Technology and Operations > IT System Security

Title	Perform incident response management during encounter of security risk
Code	106759L5
Range	Manage incidents broken out in IT systems. This applies to different kinds of incidents arising in different types of IT systems.
Level	5
Credit	4 (for reference only)
Competency	Performance Requirements 1. Investigate security incidents Be able to: • Detect and identify security incidents in technology systems • Analyze security incidents and conduct investigation on technology security • Design different measures to collect necessary data related to the incidents in order to find out the truth • Respond to any report of security violations and carry out investigation to diagnose the causes 2. Formulate solutions to tackle security incidents Be able to: • Direct contingency or recovery plan for minimizing damages of technology security incidents promptly • Devise response procedures for the incidents • Oversee the writing of report on technology security incidents for record and documentation • Conduct post-mortem review and follow up as well as carry out necessary remedial actions to ensure security of the bank systems or databases
Assessment Criteria	The integral outcome requirements of this UoC are: • Investigation on security incidents in order to find out the causes. The investigation should be based on the analysis of the data collected • Recommendation of solutions to contain the damage caused by the incident. These should be based on evaluation on findings from investigation and analysis on information from different sources.
Remark	