Unit of Competency

Functional Area: Operational Support & Services

Title	Develop information security policies
Code	105638L6
Range	This unit of competency is applicable to those who are responsible for developing information security policies to protect customer records. It involves analyzing record flow in day-to-day operations, prioritizing sensitivity of records, identifying potential risks and loopholes, developing internal control mechanism and record handling guidelines.
Level	6
Credit	5 (for reference only)
Competency	Performance Requirements 1. Possess knowledge in information security • Familiar with operations of different business units • Fully aware of relevant regulatory requirements on information security • Alert to trends and developments in information security 2(a). Develop information security policies • Work with business units to analyze the data flow in day-to-day operations • Consolidate types of customer data to be processed • Prioritize the sensitivity of data • Identify potential risks and loopholes in data processing, e.g. unauthorized accesses • Assess the implications of regulatory requirements on data processing in day-to-day operations • Introduce internal control mechanism to protect data from identified risks • Develop record handling guidelines for relevant staff members 2(b). Introduce information security policies • Educate staff members on information security policies • Ensure staff members comply with the policies 2(c). Monitor effectiveness of information security policies • Work with business units to review the appropriateness and effectiveness of information security policies, as well as the compliance of staff members towards the policies • Pay attention to latest developments in information security • Improve information security policies as necessary 3. Ensure information security policies effectively protects data from risks and loopholes in day-to-day operations • Ensure policy effectively addresses the risks and loopholes in customer records processing • Ensure staff members well understand the significance of data protection and support information security policies • Improve information security policies in light of staff feedback and latest developments in information security.
Assessment Criteria	The integrated outcome requirements of this unit of competency are: • Able to identify potential risks and loopholes in customer data processing • Able to develop information security policies • Able to develop data handling guidelines for relevant staff members.
Remark	This unit of competency is also applicable to general insurers, life insurers and broker.