



Australian Government

Department of Education, Employment and Workplace Relations

ICAICT706A Direct outsourced ICT services

Release: 1

ICAICT706A Direct outsourced ICT services

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to direct outsourced information and communications technology (ICT) services for a medium to large organisation.

The management of this new arrangement is through a contract that may include a service level agreement (SLA). Setting, tracking and managing SLAs are an important part of outsourcing relationship management (ORM) discipline.

Application of the Unit

Chief information officers in medium to large organisations apply the skills and knowledge in this unit to direct the strategic planning, risk management and security of outsourced and virtualised ICT services for their organisation.

Their job roles combine high-level management and business skills to perform strategic planning and direction of emerging and converging technologies within the ICT industry.

Licensing/Regulatory Information

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

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.</i>

Elements and Performance Criteria

1. Direct strategic planning for outsourced IT services	1.1 Identify <i>IT services to be outsourced</i> 1.2 Establish criteria for <i>outsourcing model</i> 1.3 Analyse impact on current <i>organisational environment</i> 1.4 Select an appropriate <i>business model</i> for outsourcing against identified criteria 1.5 Research appropriate <i>IT service providers (vendor evaluation)</i> against identified criteria 1.6 Develop the <i>strategic plan</i> for outsourced IT services
2. Lead risk management of outsourced IT services	2.1 Specify relevant <i>security requirements</i> 2.2 Lead development of <i>change-management strategy</i> 2.3 Negotiate performance and <i>security strategy</i> with IT service provider 2.4 Ensure risk assessment process undertaken for outsourced services complies with <i>organisational policy</i> 2.5 Ensure <i>risk mitigation</i> addresses identified risks
3. Monitor performance levels of outsourced IT service performance agreement	3.1 Develop external IT provider <i>SLAs</i> 3.2 Ensure external IT service provider agreed <i>performance levels</i> are maintained 3.3 Monitor the setting, tracking and management of SLAs as an important part of <i>outsourcing relationship management (ORM)</i> 3.4 Ensure <i>continuous improvement</i> of outsourced IT services

Required Skills and Knowledge

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

Required skills

- analytical skills to:
 - conduct enterprise resource planning and management
 - investigate a critical incident and provide recommendations and remedies
- communication skills to:
 - resolve conflict
 - prepare reports to senior management
 - present and articulate complex information and ideas clearly
 - read and interpret an organisation's reports, policies and procedures to establish and review business continuity management framework
- initiative, enterprise and problem-solving skills to:
 - act as a positive role model
 - assess vulnerabilities in organisational processes and infrastructure set-up
 - evaluate competitive technologies
 - solve problems individually and in teams in response to changing environments
 - translate a range of ideas into appropriate action
- planning and organisational skills to:
 - establish and monitor organisation's continuous improvement and planning processes
 - undertake the necessary background research for the development and monitoring of the strategic management plans
- technology skills to:
 - compare and recommend new technology solutions to improve organisational outcomes
 - evaluate complex information technology issues within the organisation's environment.

Required knowledge

- AS/NZS ISO 31000:2009 Risk management
- business continuity issues for the organisation
- organisation's current functionality, including existing data and information systems
- organisation's internal and external dependencies and interdependencies
- organisational policies and procedures, including risk management strategy
- past and current internal, external and industry disruptions
- relevant legislation and regulations that impact on business continuity, such as OHS, environment, duty of care, contract, company, freedom of information, industrial relations, privacy and confidentiality, due diligence and records management
- organisation's industry.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • develop strategic directions for outsourcing of IT resources in alignment with organisational goals • conduct risk analysis on outsourced IT services and implement procedures that identify where risk occurs and what measures need to be taken to handle the risk • produce contingency plans in cooperation with external parties • establish warning systems and an ongoing process that includes regular or programmed reviews of the risk profile of outsourced IT services • negotiate and monitor SLAs with external clients.
Context of and specific resources for assessment	Assessment must ensure access to: • relevant strategic level enterprise documentation, including planning, financial and IT infrastructure documentation • relevant legislative policies. Where applicable, physical resources should include equipment modified for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • direct observation of the candidate carrying out project work • verbal or written questioning to assess required knowledge and skills • review of reports and implementation plans • review of a portfolio of the project work undertaken. Note: The preferred assessment method is through a workplace project or through a simulated medium to large enterprise workplace.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level,

	language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.
--	---

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

<i>IT services to be outsourced</i> may include:	• backup or recovery • data cleansing • data storage • disaster recovery • hardware, software or network support • help desk • network infrastructure • programming.
<i>Outsourcing model</i> refers to:	• business model for the procurement of external services approved by the organisation • financial penalties and the right to terminate if SLAs are consistently missed • transfer of responsibility from an organisation to a supplier.
<i>Organisational environment</i> may include:	• business or management structure • conglomerate of business entities • external environment in which a business is operating, including contractors and externally provided services • specific business entity • way in which organisational members perceive and characterise their environment in an attitudinal and value-based manner.
<i>Business model</i> may include:	• broad range of formal and informal descriptions to represent core aspects of a business, including purpose, offerings, strategies, infrastructure, organisational structures, trading practices, and operational processes and policies • business, system, application, network or people in the organisation • framework or strategy to enable business targets to be met.
<i>IT service providers (vendor evaluation)</i> may include:	• individuals or organisations contracted to provide services to the organisation to achieve financial or operational targets • internal departments, external organisations, individual people and employees.
<i>Strategic plan</i> may include:	• components from separate disciplines, such as IT or human resources

	• mission, vision and values • objectives and targets • organisational environment • part of organisational strategic plan or a stand-alone document • process of the organisation's definition of its strategy or direction, and making decisions on allocating its resources to pursue this strategy, including its capital and people.
Security requirements may include:	• plans to address theft, viruses, standards (including archival, backup, network), privacy, audits, alerts and usually relate directly to security objectives of organisation • relevant government legislation, organisational security policies, customs, expertise and knowledge • system in terms of databases, applications, servers, operating system, gateways, application service provider (ASP) and internet service provider (ISP) • threats relating to eavesdropping, manipulation, impersonation, penetration, denial of service and by-pass, hackers and viruses • threats to security that are, or are held to be, present in the environment, encryption, passwords, hardware, authentication and policies.
Change-management strategy may refer to:	• benchmarks that could include technical, cost savings, performance and quality benchmarks • business, system, application, network or people in the organisation • change procedures that are verbal, documented, process-based, socially-based or incremental, and may be the result of an impact on quality, cost or OHS • department within the organisation or a third party • formal procedures that must be adhered to • stakeholders, including end user, internal or external client, government body, corporate body and community groups.
Security strategy may include:	• person within a department, a department within the organisation or a third party • privacy, authentication, authorisation and integrity, and usually relates directly to the security objectives of the organisation.
Organisational policy may refer to:	• documentation internal to the organisation that guides actions that are particular to the organisation issuing the policy, and guides processes that are most likely to achieve a desired outcome • process of making important organisational decisions, including the identification of different alternatives, such as programs or spending priorities, and choosing among them

	on the basis of the impact they will have political, management, financial and administrative mechanisms arranged to reach explicit goals.
Risk mitigation may include:	- identification of one or more potential solutions to reduce or remove each risk if it arises - implementation of policies or actions that identify risks in an existing or planned process.
SLAs may refer to:	- common understanding about services, priorities, responsibilities, guarantees and warranties - negotiated agreement between two parties where one is the customer and the other is the service provider; this can be a legally binding formal or informal 'contract' - part of a service contract where the level of service is formally defined - specific SLAs that are negotiated up front as part of the outsourcing contract, and are used as one of the primary tools of outsourcing governance.
Performance levels may refer to:	- contracted delivery time or performance of the service - levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing.
Outsourcing relationship management may refer to:	- elements of organisational structure, management strategy and information technology infrastructure - management of one or more external service providers as part of an outsourcing strategy - the three aspects of ORM that companies typically pursue as part of their outsourcing strategy: - IT infrastructure - management strategy - organisational structure.
Continuous improvement may relate to:	- efforts that seek incremental improvement over time or breakthrough improvement at once - ongoing effort to improve products, services or processes - processes that are constantly evaluated and improved in the light of their efficiency, effectiveness and flexibility.

Unit Sector(s)

General ICT