Functional Area: Network Infrastructure & Operation (Security)

1. Title	Define access control in network systems	
2. Code	ITCSNO531A	
3. Range	A network is a common means of connecting devices and sharing resources. A network system is a mesh of interconnected devices on a LAN, WAN or MAN. Controls are required to manage authorised access to the network system. This UoC describes the competencies for defining access control to network systems from a telecommunicate services provider perspective i.e. controls at "Access network" level.	
4. Level	5	
5. Credit	4	
6. Competency		Performance Requirement
	6.1 Possess the knowledge in the subject area	• Possess extensive knowledge of the organisation access and security policies • Extensively experienced with the organisation's security framework or international standards regarding security framework e.g. ISO 17799 • Experienced with the organisation network infrastructure (hardware and software components) • Possess extensive experience with security principles, mitigation techniques, implementation of controls and best practices • Expert in analysing and identifying various security risks, such as possible methods of attacks on signalling layer, database of subscribers, network elements, gateways, frauds, and service interruptions, etc. • Fully comprehend the network access requirements of products and services • Knowledgeable of health and safety rules and hazards.
	6.2 Define access control in network systems	Be able to: • Work with the network support team to identify security risks • Group and rank the risks into three areas. The three areas to be considered are: Physical, Technical and Administrative • Define security controls for the three areas: *Physical Controls*: Security measures used to deter unauthorized access to the physical network using physical means, such as security guard, closed circuit TV, locks, etc. *Technical controls*: managing access without using physical structures, such as Encryptions, SIM cards, Network Authentication, etc. *Administrative*: defines human factors security determining which users have access to which resources: level of access, personal registration and accounting, training and awareness, separation of duties, disaster preparedness, etc. • Define benchmarks for measuring the controls. • Define monitoring and measuring procedures/plans. This procedure should also indicate the duties and responsible person for each control (i.e. define ownership) • Document the controls with what precautionary actions to take and remedies for security breaches • Distribute the security control document to appropriate stakeholders. Arrange briefings and presentations to ensure full comprehension of the contents and responsibilities

	6.3 Exhibit professionalism • Ensure the defined protections are inline with the organisation security policies • 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. communicate effectively with colleagues to determine the network access security risks; and rank the levels of risk ii. identify and formulate correct controls to enable legitimate authorised access is made to the network and unauthorised access is prevented iii. design effective monitoring and measuring functions or procedures that can measure the effectiveness of the controls so that weaknesses are countered and amended with speed iv. use appropriate means, such as training and documents, to ensure stakeholders are aware of these controls and able to put these control into operational use
Remark	