Functional Area: Network Infrastructure & Operation (Security)

1. Title	Maintain "white list" or "black list" for mobile account access to the network	
2. Code	ITCSNO334A	
3. Range	A telecom operator will require stringent control on allowing authorised mobile equipment to access its network and keep unauthorised users out. This can be done in the form of "Whitelist", "Graylist" and "Blacklist" using IMEI (International Mobile Equipment Identity) of the device and EIR (Equipment Identity Registrar) of the mobile network system. This UoC describes the competencies for maintaining the lists to control mobile account access to the network. Work required includes maintaining local internal EIR which will be synchronised with CEIR (Central Equipment Identity Registrar) database. It is assumed that the IMEI is manually entered via OSS (Operational Support System).	
4. Level	3	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Possess the knowledge in the subject area	• Possess extensive knowledge of security policies, operation principles and best practices • Possess extensive experience with mobile telecommunication systems and security access control • Extensively knowledgeable of how and when "whitelist", "graylist, and "blacklist" is used within the organisation's mobile network • Knowledgeable of OSS functions, particularly in the area of security control • Experienced in operating OSS control systems with commands or other scripting or programming languages • Knowledgeable of the industry standards and regulatory requirements for handling mobile security
	6.2 Maintain "white list" or "black list" for mobile account access to the network	Be able to: • Work with colleagues to determine the schedules for whitelist, blacklist, that perform entry of device serial number (IMEI) or database maintenance update • Use OSS tools to add newly reported lost phone to the local EIR • Perform synchronisation of local EIR with CEIR and produce report of discrepancies or abnormalities • Reconcile the differences between the two databases and make appropriate adjustments to local EIR after verification of reported lost phones, new subscribers, mapping of IMEI with SIM card ID, etc. Follow required procedures to amend CEIR • Bring suspected anomalies to the attention of appropriate security parties or supervisors • Document and record actions taken to local EIR and CEIR when discrepancies were found • Acquire work completion sign off from supervisors or job controllers
	6.3 Exhibit professionalism	• Follow the heath and safety guidelines of the organisation while operating OSS systems • Follow the security policies of the organisation to prevent unauthorised access of the network and comply with the industry and regulatory standards.

7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: i. follow work schedule to maintain the EIR "whitelist", "blacklist" ii. analyse unsynchronised lists iii. follow the security policies to report anomalies and reconcile the differences after investigation iv. use the OSS functions effectively to synchronised EIR and CEIR databases v. effectively document the work and obtain signoff by supervisor or work controller
Remark	Local EIR database contains the operator's registered users reported lost equipment. CEIR contains the international list of reported lost phones or equipment If an automated program is created then more in-depth technical knowledge is required such as the need to understand the API (Application Programming Interface) of CEIR and EIR management functions of OSS (Operation Support System)