the Incident response activation and operation • Evaluation of the incident response
Context of and specific resources for assessment	Assessment must ensure: • The creation of incident response plans • The development of procedures for performing incident handling and reporting • Application of response actions in reaction to security incidents • Identify incident management improvement actions 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 • Incident 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 practices in order to accommodate people who may have special needs. Additional guidance on these and related matters is provided in ICA05 Section 1.

EVIDENCE GUIDE	
	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.	
Incident may include:	• fire • theft of data or property • misuse or improper access • unauthorised publication • other physical damage
According to requirements *may include*:	• standards • procedures • directives • policy • regulations • law

Unit Sector(s)

Unit sector	Implement

Co-requisite units

Co-requisite units		

Competency field

Competency field	