Functional Area: Network Infrastructure & Operation (Security)

1. Title	Define network security plans
2. Code	ITCSNO429A
3. Range	As networks are getting more and more complex and network users are getting more and more sophisticated, they expect reliabilities and continuous connectivity from the operator's network. Security of the whole network infrastructure and all its components are essential factors to ensure an optimal operation of the network. This UoC describes the competencies for defining network security plan. Security considerations include: hackers, fraudulent users, or even careless staff, etc.
4. Level	4
5. Credit	3
6. Competency	Performance Requirement 6.1 Possess the knowledge in the subject area • Knowledgeable of the organisation's policies regarding network security • Knowledgeable of the network infrastructure and the services that it supports • Experienced with security principles and best practices • Possess extensive experience with risk management principles and be able to identify different network security components • Experienced with project planning and management techniques • Possess knowledge of health and safety rules and hazards regarding network infrastructure 6.2 Define network security plans Be able to: • Perform security assessment of the organisation's "asset" to determine the level of risk and vulnerability • Perform identification of suitable network security components for securing the organisation's assets, such as: physical security, network security, access control, authentication, encryption, key management, or just plain security awareness, etc • Budget for the project should line up roughly with expectations to secure the exposures uncovered in the initial assessment • Formulate a deployment program of security technologies (firewall, Intrusion Detection Systems, etc) and security components. Manpower requirements should also be included • Formulate measuring and monitoring procedures, with benchmarks, on each network security control • Formulate security contingency plan by performing impact analysis to delineate tolerable downtime for each network and service. This task should be aligned with the organisation's disaster recovery and business continuity strategies • Document the security plan and present to appropriate stakeholders for seeking approval 6.3 Exhibit professionalism • Ensure all documents are produced conforming to organisation standards • Always take into consideration and strike a proper balance among all related technological, environmental and legal factors
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: i. define network security vulnerabilities and assess where these vulnerability exist in the organisation's network ii. formulate security plans to strengthen and counter the risk areas of the network iii. design tools that can measure the effectiveness of the security plans iv. identify cost of implementing the security plans v. effectively document, present and make recommendation of suitable security plan to stakeholders and seek approval for implementation
Remark	