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

Functional Area - Content Security

Title	Formulate DRM implementation plan
Code	108062L5
Description	This unit of competency applies to all Digital Media Technology (DMT) practitioners responsible for digital content security. Protecting data in storage and transit is no longer enough. The ability to share contents for business collaboration such as merger and acquisition plans, employee data or documents outlining the next product line with employees, partners and customers on intranets, extranets and the Internet requires the extra level of protection that require granular and flexible control that only DRM (Digital Rights Management) can offer. To avoid negativity, careful planning of DRM implementation is necessary.
Level	5
Credit	3
Competency	Performance Requirements 1. Knowledge for formulating DRM implementation plan • Possess good project management and communication skills • Possess in-depth knowledge of developing implementation plans • Possess in-depth knowledge of information and cyber security • Possess in-depth knowledge of Digital Rights Management (DRM) technologies and trends • Possess good knowledge of DRM lifecycle • Possess good knowledge of digital media content security and business operations • Possess good knowledge of pros and cons of DRM systems 2. Formulate DRM implementation plan • Familiarised with the DRM business strategy and goals, for example: o Control access to copying and use of the organisation's assets o Limit the number of copies users can make o Track users' habits and personal information • Determine the organisation digital media contents and create a matrix of contents against "protection rights/ rules" (e.g. no. of downloads, no. of copied, opened, licensed period, etc.) to apply. Clarify with stakeholders on the type of contents and DRM protection rules • Determine the type of DRM solution to implement after considering its pros and con, such as: o Software platform o Hosted service (cloud) o Application that include DRM capabilities • Determine components of DRM needed to implement, such as: o Content creation and capture management o Asset management (payment system, license control system) o Permission management o Tracking management • Determine and develop DRM systems sourcing criteria guidelines, such as but not limited to the following : o Standard or proprietary based cryptography algorithm o How keys are distributed, authenticated, revoked, and renewed o Does it work with all kind of content or multi-DRM is needed o Can it support the range of current customers devices o How well it handles contents sent between users at different organisations

Functional Area - Content Security

	○ How well it integrates with existing security systems, such as: ▪ Web server and portal ▪ Database and content repositories ▪ Email systems ▪ Billing systems ▪ Security logs ○ How many of the features are performed automatically • Identify possible DRM systems and vendors that can supply the required systems • Draft implementation plan with schedules and milestones. Also develop procedures for implementation teams to follow • Seek comments from various stakeholders and refine implementation plan, if required 3. Exhibit professionalism • Apply industry standards and best practices to implement DRM systems, such as ISO 27000 standards family • Committed to protect the organisation's properties
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Fully grasp and confirm the organsiation's DRM business strategy • Identify the type of DRM system that is best fit to be implemented to protect the organisation's contents • Create a DRM sourcing guideline with all the expected sourcing criteria • Develop a representative implementation plan fulfilling all stakeholders' expectation and achieve the organisation's business goals
Remark	