

Specification of Competency Standards
for the Banking Industry
Unit of Competency

Functional Area - 6. Technology Management
(Key Function – 6.2 IT System Security/ Cybersecurity)

Title	Conduct security risk assessment and audit of different IT systems and suggest mitigation strategies
Code	109368L5
Range	Assessment of security risks in IT systems. This applies to different kinds of IT systems including Blockchain, Artificial Intelligence (AI), Big Data collection and storage, etc. and covers the assessment of different kinds of risks.
Level	5
Credit	4 (For Reference Only)
Competency	<p>Performance Requirements</p> <p>1. Knowledge in the Subject Area</p> <p>Be able to:</p> <ul style="list-style-type: none"> • Understand risk exposure of different IT systems and apply the knowledge to evaluate risk assessment framework of the bank to develop comprehensive understanding on the procedures in measuring different kinds of security risks which the bank is potentially exposed to; • Understand the functions and features of different risk assessment mechanisms and apply the knowledge to evaluate common methods in risk assessment adopted by the bank. <p>2. Applications</p> <p>Be able to:</p> <ul style="list-style-type: none"> • Measure risks on systems and networks for identifying hazards and potential loss of unauthorized access; and identify possible areas which may threaten information security of the bank; • Make judgment and adjust the assessment procedures when necessary in order to ensure smooth operations and fulfilment of the stated objectives; • Identify potential IT security weaknesses and recommend remedial improvement measures; • Communicate the identified risks in IT security with related business and operation units and recommend any changes in the system to enhance the security. <p>3. Professional Behaviour and Attitude</p> <p>Be able to:</p> <ul style="list-style-type: none"> • Develop comprehensive precautionary measures which can safeguard the bank from potential loss arising from the breaching of security of business information by customers or business partners; • Summarise the findings of assessment and report the risk potentials and remedial recommendations on different IT systems to relevant parties.
Assessment Criteria	<p>The integral outcome requirements of this UoC are:</p> <ul style="list-style-type: none"> • Presentation of report on security risks assessment. The report should outline clearly the risks levels of different systems, high risks areas and measures to mitigate risks identified; • Execution of the risks assessment procedures (risk measurement, identification and reporting, etc.) in IT system according to the bank's risk assessment framework and make necessary adjustment during the course to ensure smooth operation.

Specification of Competency Standards
for the Banking Industry
Unit of Competency

Functional Area - 6. Technology Management
(Key Function – 6.2 IT System Security/ Cybersecurity)

Remark	
--------	--