Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

Functional Area - Content Security

Title	Develop cloud disaster recovery strategy
Code	108061L5
Description	This unit of competency applies to all Digital Media Technology (DMT) practitioners responsible for digital content security. Cloud computing is vulnerable to the same genetic flaws that plagues traditional IT operations: Everything fails (servers, networks) sooner or later, not to mention human mistakes and failure. When this happens there will be lots of unhappy users and customers. Protecting the organisation from unplanned downtime is widely dependent on building redundancy and diversity directly into the disaster recovery (DR) and business continuity strategy. Cloud strategy is unique to every orgnaisation which depends of cloud strategy adopted (private cloud, hybrid or public cloud).
Level	5
Credit	3
Competency	Performance Requirements 1. Knowledge for developing cloud disaster recovery strategy • Possess good project management and business strategies formulation skills • Possess in-depth knowledge of risk and impact analysis techniques • Possess in-depth knowledge of information security and business continuity • Possess in-depth knowledge of traditional DR and cloud DR technologies • Possess good knowledge of cloud and virtualisation DR methodology • Possess good knowledge of business analytic tools • Possess good knowledge of the organisation infrastructure and operation workflow 2. Developing cloud disaster recovery strategy • Perform risk assessment and business impact analysis on the orgnaisation when loss of cloud systems and loss of contents. For example: o Impact to the production and customer on loss of cloud infrastructure components o Content security, control effects on Digital Rights Management (DRM) and Digital Asset Management (DAM) system o Financial impacts when cloud payment systems and customer records are incapacitated o Reputation of the organisation • Determine Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) during the business impact analysis • Determine DR model/approaches based on RTO and RPO needs, such as: o Hot site (mirrored cloud) or active/active approach ▪ Absolutely minimal downtime ▪ Expensive, mirrored site/cloud running continuously ▪ Synchronisation issues with multi-cloud providers o Warm or cold site active/passive ▪ Some downtime is allowed, but not prolonged ▪ Less expensive and can be adopted under a “pay-as-you-use” cloud model ▪ Still have issues with bring the data current o Cloud backup-based recovery ▪ Downtime is not a major factor – but the application, or workload is still very important and needs to be brought up quickly

	▪ Cloud services replicate data, applications or other services to a cold VM-based backup • Determine the additional network bandwidth required to support the DR strategy • Determine cost and additional resources required for the implementation of DR strategy. Additionally the DR strategy needs to complement the other security and business continuity aspects of the organisation • Document and present strategy to management for support 3. Exhibit professionalism • Apply industry best practices when developing cloud DR strategy • Always take into consideration and strike a proper balance among all related technological, political, social, environmental, business and legal factors
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform a complete risk assessment and business impact analysis of the organisation’s cloud infrastructure and contents with their RTO and RPO • Determine the best DR approach to adopt which can minimise downtime of the organisation cloud infrastructure and the contents hosted at the cloud systems • Present and gain support from management to implement the DR strategy
Remark	