Specification of Competency Standards for the Retail Banking

## Unit of Competency

### Technology Management > 5.1 Information and Cyber Security

| | |
|---|---|
| Title | Perform incident response management for IT, digital banking and financial technology issues |
| Code | 107423L5 |
| Range | Manage incidents broken out in cyber systems. This applies to different kinds of incidents arising in different types of IT systems and digital platforms |
| Level | 5 |
| Credit | 4 |
| Competency | Performance Requirements<br>1. Investigate security incidents<br>Be able to:<br>• Detect and identify security incidents in technology systems<br>• Analyse security incidents and conduct investigation on technology security<br>• Design different measures to collect necessary data related to the incidents in order to find out the truth<br>• Respond to any report of security violations and carry out investigation to diagnose the causes<br>2. Formulate solutions to tackle security incidents<br>Be able to:<br>• Direct contingency or recovery plan for minimizing damages of technology security incidents promptly<br>• Devise response procedures the incidents<br>• Oversee the writing of report on technology security incidents for record and documentation<br>• Conduct post-incident follow up and carry out necessary remedial actions to ensure security of the bank systems or databases |
| Assessment Criteria | The integral outcome requirements of this UoC are:<br>• Investigation on security incidents in order to find out the causes. The investigation should be based on the analysis of the data collected |
| Remark | |