Interpretation Guide to fast track delivery of
Cyber Security and Cloud Computing skill sets

On 16 June 2020 the Australian Industry and Skills Committee (AISC) endorsed fast-tracked ICT projects ‘Getting a job in IT’ and ‘Getting a better job in IT’. These projects received Ministerial endorsement on 14 July 2020. These fast-tracked projects responded to industry’s need for short, industry relevant courses (skill sets) to assist in transitioning new workers into the ICT industry and upskilling existing workers. The approved skill sets were created to cover skills in cloud computing, cyber security, data analytics and the internet of things.

The ICT Industry Reference Committee (IRC) has created this Interpretation Guide (‘the Guide’) in relation to the five skill sets listed below:

- ICTSS00099 Cloud Design and Configuration Skill Set
- ICTSS00100 Cloud Implementation and Maintenance Skill Set
- ICTSS00101 Cyber Incident Response Skill Set
- ICTSS00102 Cyber Incident Threat Detection and Prevention Skill Set
- ICTSS00103 Cyber Security Strategy and Governance Skill Set.

The Guide was created to support registered training organisations (RTOs) use of these skill sets, through additional guidance for creating course content and assessment plans. The use of these skill sets will support the ICT industry to respond quickly to areas of critical workforce and skill needs in the recovery phase of the COVID-19 pandemic.

Purpose of the Guide

This Guide provides trainers and assessors delivering the above skill sets with insight from industry stakeholders, peak bodies, and other RTOs that will assist in creating meaningful and effective support material. The Guide consists of notes and interpretations relating to certain parts of units of competency within each skill set which may benefit from further clarification.
### ICTSS00099 Cloud Design and Configuration Skill Set Overview

<table>
<thead>
<tr>
<th>Code</th>
<th>Skill Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICTCLD501</td>
<td>Develop cloud disaster recovery plans</td>
<td>4</td>
</tr>
<tr>
<td>ICTCLD502</td>
<td>Design and implement highly-available cloud infrastructure</td>
<td>8</td>
</tr>
<tr>
<td>ICTCLD503</td>
<td>Implement web-scale cloud infrastructure</td>
<td>10</td>
</tr>
<tr>
<td>ICTCLD504</td>
<td>Improve cloud-based infrastructure</td>
<td>12</td>
</tr>
</tbody>
</table>

### ICTSS00100 Cloud Implementation and Maintenance Skill Set Overview

<table>
<thead>
<tr>
<th>Code</th>
<th>Skill Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICTCLD505</td>
<td>Implement cloud infrastructure with code</td>
<td>16</td>
</tr>
<tr>
<td>ICTCLD506</td>
<td>Implement virtual network in cloud environments</td>
<td>18</td>
</tr>
<tr>
<td>ICTCLD507</td>
<td>Build and deploy resources on cloud platforms</td>
<td>20</td>
</tr>
<tr>
<td>ICTCLD508</td>
<td>Manage infrastructure in cloud environments</td>
<td>21</td>
</tr>
</tbody>
</table>

### ICTSS00101 Cyber Incident Response Skill Set Overview

<table>
<thead>
<tr>
<th>Code</th>
<th>Skill Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICTCYS402</td>
<td>Identify and confirm cyber security incidents</td>
<td>23</td>
</tr>
<tr>
<td>ICTCYS403</td>
<td>Plan and implement information security strategies for an organisation</td>
<td>25</td>
</tr>
<tr>
<td>ICTCYS406</td>
<td>Respond to cyber security incidents</td>
<td>28</td>
</tr>
</tbody>
</table>

### ICTSS00102 Cyber Incident Threat Detection and Prevention Skill Set Overview

<table>
<thead>
<tr>
<th>Code</th>
<th>Skill Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICTCYS404</td>
<td>Run vulnerability assessments for an organisation</td>
<td>31</td>
</tr>
<tr>
<td>ICTCYS405</td>
<td>Develop cyber security incident response plans</td>
<td>32</td>
</tr>
<tr>
<td>ICTCYS407</td>
<td>Gather, analyse and interpret threat data</td>
<td>33</td>
</tr>
</tbody>
</table>

### ICTSS00103 Cyber Security Strategy and Governance Skill Set Overview

<table>
<thead>
<tr>
<th>Code</th>
<th>Skill Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICTCYS601</td>
<td>Create cyber security standards for organisations</td>
<td>36</td>
</tr>
<tr>
<td>ICTCYS604</td>
<td>Implement best practices for identity management</td>
<td>37</td>
</tr>
<tr>
<td>ICTCYS606</td>
<td>Evaluate an organisation’s compliance with cyber security standards and law</td>
<td>40</td>
</tr>
<tr>
<td>ICTCYS608</td>
<td>Perform cyber security risk assessments</td>
<td>41</td>
</tr>
</tbody>
</table>
Cloud Design and Configuration Overview

The Cloud Design and Configuration Skill Set incorporates specialist units of competency that support the development of cloud infrastructure in information and communications technology (ICT) environments. This skill set covers the following skills:

- develop cloud disaster recovery plans
- identify current and potential risk factors, including impact, likelihood, duration and cost of disruption in the cloud computing environment
- design and implement fault tolerant and scalable workloads to achieve high availability in a cloud environment
- design and deploy cloud infrastructure to support highly-scalable web applications
- assess, design, improve and monitor cloud architecture on a cloud platform, including security, reliability, scalability and cost optimisation impacts for an organisation.

Completion of this skill set will allow learners to pursue the following roles: cloud architects, cloud network engineers, cloud consultants and cloud developers.

Glossary of Common Terminology

<table>
<thead>
<tr>
<th>Cloud environments</th>
<th>These may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>public cloud</td>
</tr>
<tr>
<td></td>
<td>private cloud</td>
</tr>
<tr>
<td></td>
<td>hybrid cloud</td>
</tr>
<tr>
<td></td>
<td>community cloud</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud services</th>
<th>These may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infrastructure as a Service (IaaS)</td>
</tr>
<tr>
<td></td>
<td>Platform as a Service (PaaS)</td>
</tr>
<tr>
<td></td>
<td>Software as a Service (SaaS)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud Security</th>
<th>These may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cloud security monitoring (Application Programming Interface (API) logs and audit, event management)</td>
</tr>
<tr>
<td></td>
<td>encryption (in-transit vs at-rest, key management)</td>
</tr>
<tr>
<td></td>
<td>identity and access management (managing user credentials, identity federation)</td>
</tr>
<tr>
<td></td>
<td>network security (flow logs, web application firewall)</td>
</tr>
<tr>
<td></td>
<td>remediation (automate remediation of security events)</td>
</tr>
</tbody>
</table>

| General Data Protection Regulation (GDPR) | The European Union’s (EU’s) data protection standard. Australian businesses of any size may need to comply with the standard if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU (such as number of clicks on a website). |
### ICTCLD501 Develop cloud disaster recovery plans (1 of 4)

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.1 Identify disaster recovery plan requirements according to business needs and requirements | Disaster recovery plan requirements may include:  
   - organisational commitments set out in contracts and terms of conditions with customers  
   - scenarios covered by force majeure provisions. |
| 1.3 Identify vendor disaster recovery plan and service level agreements | Vendor disaster recovery plan may include:  
   - focusing on:  
     - gathering of disaster recovery personnel at the command center  
     - deciding if the incident is a disaster  
     - salvage operations, recovery operations, communications, restoration to normal operations  
     - creating a plan consisting of:  
       - backup procedures  
       - dedicated team and individual roles and responsibilities  
       - notification processes  
       - procedures for personnel and system recovery to normal operations  
       - senior management/board approval and involvement  
       - testing and updates.  
   - Service level agreements may include contracted service levels of vendors upon which the organisation depends. |
| 2.1 Determine time and recovery point objectives according to business needs | Recovery time objectives and recovery point objectives may be impacted by:  
   - customer expectations  
   - market area  
   - operational processes of an organisation  
   - size of the company  
   - type of business/industry. |
| 2.2 Assess potential risks plan exclusions according to business requirements | Risks plan exclusions may include:  
   - inflation risk  
   - interest rate risk  
   - liquidity risk  
   - longevity risk  
   - market risk  
   - opportunity risk  
   - sequence of returns risk  
   - tax risk. |
| 3.1 Develop range of disaster recovery solutions according to business requirements | Disaster recovery solutions may include:  
   - point in time snapshots  
   - backups and recovery  
   - automatic failover to standby resources  
   - synchronous/asynchronous replication of storage. |
| 3.2 Determine vendor protections and prioritise risks | Vendor protections may refer to:  
   - Australian Competition and Consumer Commission (ACCC) and their reference to business rights and protection  
   - Understanding Australian Business Regulation |

Cont'd on next page...
3.3 Assess external insurance protection levels and their suitability requirements

When assessing external insurance protection, the impact that business and/or cyber protection insurance has on the risk profile of the organisation may be considered.

External insurance may include:
- business insurance
- cyber protection insurance.

3.4 Identify other disaster recovery solution components

Components may include:
- dependencies of each service and their respective disaster recovery plan
- tools, resources and personnel required and their availability post-disaster.

4.2 Outline steps of disaster recovery plan including timelines, key features, service providers and any other aspect

Other aspects may include:
- ensuring stakeholder buy-in
- forming a team to execute the plan
- evaluating current plan and redesigning accordingly.

Foundation Skills

Self-management: Demonstrates a sophisticated knowledge of principles, concepts, language and practices associated with the cloud and digital world and uses them to troubleshoot and understand the uses and potential of new technology

Principles, concepts, language and practices may include:
- service model types, such as:
  - function as a service (FaaS)
  - infrastructure as a service (IaaS)
  - mobile backend as a service (MBaaS)
  - platform as a service (PaaS)
  - serverless computing
  - software as a service (SaaS)
- development models, such as:
  - public cloud
  - private cloud
  - hybrid cloud
  - community cloud.

Problem solving: Uses knowledge of context to address common threats in the cloud and technical environment

Common threats in cloud and technical environment may include:
- abuse and nefarious use of cloud services
- account or service hijacking
- compute/storage/network hardware failure
- data breaches
- data loss
- database/storage corruption
- failed software updates
- infrastructure/software failures
- insufficient identity, credential, and access management
- insecure interfaces or application programming interfaces (APIs)
- lack of due diligence
- loss of connectivity or power
- loss of network/DNS connectivity
- malicious insider
- physical threats (power outage, fire, terrorism, natural disasters, pandemics etc.)
- shared technology vulnerabilities
- system vulnerability.
## ICTCLD501 Develop cloud disaster recovery plans (3 of 4)

### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00099 Cloud Design and Configuration Skill Set</td>
</tr>
</tbody>
</table>

### Unit of Competency Interpretation Summary

#### Performance Evidence

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Develop and evaluate a cloud disaster recovery plan that includes at least three major risk events | Major risk events may include:  
- compliance violations  
- contractual breach  
- loss of control over end user actions  
- loss of critical service (e.g. primary database server)  
- loss of data centre/availability zone, including data breaches  
- loss of network connections in a hybrid cloud environment and cloud region  
- malware infections. |

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Document disaster recovery plan and ways the plan reaches Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets. | Disaster recovery plan may include:  
- service levels of vendors  
- time to detect an event  
- recovery time of services when calculating expected RTO and RPO. |

#### Knowledge Evidence

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Data analysis methodologies to determine risk environment             | Data analysis methodologies may include:  
- bow-tie analysis  
- Delphi technique  
- decision tree analysis  
- probability/consequence matrix  
- Structured What-if Technique (SWIFT) analysis. |

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Disaster recovery techniques applicable to cloud environments         | Disaster recovery techniques vary depending on an organisation’s preference for saving costs or recovery time. They may include:  
- asynchronous replication  
- synchronous replication  
- mixed techniques. |

Different disaster recovery techniques vary depending on the disaster recovery strategy stages, which may include:  
- backup and restore  
- pilot light  
- warm standby  
- multi-site solution.  
(Note: these strategy stages may be named something different depending on the cloud vendor)

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| ISO27001, ISO27002 and ISO27031 standards                             | ISO standards are international standards on how to manage information security. Standards may refer to those relating to:  
- disaster recovery  
- existing information security  
- organisation continuity. |

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Recovery Time Objective (RTO) and Recovery Point Objective (RPO) standards and techniques | Techniques may include:  
- analysis of recovery time and inclusion of contingency plan  
- applying a tracking system  
- business impact analysis  
- discovery and process mapping  
- mapping infrastructure. |
<table>
<thead>
<tr>
<th>Assessment Conditions</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Access to: Data required to assess current and future risk events in specified environment | Data required to assess risk events may include:  
● last point where data was in a usable format  
● time at which an event occurred  
● system recovery time point.                                                                                                                   |
| Access to: Legislation applicable to risk type              | Legislation may include:  
| Access to: Reporting standards for documenting and communicating disaster recovery plan | Reporting standards may include:  
● business continuity plan which consists of 5 components:  
  ○ business resumption plan  
  ○ continuity of operations plan  
  ○ disaster recovery plan.  
  ○ incident management plan  
  ○ occupant emergency plan  
● styles of plans such as prevention, detection and correction.                                                       |
## ICTCLD502 Design and implement highly-available cloud infrastructure (1 of 2)

### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00099 Cloud Design and Configuration Skill Set</td>
</tr>
</tbody>
</table>

### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify high-availability requirements</td>
<td>High-availability may include systems that: ● are capable of maintaining high level of traffic for longer time periods than normal ● detect failures as they occur ● eliminate single points of failure ● have reliable crossover.</td>
</tr>
<tr>
<td>2. Evaluate architecture availability</td>
<td>Architecture may include different types of cloud solutions used to ensure broad knowledge transfer across multiple vendors, including: ● public cloud ● private cloud ● hybrid cloud ● community cloud.</td>
</tr>
</tbody>
</table>

### Performance Criteria

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Review architecture of traditional multi-tier web application in non-cloud environment and identify high availability requirements</td>
<td>Traditional multi-tier web applications may include: ● segregation of organisation processes ● the following layers: ○ application ○ business ○ data access ○ presentation.</td>
</tr>
<tr>
<td>2.2 Identify any single points of failure</td>
<td>Single points of failure may include: ● lack of auto-scale core services ● single network address translation instance ● single domain name system (DNS) server ● workloads in a single data centre.</td>
</tr>
<tr>
<td>2.3 Estimate recovery objectives for multi-tier web components and for overall architecture</td>
<td>Recovery point objectives may be impacted by: ● customer expectations ● market area ● operational processes of an organisation ● size of the company ● type of business/industry.</td>
</tr>
<tr>
<td>2.4 Determine components that must scale vertically and the potential impact on system availability</td>
<td>Potential impacts of scaling vertically may include: ● data consistency ● less network load ● higher risk of server downtime compared to horizontal scaling method ● higher cost compared to horizontal scaling method ● no load balancing ● seamless upgrade ● single point of failure.</td>
</tr>
<tr>
<td>4.2 Demonstrate connectivity between resources at all tiers</td>
<td>Connectivity may include: ● connection from web server to app server using netcat ● to a page on the web server from the internet ● SQL query from application server to database. Tiers may refer to: ● infrastructure as a service (IaaS) ● platform as a service (PaaS) ● software as a service (SaaS).</td>
</tr>
</tbody>
</table>

Cont'd on next page...
### ICTCLD502 Design and implement highly-available cloud infrastructure (2 of 2)

#### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00099 Cloud Design and Configuration Skill Set</td>
</tr>
</tbody>
</table>

#### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4 Simulate failures of component and confirm that infrastructure is fault tolerant</td>
<td>Simulating failures may be performed by terminating hosts or network reconfiguration to block traffic. Fault tolerance may include: ● hardware systems that are backed up by equivalent systems ● software systems that are backed up by other software instances ● power sources that are made fault tolerant using alternative sources.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performance Evidence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design and deploy automated infrastructure scaling for at least one business need</td>
<td>Automated infrastructure scaling may include the use of an auto scaling service that increases the number of servers based on load.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Different cloud cost models as they relate to scalability of cloud infrastructure</td>
<td>Cloud cost models may include: ● free service (limited functionality but offer full functionality at a cost) ● pay as you use (pay only for what you use) ● planned payment (subscription model) ● tiered plan (different rates for additional add-ons to cloud platform).</td>
</tr>
<tr>
<td>Tools and techniques to measure availability impact</td>
<td>Techniques may include: ● measuring average availability of services ● triggering failure to measure impact in a test environment.</td>
</tr>
<tr>
<td>Purpose and features of load balancing and autoscaling as related to improve availability within cloud environment</td>
<td>Load balancing and autoscaling may include: ● distribution of load to application instances ● no disruption to the cloud infrastructure when there are traffic surges ● scaling of instance as required by demand.</td>
</tr>
</tbody>
</table>
### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Design scalable microservice architecture</td>
<td>Scalable microservice may include:</td>
</tr>
<tr>
<td>for a simple application</td>
<td>● cache</td>
</tr>
<tr>
<td></td>
<td>● content delivery network</td>
</tr>
<tr>
<td></td>
<td>● database scaling</td>
</tr>
<tr>
<td></td>
<td>● frontend and backend separation</td>
</tr>
<tr>
<td></td>
<td>● horizontal scaling</td>
</tr>
<tr>
<td></td>
<td>● load balancing</td>
</tr>
<tr>
<td></td>
<td>● microservices and containers</td>
</tr>
<tr>
<td></td>
<td>● vertical scaling</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Implement scalable microservice using cloud</td>
<td>Microservices could be implemented using:</td>
</tr>
<tr>
<td>services</td>
<td>● containers</td>
</tr>
<tr>
<td></td>
<td>● serverless functions</td>
</tr>
<tr>
<td></td>
<td>● other serverless infrastructure, including application programming</td>
</tr>
<tr>
<td></td>
<td>interface (API) gateways, object storage, message queues and</td>
</tr>
<tr>
<td></td>
<td>notification services</td>
</tr>
</tbody>
</table>

#### Performance Criteria

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Determine and</td>
<td>Web-scaling needs may include maintaining an average request</td>
</tr>
<tr>
<td>confirm cloud</td>
<td>response time even as number of requests increases and source of</td>
</tr>
<tr>
<td>web-scaling needs</td>
<td>requests spreads to other geographies.</td>
</tr>
</tbody>
</table>

#### Foundation Skills

| Reading: Interprets  | Notes                                                                 |
| complex technical   | Complex technical and operational documentation may include:          |
| and operational      | ● architecture diagrams of on-premise or cloud infrastructure         |
| documentation        | ● performance data that illustrates lack of scalability in particular |
| to determine and     | architectures.                                                       |
| confirm job          |                                                                      |
| requirements         |                                                                      |

#### Performance Evidence

| Design at least one  | Examples of architecture that would scale include:                    |
| architecture that    | ● networking                                                          |
| will scale           | ○ firewalls and other access controls                                 |
| networking, compute  | ○ IP networking and domain name system (DNS)                           |
| and storage for a    | ○ load balancers and content delivery networks                        |
| multi-tier web       | ○ traffic routing within a virtual network                            |
| application          | ○ virtual networking                                                 |
|                      | ● compute:                                                            |
|                      | ○ use of auto scaling                                                |
|                      | ● storage:                                                           |
|                      | ○ archive storage                                                   |
|                      | ○ block storage                                                     |
|                      | ○ network file systems                                              |
|                      | ○ object storage                                                    |
|                      | ○ storage lifecycle                                                 |
### ICTCLD503 Implement web-scale cloud infrastructure (2 of 2)

#### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00099 Cloud Design and Configuration Skill Set</td>
</tr>
</tbody>
</table>

#### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Testing and debugging techniques**                     | Testing and debugging techniques may include:  
  ● auto-scale core services  
  ● backtracking  
  ● binary search  
  ● black box testing  
  ● glass box testing  
  ● introduce multi region single domain name system (DNS)  
  ● randomised testing  
  ● removing single network address translation instance  
  ● testing data abstractions. |
| **Web-scaling principles and technologies**              | Web-scaling principles and technologies may include:  
  ● auto scaling  
  ● controlled virtual machines  
  ● embarrassingly parallel approach  
  ● HTTP-based services  
  ● load balancing  
  ● performance monitoring and alarms  
  ● removing single points of failure. |
## Unit of Competency Interpretation Summary

### Elements

| 2. Design and improve architecture on cloud platform | Improving architecture may involve:  
● reviewing the security, reliability, scalability, or cost  
● meeting organisational goals without over engineering  
● introducing more complexity. |

### Performance Criteria

| 1.1 Identify and review business's cloud architecture design | Business’s cloud architecture design may include:  
● cloud environment  
● hybrid environment  
● traditional on-premise environment. |

| 1.2 Evaluate cloud architecture and identify business impact of design decisions | Business impacts may include considerations of:  
● cost  
● reliability  
● security  
● scalability.  

E.g. the organisation may have suffered a security breach that was not detected for months in the current platform or they have a new customer that requires a higher service level agreement (SLA) and shorter Recovery Time Objective (RTO), and the new customer may add significant but varying load to the application.  
The demand on RTO may impact the business from a cost perspective as it is harder to address a demanding RTO. |

| 1.6 Set business goals as they relate to security, reliability, high-performance and cost efficiencies of cloud architecture according to business requirements and needs | Considerations for setting business goals may include:  
● platform service capabilities  
● regulation and compliance requirements applicable to cloud security mechanisms and protocols  
● types and levels of security requirements  
● security protocols and mechanisms  
● service infrastructure necessary for cloud security mechanisms.  

Security may include cloud cyber security protection measures to ensure recommendations to prevent against modern and sophisticated cyber attacks. |

| 3.3 Test and demonstrate security, reliability, scalability and cost optimisation of deployed resources | Demonstration may include:  
● product demonstrations to the organisation  
● articulating new product designs  
● identifying improvements which address organisational goals. |

| 4.2 Describe long-term improvement strategies and their benefits as applied to deployed resources | Long-term improvement strategies may include:  
● automating manual operational tasks  
● analysing and reviewing cloud service and provider selection  
● cloud modernisation of traditional applications  
● consolidating capabilities into a single tooling  
● developing on-premise infrastructure. |
## ICTCLD504 Improve cloud-based infrastructure (2 of 3)

### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00099 Cloud Design and Configuration Skill Set</td>
</tr>
</tbody>
</table>

### Unit of Competency Interpretation Summary

#### Foundation Skills

| Problem solving: Uses knowledge of context to address common problems in cloud computing applications and cloud-based environments | Common problems may include those relating to:  
- compliance  
- cost management and containment  
- governance/control  
- lack of resources/expertise  
- security. |

#### Performance Evidence

| Deploy, test and measure at least one architecture design, against architecture principles, metrics and business goals. | Architecture principles may include:  
- cost optimisation  
- operational excellence  
- performance efficiency  
- reliability  
- security.  

Metric and business goals may include:  
- bandwidth  
- capacity  
- cost per customer  
- latency  
- reliability  
- response time  
- scalability  
- security  
- service availability. |

#### Knowledge Evidence

| Methods and impacts of cloud adoption as they relate to IT system changes | Methods may include:  
- planned - set goals in establishing a cloud infrastructure  
- piecemeal - upgrade as required  
- random - use of other metrics as driving factors e.g. cost or worker skill level.  

Impacts may include:  
- fast and ubiquitous network connectivity  
- infinitely scalable computing platforms. |

| Design principles for cloud applications | Design principles may include:  
- automation is critical  
- cost optimisation  
- implementation of loose coupling to reduce dependencies  
- removal of single points of failure  
- secure database  
- servers as disposable resources. |

Cont'd on next page...
### ICTCLD504 Improve cloud-based infrastructure (3 of 3)

#### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00099 Cloud Design and Configuration Skill Set</td>
</tr>
</tbody>
</table>

#### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Migrating principles for cloud applications** | Migrating principles may include:  
  - access management  
  - identify areas that can be consolidated or automated  
  - identify migrating strategies  
  - monitoring and governance  
  - network management  
  - team technical expertise  
  - understand licensing and migration cost. |
| **Testing and debugging techniques, including techniques to avoid single point failures** | Testing and debugging techniques may include:  
  - auto-scale core services  
  - backtracking  
  - binary search  
  - black box testing  
  - glass box testing  
  - introduce multi region single domain name system (DNS)  
  - randomised testing  
  - removing single network address translation instance  
  - testing data abstractions. |
| **Tools and uses of security layers and security-focused content within cloud services** | Tool types may include:  
  - discover, analyse and secure  
  - discover and monitor  
  - encryption  
  - single sign on  
  - transparent protection.  
  Security layers may include:  
  - alerts and reporting  
  - disaster recovery  
  - encryption  
  - identity and access management  
  - network segmentation  
  - password control  
  - patching and maintenance  
  - user activity monitoring. |
Cloud Implementation and Maintenance Overview

The Cloud Implementation and Maintenance Skill Set incorporates specialist units of competency that support cloud implementation and maintenance in an organisation. This skill set covers the following skills:

- create and implement cloud infrastructure as code using cloud platform templates
- design and configure a virtual network according to networking requirements for a multi-tiered application on a cloud platform
- configure, deploy and monitor a range of technology resources of core cloud computing service on a cloud platform
- configure, monitor, maintain and update resources running in a cloud environment.

Completion of this skill set will allow learners to pursue the following roles: cloud engineers, cloud systems administrators and those in cloud computing operations to program, implement and maintain cloud computing solutions for organisations.

Glossary of Common terminology

<table>
<thead>
<tr>
<th>Cloud environments</th>
<th>Cloud environments may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>public cloud</td>
</tr>
<tr>
<td></td>
<td>private cloud</td>
</tr>
<tr>
<td></td>
<td>hybrid cloud</td>
</tr>
<tr>
<td></td>
<td>community cloud</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud resources</th>
<th>Cloud resources may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>application programming interface (API) gateways</td>
</tr>
<tr>
<td></td>
<td>block or object storage</td>
</tr>
<tr>
<td></td>
<td>container services</td>
</tr>
<tr>
<td></td>
<td>content delivery networks</td>
</tr>
<tr>
<td></td>
<td>domain name system (DNS)</td>
</tr>
<tr>
<td></td>
<td>load balancers and autoscaling</td>
</tr>
<tr>
<td></td>
<td>managed databases</td>
</tr>
<tr>
<td></td>
<td>serverless functions</td>
</tr>
<tr>
<td></td>
<td>virtual machines</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud services</th>
<th>Cloud services may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infrastructure as a Service (IaaS)</td>
</tr>
<tr>
<td></td>
<td>Software as a Service (SaaS)</td>
</tr>
<tr>
<td></td>
<td>Platform as a Service (PaaS)</td>
</tr>
</tbody>
</table>

| Infrastructure as Code (IaC) | Infrastructure as Code (IaC) is the process of managing the IT infrastructure using configuration files. |

<table>
<thead>
<tr>
<th>Policies and standards</th>
<th>Policies and standards may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloud Native Computing Foundation (CNCF) technology</td>
</tr>
<tr>
<td></td>
<td>open standards.</td>
</tr>
</tbody>
</table>

ICTSS00100 Cloud Implementation and Maintenance Skill Set guidance

Refer to pages 16 - 21 for the detailed interpretation of the units of competency in ICTSS00100.

The information in this Guide is offered as supplementary interpretation guidance for ICTSS00100. The interpretations and advice in this Guide are not enforceable and serve as guidance only. ASQA, VRQA and TAC are the sector regulators responsible for determining matters of compliance in relation to RTOs and training providers.
### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 2. Deploy cloud infrastructure as code templates | Code templates may include:  
  ● templates that deploy several resources  
  ● templates with modifiable and updatable components  
  ● templates that emulate cloud platforms. |

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.1 Identify and review benefits of infrastructure as code according to business needs | Benefits of infrastructure as code may include:  
  ● reproducibility  
  ● reusability  
  ● revision control of templates  
  ● speed of deploy  
  ● use of Continuous Integration/Continuous Deployment (CI/CD) pipelines for deployment and update of infrastructure. |
| 1.3 Determine and assess potential issues and errors when implementing infrastructure as code | Potential issues may include:  
  ● dependencies and race conditions between different resources  
  ● modifications to resources outside of templates  
  ● syntax errors in templates. |
| 3.5 Parameterise and deploy template to reuse configuration with a modified resource configuration | Parameterise may include:  
  ● changing the instance size  
  ● deploying a single database or a database cluster  
  ● the volume of storage  
  ● the number of machines in an autoscaling group. |
### ICTCLD505 Implement cloud infrastructure with code (2 of 2)

#### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00100 Cloud implementation and maintenance skill set</td>
</tr>
</tbody>
</table>

#### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Industry technology standards used in **cloud computing solutions and services** | Cloud computing solutions and services may include:  
  - infrastructure as a service (IaaS)  
  - platform as a service (PaaS)  
  - platform specific tools  
  - programming language toolkits  
  - software as a service (SaaS)  
  - third party tools. |
| **Syntax** of selected infrastructure as code service templates | Syntax may include:  
  - JSON  
  - YAML. |
| **Tooling** required to execute cloud infrastructure templates | Tooling may include:  
  - any framework that performs changes or configures infrastructure declaratively or imperatively based on a programmatic approach  
  - continuous configuration automation. |
| **Testing and debugging techniques**, including common issues and errors relating to deploying cloud infrastructure as code | Testing and debugging techniques may include:  
  - blue/green tests  
  - integration tests  
  - static or style checks  
  - system tests  
  - unit tests  
  - use of debugging scripts if applicable. |
| **Uses and methods** to create, manage, provision and update cloud resources and templates | Uses may include:  
  - checklist  
  - governance  
  - project planning  
  - strategy development. |
  
  Methods should be referred to by the respective cloud vendor provider as each provider may vary in method. |
| Techniques, methods and **industry standard metrics** used to leverage cloud platform capabilities and deploy and manage templates. | Industry standard metrics may include:  
  - metrics that are proportion of infrastructure defined as code,  
  - the time required to deploy a new infrastructure stack  
  - the level of reuse of these templates. |

#### Assessment Conditions

| Access to: Cloud vendor or third party **infrastructure as code service** | Infrastructure as code (IaC) services may include access to one of many different IaC providers. |
### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.1 Gather multi-tier application networking requirements according to business needs| Network requirements may include:  
  - network ports required for each service and traffic connectivity between services  
  - traffic to and from the internet.                                                                                                           |
| 1.2 Identify business and industry requirements for virtual network in cloud environment | Industry requirements may include:  
  - avoiding single points of failure  
  - minimising public facing resources  
  - spreading resources across data centres/availability zones to improve reliability  
  - using bastion hosts to minimise remote access points to other hosts.                                                                       |
| 2.3 Enable network gateways and its service as required                               | Enabling network gateways may include enabling remote gateways to control the increasing IT traffic from remote workers, so that rules can be applied and data can be protected.|

**Performance Evidence**

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design and deploy virtual network to support a multi-tier application in a cloud environment</td>
</tr>
</tbody>
</table>
| Multi-tier applications may include:  
  - application servers  
  - database servers  
  - web servers.                                                                                                                   |

**Knowledge Evidence**

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses and purpose of routing, routing targets, subnets, networking security controls, virtual private network (VPN) and IP address ranges</td>
</tr>
<tr>
<td>Uses and purposes of routing targets include defining VPN membership.</td>
</tr>
</tbody>
</table>
| Uses and purposes of subnets include:  
  - reducing congestion on network  
  - relieving stress on network.                                                                                                     |
| Uses and purposes of networking security controls include protecting data that is stored on the network or in transit across, into or out of the network. |
| Uses and purposes of virtual private network (VPN) may include training on cryptography and Public Key Infrastructure.          |
| Uses and purposes of IP address ranges include host or network interface identification and location addressing.                    |
## ICTCLD506 Implement virtual network in cloud environment (2 of 2)

### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00100 Cloud implementation and maintenance skill set</td>
</tr>
</tbody>
</table>

### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Testing and debugging techniques | Testing and debugging techniques may include:  
  ● packet analysis  
  ● port scanning  
  ● scenario testing (i.e. simulate network connections and traffic). |
| Methodology and techniques to collect and analyse network traffic metrics and traffic logs. | Network traffic metrics and traffic logs may include:  
  ● bandwidth and throughput  
  ● jitter  
  ● latency  
  ● packet loss. |
# Unit of Competency Interpretation Summary

## Performance Criteria

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.1 Review and confirm deploying and configuring a cloud resource task according to business needs | Business needs may include:  
- business standard practice  
- configuration details of resource  
- level of control the organisation requires. |
| 1.2 Determine cloud computing technology resources according to business needs       | Business needs may include cloud platforms which have more than one service for provisioning a type of resource  
E.g. a database could be installed on a virtual machine or by using a managed database service. |

## Foundation Skills

| Writing: Prepares and develops complex documentation in required formats using clear succinct and detailed language to convey explicit information, requirements and recommendations | Complex documentation may include:  
- explanatory documentation on code, fixes and changes made  
- maintenance guides  
- troubleshooting guides  
- organisational policy documents  
- operational guide. |

| Problem solving: Uses a mix of intuitive and formal processes to identify key information and issues, evaluates alternative | Intuitive and formal processes may include:  
- using a mix of analytical skills and soft-skills and working in cross-functional teams such as with designers and business analysts  
- using agile software development life cycles and design thinking methodology  
- recording the incident and development of mitigating actions for future reference. |

## Knowledge Evidence

| Industry technology standards used in cloud computing solutions and services | Industry technology standards may include:  
- cloud computing vendor specific policies and standards  
- National Institute of Standards and Technology (NIST) definition of cloud computing. |
### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT50120 Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00100 Cloud implementation and maintenance skill set</td>
</tr>
</tbody>
</table>

### Unit of Competency Interpretation Summary

#### Foundation Skills

| Writing: Prepares complex documentation detailing analysis, work performed and results using succinct language and logical structure | Complex documentation may include:  
  ● explanatory documentation on code, fixes and changes made  
  ● maintenance guides  
  ● troubleshooting guides  
  ● organisational policy documents  
  ● operational guide. |

#### Elements

| 6. Monitor and track complex cloud resources | Complex cloud resources may include:  
  ● compute  
  ● databases  
  ● networks  
  ● storage. |

#### Performance Criteria

| 2.4 Conduct maintenance with resources in specific category | Specific category may include virtual machines.  
  5.1 Identify data retention policy according to business needs and cloud resource | Data retention policy may include:  
  ● disposing information that is no longer needed at predetermined times  
  ● organising information to improve accessibility. |
Cyber Incident Response Overview

The Cyber Incident Response Skill Set incorporates specialist units of competency that support organisations in developing and responding to cyber security incidents. This skill set covers the following skills:

- identify, confirm and report cyber security incidents in an organisation
- develop an information security and risk management strategy (ISRM) within an organisation that supports organisational processes
- establish and respond to cyber security incidents in an organisation, and evaluate actions performed to mitigate risk of future incidents.

Completion of this skill set will allow learners to pursue the following roles: information technology security administrators and network administrators who work in information technology security in organisational environments.

Glossary of Common Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Government</td>
<td>The Australian Government Information Security Manual (ISM) outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats. The ISM is highly dependant on the National Institute of Standards and Technology (NIST) SP 800-37 and on the ISO 27000 series of Information Security Management Strategies.</td>
</tr>
<tr>
<td>Legislative requirements</td>
<td>May include:</td>
</tr>
<tr>
<td></td>
<td>- Privacy Act 1988.</td>
</tr>
<tr>
<td></td>
<td>- Report cybercrimes - Australian Signals Directorate (ASD) -</td>
</tr>
<tr>
<td>General Data Protection</td>
<td>European Union’s (EU’s) data protection standard. Australian businesses of any size may need to comply with the standard if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU (such as number of clicks on a website).</td>
</tr>
<tr>
<td>Regulation (GDPR)</td>
<td>MITRE corporation Manages federally funded research and development centers (FFRDCs) supporting several United States government agencies, and currently sets the global standard for Common Vulnerabilities and Exposures (CVEs). CVEs are unique, common identifiers for publicly known information-security vulnerabilities in publicly released software packages.</td>
</tr>
</tbody>
</table>

ICTSS00101 Cyber Incident Response Skill Set guidance

Refer to pages 23 - 29 for the detailed interpretation of the units of competency in ICTSS00101.

The information in this Guide is offered as supplementary interpretation guidance for ICTSS00101. The interpretations and advice in this Guide are not enforceable and serve as guidance only. ASQA, VRQA and TAC are the sector regulators responsible for determining matters of compliance in relation to RTOs and training providers.
ICTCYS402 Identify and confirm cyber security incidents (1 of 2)

**Unit of Competency Interpretation Summary**

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1. Identify cyber security incidents | Identifying cyber security incidents, specific to ICTCYS402, may include:  
  ● preparation before the incident, including leveraging:  
    ○ communication plan  
    ○ containment, eradication and recovery plans  
    ○ detection and analysis of the incident procedures  
    ○ the incident response team/key stakeholders  
    ○ the organisational incident response policy.  
  ● referring to NIST 800-61 R2:  
    ○ computer Security Incident Handling Guide  
  ● referring to Australian Government ISM - Guidelines for Cyber Security Incidents:  
    ○ ‘Managing Cyber Security Incidents’ |

**Performance Criteria**

| 1.3 Analyse and test application and confirm assumptions of incidents according to organisational security procedures | Testing incidents may include using or applying:  
  ● file integrity software  
  ● national vulnerability database (NVB)  
  ● network device logs  
  ● operating system service and application logs  
  ● penetration testing  
  ● publicly available information  
  ● server discovery  
  ● third party monitoring services.  
Confirming assumptions of incidents may include:  
  ● consultation and validation of incident events with key stakeholders within an organisation.  
  ● using intrusion, detection and prevention systems (IDPS)  
  ● using malware systems  
  ● using security information and event management (SIEM) systems. |

**Foundation Skills**

| Reading: Interprets information in a range of formats when identifying cyber security incidents | Range of formats may include:  
  ● blog posts  
  ● government websites  
  ● ICT security articles  
  ● virus protection vendor websites. |
ICTCYS402 Identify and confirm cyber security incidents (2 of 2)

Overview

ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT40120 Certificate IV in Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00101 Cyber Incident Response Skill Set</td>
</tr>
</tbody>
</table>

Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber security risks</td>
<td>Cyber security risks may include forms of cyber security vulnerabilities, and ways of remediating issues, found on MITRE's Common Vulnerabilities and Exposures (CVE) list - <a href="https://cve.mitre.org">https://cve.mitre.org</a>.</td>
</tr>
</tbody>
</table>
| Methods of testing systems, networks and applications and confirming incidents     | Methods specifies a series of instructions that can be carried out to test if an environment is susceptible to cyber attack. Methods may include:  
  ● examination of local instances of the application  
  ● network vulnerability scans  
  ● penetration testing  
  ● scanning for vulnerabilities in supporting third party services and libraries  
  ● security configuration reviews.  
  Tests may include:  
  ● checklist test  
  ● structured walkthrough test  
  ● simulation  
  ● parallel testing  
  ● full interruption testing.                                                                                          |
## ICTCYS403 Plan and implement information security strategies for an organisation (1 of 3)

### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT40120 Certificate IV in Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00101 Cyber incident Response Skill Set</td>
</tr>
</tbody>
</table>

### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 2. Design and implement information security strategy | Designing and implementing information security strategy, specific to ICTCYS403, may include:  
  ● referring to ISO/IEC 27001:  
    ○ ISO/IEC 27005 (Information security risk management),  
    ○ ISO/IEC 27014 (Security Governance),  
    ○ ISO/IEC 27017 (Cloud Security)  
    ○ ISO/IEC 27034 (Application security)  
  ● referring to NIST SP 800-37:  
    ○ Risk Management Framework  
    ○ developing, documenting and implementing security policy, standards, procedures and guidelines  
    ○ applying risk-based management concepts to the supply chain  
    ○ identifying, analysing and prioritising business continuity requirements  
    ○ identifying and planning a security awareness, education and training program strategy across the organisation  
    ○ understanding and applying risk management processes  
    ○ understanding and applying threat modelling concepts and methodologies. |

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.1 Discuss implementation opportunities for organisational information security strategies with required personnel | Implementation opportunities for organisational information security strategies may involve:  
  ● determining compliance requirements  
  ● evaluating and applying security governance principles  
  ● understanding legal and regulatory issues pertaining to information security in a global context  
  ● understanding, adhering to and promoting professional ethics. |
| 1.5 Identify legislation and industry requirements to implement information security strategies in an organisation | Legislative and industry requirements may include:  
  ● APRA's CPS 234  
  ● Australian privacy principles  
  ● Australian Government ISM - Guidelines for Cyber Security Incidents:  
    ○ ‘Managing Cyber Security Incidents’  
    ○ ‘Reporting Security Incidents’  
  ● notifiable data breaches scheme. |
| 2.2 Design secure network infrastructure and security strategy according to organisational needs | Strategies may include following the:  
  ● ASD Essential Eight  
  ● Australian Government ISM - Guidelines for Cyber Security Incidents:  
    ○ ‘Managing Cyber Security Incidents’  
    ○ ‘Reporting Security Incidents’. |

Cont'd on next page...
ICTCYS403 Plan and implement information security strategies for an organisation (2 of 3)

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 2.3 Analyse *data classifications* and levels of access in operational processes and integrate with strategy | Data classifications may be:  
  - aligned with the Privacy Act 1988  
  - explicit to organisation.  

Examples of Australian government websites with guidance on this include:  

Resources regarding data classifications may include:  
  - Data classification standard by the University of New South Wales - [https://www.datagovernance.unsw.edu.au/data-classification-standard](https://www.datagovernance.unsw.edu.au/data-classification-standard)  
| 3.1 Establish *security baselines* and *metrics* according to organisational needs | Security baselines may include:  
  - best case, worst case, average case scenario  
  - recovery time objective  
  - recovery point objective.  

Organisational needs may include:  
  - customer expectations  
  - market area  
  - operational processes of an organisation  
  - size of the company  
  - type of business/industry. |
| 3.2 Perform *testing procedures* and confirm information security strategy addresses organisational needs | Organisation needs may include:  
  - meeting legal and compliance needs  
  - meeting ethical standards  
  - meeting policy requirements  
  - developing business continuity such as scenario testing.  
  - developing risk management. |

<table>
<thead>
<tr>
<th>Performance Evidence</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Establish at least three *security baselines* and at least three *testing metrics* | Security baselines may include:  
  - best case, worst case, average case scenario  
  - recovery time objective  
  - recovery point objective.  

Planning the testing may include:  
  - applying threat model concepts  
  - establishing and maintaining security awareness. |
# ICTCYS403 Plan and implement information security strategies for an organisation (3 of 3)

## ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT40120 Certificate IV in Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00101 Cyber incident Response Skill Set</td>
</tr>
</tbody>
</table>

## Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function of information security strategy testing procedures, including:</strong></td>
<td>Testing procedures may include:</td>
</tr>
<tr>
<td>● vulnerability tests</td>
<td>● auditing</td>
</tr>
<tr>
<td>● basic penetration tests</td>
<td>● control testing</td>
</tr>
<tr>
<td></td>
<td>● full testing</td>
</tr>
<tr>
<td></td>
<td>● scenario testing</td>
</tr>
<tr>
<td></td>
<td>● table top exercises</td>
</tr>
<tr>
<td><strong>Types of data and classifications including sensitivity levels</strong></td>
<td>Types of data may include:</td>
</tr>
<tr>
<td></td>
<td>● boolean</td>
</tr>
<tr>
<td></td>
<td>● character</td>
</tr>
<tr>
<td></td>
<td>● floating-point number</td>
</tr>
<tr>
<td></td>
<td>● integer</td>
</tr>
<tr>
<td></td>
<td>● string</td>
</tr>
</tbody>
</table>

## Assessment Conditions

<table>
<thead>
<tr>
<th>Access to: Information and documents applicable to organisational procedures and processes</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Information may include organisational policies and procedures created in line with industry standards and legislation such as: | ● Australian Government ISM  
● Mandatory Breach notifications (may be State or Territory dependant)  
● Notifiable data breaches - Office of the Australian Information Commissioner (OAIC)  
## 1. Establish cyber security incident

Establishing cyber security incidents, specific to ICTCYS406, may include:

- preparation, including establishing and/or using:
  - the organisation’s incident response policy
  - communication plan
  - the incident response team
  - detection and analysis of the incident
  - containment, eradication and recovery
  - post incident activity
- referring to NIST 800-61 R2:
  - Computer Security Incident Handling Guide
- referring to the Australian Government ISM - Guidelines for Cyber Security Incidents:
  - ‘Managing Cyber Security Incidents’.

## 2. Activate cyber security incident response plan

Activating cyber security incident response plan may include:

- assembling the relevant team to address the incident
- detecting and ascertaining the source of the incident
- containing and recovering from the incident
- assessing the damage and severity of the incident
- beginning notification of breach incident
- developing prevention plans (incl. lesson learnt) and develop and implement controls to prevent future case for the given incident.

## Performance Criteria

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislative requirements may include guidance on reporting cyber security incidents from the Australian Government ISM.</td>
</tr>
<tr>
<td>Demonstration of cyber security incident response plans may include providing learners with examples of incident response plans from different industry sectors to ensure cross-sector knowledge is gained for disparate industries.</td>
</tr>
<tr>
<td>To better assist learners understand and identify cyber security incident response plans, trainers may include examples of incident response plans from different industry sectors to ensure cross-sector knowledge is gained for disparate industries.</td>
</tr>
<tr>
<td>Third party services and specialists may include:</td>
</tr>
<tr>
<td>- cyber security consultants</td>
</tr>
<tr>
<td>- hardware and software vendors</td>
</tr>
<tr>
<td>- law enforcement agencies depending on the nature of attack.</td>
</tr>
<tr>
<td>Preventative measures are methods that will reduce the risk of cyber incidents, mitigation methods are those used to prevent cyber security events from reoccurring. Preventative measures and mitigation methods may include:</td>
</tr>
<tr>
<td>- control access</td>
</tr>
<tr>
<td>- compensating measures</td>
</tr>
<tr>
<td>- firewall implementation</td>
</tr>
<tr>
<td>- monitor intrusions</td>
</tr>
<tr>
<td>- password strength</td>
</tr>
<tr>
<td>- updated programs</td>
</tr>
<tr>
<td>- use of security software.</td>
</tr>
</tbody>
</table>
# ICTCYS406 Respond to cyber security incidents (2 of 2)

## ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT40120 Certificate IV in Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00101 Cyber incident Response Skill Set</td>
</tr>
</tbody>
</table>

## Unit of Competency Interpretation Summary

### Performance Criteria

| 3.6 Share documentation and communicate with required personnel according to organisational communications plan | Documentation may include:  
|                                                                                                              | ● documented lessons learned  
|                                                                                                              | ● incident response plan  
|                                                                                                              | ● mandatory reporting requirements.  
|                                                                                                              |  
|                                                                                                              | Communicating with required personnel may include:  
|                                                                                                              | ● following organisational communications plan in an event of an incident, including  
|                                                                                                              | following priority of stakeholders to communicate with and the amount of information  
|                                                                                                              | to be communicated  
|                                                                                                              | ● involvement of law enforcement  
|                                                                                                              | ● involvement of media and public relations personnel  
|                                                                                                              | ● involvement of external organisations and agencies. |

### Performance Evidence

| Respond to at least two different cyber security incidents in at least two different business functions | An example of demonstration of responding to cyber security incidents may include creation of a cyber ‘Blue Team vs Red Team’ exercise where multiple incidents are executed and responded to by each team. |

### Knowledge Evidence

| Types of attacks, including:  
|● denial-of-service attack (DDOS)  
|● SQL injection (SQL)  
|● cross-site scripting (XSS) attacks  
|● scripted attacks  
|● hardware attacks  
|● attacks against Wi Fi | More information regarding types of attacks may be found by referring to the Common Vulnerability Scoring System (CVSS) or MITRE’s Common Vulnerabilities and Exposures (CVE) list ([https://cve.mitre.org/](https://cve.mitre.org/)) for other forms of cyber security attacks. |

| Organisational policies and procedures applicable to cyber security incident response, including procedures for:  
|● notifying and reporting to required personnel | Notifying and reporting may include referring to the Australian Government ISM - Guidelines for Cyber Security Incidents - ‘Reporting Security Incidents’. |

| Organisational policies and procedures applicable to cyber security incident response, including procedures for:  
|● assessing impact on business function and other areas | Impacts may include:  
|                                                                                                              | ● impact of time (i.e. recovery time objective)  
|                                                                                                              | ● impact on recovery point objective  
|                                                                                                              | ● reputational damage  
|                                                                                                              | ● privacy impact on stakeholder data  
|                                                                                                              | ● financial impact  
|                                                                                                              | ● impact on the security of organisational data. |

### Assessment Conditions

| Access to:  
|● organisation cyber security incident response plan  
|● required hardware and software  
|● text-editing software  
|● legislative requirements and organisational procedures and policies applicable to cyber security incident. | When conducting the assessment and considering required software to provide the learner, relevant access to systems and network logs/telemetry that has indicated a previous cyber incident may be useful to provide to learners. |
Cyber Incident Threat Detection and Prevention Overview

The Cyber Incident Threat Detection and Prevention Skill Set incorporates specialist units of competency that support organisations in identifying cyber related threats and implementing infrastructure as a prevention mechanism. Risk and threat identification and mitigation are crucial in supporting organisations, as it is easier to protect and prevent than to deal with the impacts after the fact. This skill set covers the following skills:

- run vulnerability assessments and basic penetration tests to identify potential threats to an organisation
- minimise risk and remediate vulnerabilities to confirm that the security of an organisation is maintained
- plan for and develop a response plan for cyber security incidents
- gather data from various sources, analyse, and interpret information for threats, inconsistencies and discrepancies.

Completion of this skill set will allow learners to pursue the following roles: network penetration testers, information and technology security consultants, and network and security consultants who work in organisation environments.

Glossary of Common Terminology

| Common Vulnerabilities and Exposures (CVE) | CVE provides a reference-method for publicly known information security vulnerabilities and exposures. |
| Legislative requirements (for Australian purposes) | May include:
| MITRE corporation | Manages federally funded research and development centers (FFRDCs) supporting several U.S. government agencies and currently sets the global standard for Common Vulnerabilities and Exposures (CVE). |
| Security Information and Event Management (SIEM) | SIEM provide real time analysis of security alerts generated by applications and network hardware. |

ICTSS00102 Cyber Incident Threat Detection and Prevention Skill Set guidance

Refer to pages 31 - 34 for the detailed interpretation of the units of competency in ICTSS00102.

The information in this Guide is offered as supplementary interpretation guidance for ICTSS00102. The interpretations and advice in this Guide are not enforceable and serve as guidance only. ASQA, VRQA and TAC are the sector regulators responsible for determining matters of compliance in relation to RTOs and training providers.
### ICTCYS404 Run vulnerability assessments for an organisation (1 of 1)

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 2. Run vulnerability assessment and penetration test | Vulnerability assessment may include:  
  ● preparing a system for a vulnerability test by referring to the Common Vulnerabilities and Exposures (CVE) list ([https://cve.mitre.org/cve](https://cve.mitre.org/cve)) to identify equipment that an organisation needs to acquire to manage vulnerabilities  
  ● vulnerability scanning and analysis, including:  
    ○ OS fingerprinting  
    ○ stimulus and response algorithms  
    ○ privileged logon ability  
    ○ cross referencing  
    ○ update capability  
    ○ reporting capability  
  ● scanner tools  
  ● host scanning, including:  
    ○ disabling unneeded services  
    ○ disabling insecure services  
    ○ ensuring least privilege file system permissions  
    ○ making sure file system permissions are as tight as possible  
    ○ establishing and enforcing a patching policy  
    ○ examining applications for weaknesses  
    ○ firewall and router testing  
  ● security monitoring testing  
  ● Intrusion Prevention Systems (IPS) security monitoring  
  ● security gateway testing  
  ● wireless network testing  
  ● wireless tools  
  ● war dialing  
  ● war driving.  

For web vulnerabilities, RTOs may consider referring to [https://owasp.org/www-project-top-ten](https://owasp.org/www-project-top-ten), which lists the top ten web vulnerabilities.

Penetration tests may include:  
  ● white box, grey box and black box penetration testing  
  ● phase 1 - penetration testing goals  
    ○ using penetration test software tools  
    ○ analysing test results  
  ● phase 2 - reconnaissance and network mapping techniques  
    ○ where reconnaissance includes:  
      ■ social engineering and low-tech reconnaissance  
      ■ mid-tech reconnaissance  
      ■ domain name system (DNS) zone transfers  
    ○ network mapping  
  ● phase 3 - information evaluation and risk analysis  
  ● phase 4 - active penetration  
  ● phase 5 - analysis and reporting. |
## ICTCYS405 Develop cyber security incident response plans (1 of 1)

### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1. Plan *incident response plans* | Incident response plans, specific to ICTCYS406, may include:  
- NIST 800-61 R2:  
  - Computer Security Incident Handling Guide.  
- Australian Government ISM - Guidelines for Cyber Security Incidents:  
  - ‘Managing Cyber Security Incidents’  
  - ‘Reporting Security Incidents’.  
  
Incident response plans, specific to ICTCYS406, may include:  
- preparation  
  - developing and/or using the incident response policy  
  - communication planning  
  - stakeholder management  
  - detection and analysis planning  
  - containment, eradication and recovery planning  
  - post incident activity planning  
- recovery and business continuity planning (post incident)  
  - business continuity planning  
  - disaster recovery planning  
  - plan testing  
  - plan review and maintenance. |

### Performance Criteria

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.1 Obtain work details and scope from required personnel and arrange for site access in compliance with required security arrangements, legislation, codes, regulations and standards | Standards may include:  
- NIST 800-61 R2:  
  - Computer Security Incident Handling Guide  
- Australian Government ISM:  
  - continuous monitoring plan  
  - security assessment report  
  - plan of action and milestones. |

### Foundation Skills

| Writing: Prepares *complex workplace documentation* detailing response plans using required structure, layout and technical programming language | Complex workplace documentation may include:  
- explanatory documentation on code, fixes and changes made  
- maintenance guides  
- troubleshooting guides  
- organisational policy documents  
- operational guides. |

### Knowledge Evidence

| Metrics and *baselines used in cyber security incident test plans* | Baselines may include:  
- best case, worst case, average case scenario  
- recovery time objective  
- recovery point objective. |
### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1. Gather threat data | Gathering threat data, specific to ICTCYS407, may include following relevant guidance documents such as:  
- NIST 800-61 R2:  
  - Computer Security Incident Handling Guide  
- NIST 800-92:  
- Australian Government ISM - Guidelines for Cyber Security Incidents:  
  - ‘Managing Cyber Security Incidents’  
  - ‘Reporting Security Incidents’  
  - ‘Guidelines for System Monitoring’. |
| 2. Analyse threat data | A centralised collection and analysis of data in a Security Information and Event Management (SIEM) system could be used to analyse threat data.  
Analyse threat data, specific to ICTCYS407, may include:  
- vulnerability scanning and analysis  
  - OS fingerprinting  
  - scanner tools  
  - host scanning  
  - security monitoring testing  
  - Intrusion Prevention Systems (IPS) security monitoring  
  - security gateway testing  
  - wireless network testing  
  - wireless tools  
  - war dialing  
  - war driving  
- penetration testing  
  - white box, grey box and black box penetration testing  
  - phase 1 – penetration testing goals  
  - phase 2 – reconnaissance and network mapping techniques  
  - phase 3 – information evaluation and risk analysis  
  - phase 4 – active penetration  
  - phase 5 – analysis and reporting. |

### Performance Criteria

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.3 Discuss and confirm data log requirements and strategy to process data with required personnel | Data log requirements may include:  
- logging stakeholder/client consent and accompanying circumstances  
- tracking access to data  
- tracking data modifications  
- logging specific activities, including:  
  - log files  
  - reviewing host logs  
    - reviewing incident logs  
    - log anomalies  
    - log management  
    - clipping levels  
    - filtering  
    - log consolidation  
  - log retention  
  - centralised logging  
  - syslog  
  - distributed log collectors  
  - hosted logging services. |

Cont'd on next page...
## ICTCYS407 Gather, analyse and interpret threat data (2 of 2)

### ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualifications</th>
<th>ICT40120 Certificate IV in Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ICT50120 Diploma of Information Technology (Elective)</td>
</tr>
<tr>
<td>Skill Set</td>
<td>ICTSS00102 Cyber Incident Threat Detection and Prevention Skill Set</td>
</tr>
</tbody>
</table>

### Unit of Competency Interpretation Summary

#### Foundation Skills

<table>
<thead>
<tr>
<th>Writing: Prepares complex workplace documentation detailing response plans using required structure, layout and technical language</th>
<th>Complex workplace documentation may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● explanatory documentation on code, fixes and changes made</td>
</tr>
<tr>
<td></td>
<td>● maintenance guides</td>
</tr>
<tr>
<td></td>
<td>● training guides and manuals</td>
</tr>
<tr>
<td></td>
<td>● troubleshooting guides</td>
</tr>
<tr>
<td></td>
<td>● organisational policy documents</td>
</tr>
<tr>
<td></td>
<td>● operational guides</td>
</tr>
</tbody>
</table>

#### Performance Evidence

<table>
<thead>
<tr>
<th>Gather, log and create dataset from a single security device or whole organisation device, including:</th>
<th>Single security devices or whole organisation devices may include Security Information and Event Management (SIEM) systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td>● basic router info</td>
<td></td>
</tr>
<tr>
<td>● firewall info</td>
<td></td>
</tr>
<tr>
<td>● systems</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identify and describe at least three different inconsistencies or discrepancies within data</th>
<th>Inconsistencies may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● deletion anomaly</td>
</tr>
<tr>
<td></td>
<td>● insertion anomaly</td>
</tr>
<tr>
<td></td>
<td>● update anomaly</td>
</tr>
</tbody>
</table>

#### Knowledge Evidence

<table>
<thead>
<tr>
<th>Basic troubleshooting processes related to cyber security threats</th>
<th>Basic troubleshooting processes may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● pre-installation of environment</td>
</tr>
<tr>
<td></td>
<td>● scans and reports of environment</td>
</tr>
<tr>
<td></td>
<td>● use of antivirus/malware software</td>
</tr>
<tr>
<td></td>
<td>● use of recovery console</td>
</tr>
<tr>
<td></td>
<td>● use of system recovery</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Common cyber security threats and their impacts on business functions</th>
<th>Common cyber security threats may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● fake security alerts</td>
</tr>
<tr>
<td></td>
<td>● file permission change</td>
</tr>
<tr>
<td></td>
<td>● file disappearance</td>
</tr>
<tr>
<td></td>
<td>● internet connectivity issues</td>
</tr>
<tr>
<td></td>
<td>● malicious browser redirection</td>
</tr>
<tr>
<td></td>
<td>● malware</td>
</tr>
<tr>
<td></td>
<td>● PC lock/access denied</td>
</tr>
<tr>
<td></td>
<td>● phishing</td>
</tr>
<tr>
<td></td>
<td>● physical threats, including data loss</td>
</tr>
<tr>
<td></td>
<td>● pop-ups</td>
</tr>
<tr>
<td></td>
<td>● renamed system files</td>
</tr>
<tr>
<td></td>
<td>● rogue antivirus</td>
</tr>
<tr>
<td></td>
<td>● slowed performance</td>
</tr>
<tr>
<td></td>
<td>● social engineering</td>
</tr>
<tr>
<td></td>
<td>● spam</td>
</tr>
</tbody>
</table>
Cyber Security Strategy and Governance Overview

The Cyber Security Strategy and Governance Skill Set incorporates specialist units of competency that support organisations in developing cyber security infrastructure and strategies in order to minimise cyber security risks and threats. This skill set covers the following skills:

- research, plan and implement cyber security standards for an organisation
- identify, confirm and implement best practices for identity management in the cyber environment to minimise threats, risks and cybercrime attacks
- identify cyber security standards and laws and evaluate an organisation’s working practices and compliance to these standards and laws as well as determine changes required to continue compliance
- conduct a risk assessment and analysis in a organisation environment
- identify and align an organisation’s operating environment to their required risk register and the realignment of their operations.

Completion of this skill set will allow learners to pursue the following roles: information and communications technology (ICT) security consultants, cyber security analysts, organisation development managers, cyber risk and assurance managers, network security consultants and administrators, cyber security solutions architects and network engineers who implement cyber security standards in organisations.

Glossary of Common Terminology

| Cyber security standards or legislation | Standards or legislation, specific to ICTSS00103, may include:
| --- | --- |
| Cyber security standards or legislation | ISO/IEC 27001 (Information technology — Security techniques — Information security management systems — Requirements)
ISO/IEC 27005 (Information security risk management)
ISO/IEC 27014 (Security Governance)
ISO/IEC 27017 (Cloud Security)
ISO/IEC 27034 (Application security).


Legislative requirements (for Australian purposes) | May include:

National Initiative for Cybersecurity Education (NICE) framework | National Institute of Standards and Technology (NIST)’s blueprint to categorise, organise, and describe cyber security work.

ICTSS00103 Cyber Security Strategy and Governance Skill Set guidance

Refer to pages 36 - 42 for the detailed interpretation of the units of competency in ICTSS00103.
## Unit of Competency Interpretation Summary

### Elements

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1. Determine cyber security needs | Cyber security needs, specific to ICTCYS601, may include:  
- applying risk-based management concepts to the supply chain  
- contributing to and enforcing personnel security policies and procedures  
- identifying or developing, and documenting security policy, standards, procedures and guidelines  
- evaluating and applying security governance principles  
- identifying, analysing and prioritising business continuity requirements  
- identifying risk management processes  
- identifying threat modelling concepts and methodologies  
- identifying legal and regulatory issues that pertain to information security in a global context  
- understanding and adhering to professional ethics. |

### Performance Criteria

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.1 Identify and document organisational cyber security needs | Organisational cyber security needs may include:  
- distributed denial-of-service (DDoS) protection  
- enterprise antivirus software  
- gateway/firewall stateful packet inspection  
- intrusion detection systems  
- intrusion protection systems  
- social engineering/phishing awareness training. |
| 1.3 Identify external cyber security standards according to organisational requirements | External cyber security standards may include the internationally recognised NICE framework by the National Institute of Standards and Technology (NIST). |
| 1.5 Distribute cyber security framework to required personnel | Required personnel may include:  
- law enforcement  
- media and public relations  
- official organisation and agencies  
- priority of stakeholders. |
| 4.3 Analyse recovery strategies according to cyber standards requirements | Recovery strategies may include:  
- backups made on tape/disk  
- hybrid cloud solutions  
- replication of data offsite  
- private cloud solutions. |

### Foundation Skills

<table>
<thead>
<tr>
<th>Notes</th>
<th>Writing: Prepares complex workplace documentation detailing processes and outcomes using required structure, layout and applicable language</th>
</tr>
</thead>
</table>
|       | Complex workplace documentation may include:  
- business continuity plan  
- disaster recovery plan  
- explanatory documentation on code, fixes and changes  
- risk assessments  
- security instructions based on organisation set up. |

### Assessment Conditions

<table>
<thead>
<tr>
<th>Notes</th>
<th>Access to: Standards for Cyber security ISO/IEC 27000 series, Information security management systems standards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standards may include NIST SP 800-37 Risk Management Framework.</td>
</tr>
</tbody>
</table>
ICTSY604 Implement best practices for identity management (1 of 3)

ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT60120 Advanced Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00103 Cyber Security Strategy and Governance Skill Set</td>
</tr>
</tbody>
</table>

Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.2 Analyse organisation’s identity management environment, processes and requirements | Identity management may include:  
- access controls  
- administering the identity management lifecycle  
  - authorisation  
  - proofing  
  - provisioning  
  - maintenance  
  - entitlement  
- access control concepts  
- applying logical access control in terms of subjects  
- applying logical access control in terms of objects or object groups  
- implementing access control  
- discretionary access control  
- rule set-based access controls  
- role based access controls  
- constrained user interface  
- content-dependent access control  
- context-based access control  
- temporal isolation (time-based) access control  
- non-discretionary access control  
- mandatory access control  
- attribute-based access control  
- separation of duties  
- security architecture and models  
- Bell-LaPadula confidentiality model  
- Biba and Clark-Wilson integrity models  
- Brewer-Nash (the Chinese wall) model  
- Graham-Denning model  
- Harrison-Ruzzo-Ullman model  
- implementing authentication mechanisms  
- subject identification  
  - methods (user ID, pin, account number)  
  - registration of new users  
  - periodic review of access levels  
  - clearance  
- authentication (proof of identity)  
  - knowledge (static passwords)  
  - ownership  
    - smart cards  
    - dynamic passwords/one time passwords  
    - tokens  
    - radio frequency identification (RFID)  
  - characteristics  
  - biometrics  
    - behavioural biometrics  
    - signature analysis  
    - voice pattern recognition  
    - keystroke dynamics  
    - physiological biometrics  
    - fingerprint verification technology  
    - hand geometry patterns  
    - vascular patterns  
    - eye features/retina. |

Cont'd on next page...
## Unit of Competency Interpretation Summary

### Elements

| 1. Analyse organisation’s identity management best practices | Best practice, specific to ICTCYS604, may include:  
| | ● access control concepts  
| | ● administering the identity management lifecycle  
| | ● authentication (proof of identity)  
| | ● authentication using kerberos  
| | ● authorisation  
| | ● comparing internetwork trust architectures  
| | ● discretionary access control  
| | ● identification  
| | ● implementing access control  
| | ● implementing authentication mechanisms  
| | ● non-discretionary access control  
| | ● role based access controls  
| | ● security architecture and models  
| | ● separation of duties  
| | ● trust direction  
| | ● user/device authentication policies. |

### Performance Criteria

| 1.3 Identify legislation and industry requirements required to implementing best practices for identity management | Industry requirements, specific to ICTCYS604, may include:  
| | ● NIST SP 800-63-3 (Digital Identity Guidelines):  
| | o SP 800-63A (Enrolment and Identity Proofing)  
| | o SP 800-63B (Authentication and Lifecycle Management)  
| | o SP 800-63C (Federation and Assertions).  
| | ● Australian Government ISM:  
| | o Authentication Hardening (page 80-84).  
| | Best practices may include:  
| | ● centralised identity management  
| | ● conditional access  
| | ● discretionary access  
| | ● elimination of high-risk systems  
| | ● elimination of orphaned accounts  
| | ● multi-factor verification  
| | ● non-discretionary access control (i.e. mandatory control)  
| | ● restricted privileged access  
| | ● role-based access  
| | ● separation of duties/data  
| | ● single sign-on. |

### Foundation Skills

| Writing: Prepares complex workplace documentation detailing processes and outcomes using required structure, layout and required language | Complex documentation may include:  
| | ● explanatory documentation on code, fixes and changes made  
| | ● maintenance guides  
| | ● operational guides  
| | ● organisational policy documents  
| | ● troubleshooting guides. |
### Unit of Competency Interpretation Summary

#### Performance Evidence

| Design, implement and analyse best practices for identity management in an organisation on at least one occasion. | Best practices may include:  
| ● auditing access to resources  
| ● avoiding privileged accounts for day-to-day operations  
| ● enforcing strong passwords  
| ● never embedding keys into code or instances  
| ● treating identity as primary security perimeter  
| ● using groups for defining permissions  
| ● using multi-factor authentication (MFA). |

#### Knowledge Evidence

| Identity management methodologies required in the cyber environment | Identity management methodologies may include:  
| ● authentication services  
| ● authorisation services  
| ● directory services  
| ● user management services. |

#### Assessment Conditions

| Access to: Hardware, software and digital devices required to undertake identity management tasks | To better assist learners to in accessing hardware, software and digital devices, trainers may consider equipment implementation requirements and authentication requirements  
| E.g. biometrics or smartcards  
| Hardware, software and digital devices may include consideration of equipment requirements for implementation if secondary authentication is required via biometric or smartcard. |
## ICT Training Package Product Listing the Unit of Competency

<table>
<thead>
<tr>
<th>Qualification</th>
<th>ICT60120 Advanced Diploma of Information Technology (Elective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Set</td>
<td>ICTSS00103 Cyber Security Strategy and Governance Skill Set</td>
</tr>
</tbody>
</table>

## Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Elements</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Research existing security standards and laws</td>
<td>Security standards and laws may include:</td>
</tr>
<tr>
<td></td>
<td>● Australian Government ISM</td>
</tr>
<tr>
<td></td>
<td>● NIST SP 800-37 Risk Management Framework for Information Systems and Organizations</td>
</tr>
<tr>
<td></td>
<td>● federal, state or territory legislation</td>
</tr>
<tr>
<td></td>
<td>● state or territory standards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performance Criteria</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4 Determine time periods and benchmarking of compliance evaluation</td>
<td>Compliance evaluation requirements may include:</td>
</tr>
<tr>
<td>requirements</td>
<td>● determining compliance requirements, including:</td>
</tr>
<tr>
<td></td>
<td>○ legal compliance</td>
</tr>
<tr>
<td></td>
<td>○ legal compliance expectations</td>
</tr>
<tr>
<td></td>
<td>○ jurisdiction</td>
</tr>
<tr>
<td></td>
<td>● understanding overall business strategy, goals, mission and objectives (including governance structure within organisations)</td>
</tr>
<tr>
<td></td>
<td>● understanding the legal and regulatory issues pertaining to information security in a global context</td>
</tr>
<tr>
<td></td>
<td>● understanding, adhering to and promoting professional ethics.</td>
</tr>
</tbody>
</table>

## Knowledge Evidence

<table>
<thead>
<tr>
<th>Principles of cyber security</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Principles may include:</td>
</tr>
<tr>
<td></td>
<td>● identify</td>
</tr>
<tr>
<td></td>
<td>● govern</td>
</tr>
<tr>
<td></td>
<td>● protect</td>
</tr>
<tr>
<td></td>
<td>● detect</td>
</tr>
<tr>
<td></td>
<td>● respond</td>
</tr>
<tr>
<td></td>
<td>● recover.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Methods of identifying cyber security incidents</th>
<th>Methods of identifying cyber security incidents may include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● reviewing excessive consumption of server memory</td>
</tr>
<tr>
<td></td>
<td>● reporting unusual behaviour from privileged users</td>
</tr>
<tr>
<td></td>
<td>● traffic sent to and from unknown locations.</td>
</tr>
</tbody>
</table>
### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Element</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **1. Prepare to perform risk assessment** | Preparing to perform a risk assessment may include:  
- evaluating and applying security governance principles, including:  
  - alignment of security functions to business strategy, goals, mission and objectives  
  - the vision, mission, and strategy  
  - governance  
  - due care  
- determining compliance requirements, including:  
  - jurisdiction  
  - legal compliance  
  - legal compliance expectations  
- understanding the legal and regulatory issues that pertain to information security in a global context  
- understanding, adhering to and promoting professional ethics. |
| **2. Perform risk assessment** | Performing a risk assessment may include:  
- developing, documenting and/or leveraging security policy, standards, procedures and guidelines, including:  
  - organisational documents  
  - policy development  
  - policy review process  
- identifying, analysing and prioritising business continuity requirements, including:  
  - using a predetermined scope and plan documentation  
  - conducting a business impact analysis  
  - developing the business continuity plan  
- contributing to and/or enforcing personnel security policies and procedures, including:  
  - key control principles  
  - candidate screening and hiring  
  - onboarding and termination process  
  - vendor, consultant and contractor agreements and controls  
  - privacy in the workplace standards and procedures  
- understanding and applying risk management processes, including:  
  - risk management framework  
  - risk assessment methodologies  
- understanding and applying threat modelling concepts and methodologies, including:  
  - threat modelling concepts  
  - threat modelling methodologies  
- applying risk-based management concepts to the supply chain, including:  
  - understanding supply chain risks and supply chain risk management. |
### Unit of Competency Interpretation Summary

<table>
<thead>
<tr>
<th>Knowledge Evidence</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Risk assessment methodologies and processes required in cyber security** | Risk assessment methodologies may include:  
  ● identifying threats to the organisation  
  ● identifying internal and external vulnerabilities  
  ● identifying impact of vulnerabilities  
  ● understanding the likelihood of vulnerabilities being exploited. |
| **Methodologies of identifying and measuring risk culture and risk appetite in the cyber environment** | Risk culture and risk appetite may include:  
  ● behaviour of personnel which may influence risks and impact outcomes of the organisation  
  ● level of risk an organisation is willing to take to reach a goal, before the action is deemed risky. |

#### Assessment Conditions

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to: Legislative documentation required to conduct a cyber security risk assessment</td>
</tr>
</tbody>
</table>
| Legislative documentation specific to conducting a cyber security risk assessment may include:  
  ● NIST SP 800-37 (Risk Management Framework)  