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

Functional Area - Information Security

Title	Evaluate the results of application security assessment for improvement recommendation
Code	111173L5
Range	Evaluate the results of application security assessment and propose possible directions for security improvement.
Level	5
Credit	3 （For Reference Only）
Competency	Performance Requirements 1. Knowledge of the requirements of application security assessment • understand the basic principles, methodologies and tools in the application security assessment process (e.g. RASP, MAST) • appreciate the objectives of the security assessment • understand the requirements and goals of the security assessment of the organization 2. Evaluate the results of application security assessment • any security weaknesses and vulnerabilities in source code • any security weaknesses in architecture, design, open source and third-party components • consolidate the impacts from possible application security risks in qualitative and quantitative terms • properly document the evaluation results 3. Propose possible directions for improvement • develop a structured plan to coordinate security improvements in according to the organization's guidelines and requirements • propose best practices for security assessment • develp training programmes for internal staff to upgrade their competency
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： • critically evaluate the results of application security assessment • propose possible directions for security improvement in according to the organization's guidelines and requirements
Remark	