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

Functional Area - Content Security

Title	Formulate Digital Rights Management (DRM) strategy for business
Code	108060L6
Description	This unit of competency applies to all Digital Media Technology (DMT) practitioners responsible for digital content security. Digital Rights Management (DRM) is a systematic approach to copyright protection for digital media. The purpose of DRM is to prevent unauthorised redistribution of digital media and restrict the ways customers can copy content they have purchased. But there are well known issues and barriers which organisations need to surmount before implementing DRM.
Level	6
Credit	3
Competency	Performance Requirements 1. Knowledge for formulating DRM strategy for business • Possess good project management and business strategies formulation skills • Possess in-depth knowledge of information and cyber security • Possess good knowledge of digital media security and business operations • Possess in-depth knowledge of Digital Rights Management (DRM) • Possess good knowledge of content security & content development lifecycle 2. Formulate DRM strategy for business • Determine how better use DRM for business, for example: o Servers can be set to block the forwarding of content o Server can control access to copying of and printing of material based on constraints set by the copyright holder of the content o Movie studio limits the number of copies a user can make o Encryption technology can be used as a form of licensing • Categorise the organisation's media contents and evaluate different DRM technologies to protect them • Perform gap analysis to determine how DRM ready the organisation is for adoption of DRM technologies o Content – Amount of time and effort needed to convert and prepare contents for DRM control o Production workflow – How many production systems needed to be updated or replaced to enable produced contents to automatically be controlled by DRM systems o Delivery systems – Can one DRM system control delivery of all the contents or multi-system is required o Inter-operability with different customer devices o Evaluate the effects it will have on customers and agents o Proprietary or open DRM technologies to adopt • Define DRM components needed for implementation. For example: o IP Asset Creation and Capture ▪ Right creation ▪ Right validation o IP Asset Management ▪ Repository functions ▪ Trading functions (payments, licenses) o Permissions Management o Tracking Management

Functional Area - Content Security

	• Define policies
	  ○ Content rights (protection rules)
	  ○ Staff (DRM knowledge update, training, procedures, responsibilities)
	  ○ DRM monitoring
	  ○ Reporting and reviews
	• Define implementation schedule with estimation and breakdown of implementation cost
	
	3. Exhibit professionalism
	• Apply industry standards and best practices when formulating and establishing security polices, such as ISO27000 standards family
	• 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: • Critically evaluate and determine the most applicable content security approach that matches the organisation business • Formulate a complete set of metadata for the organisation's contents that can be used by content management tools • Create a concise and precise content security policy that can protect the organisation's asset (contents) with complete sets of guidelines for implementation which all stakeholders can adhere to
Remark	