SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
TECHNICAL SKILLS & COMPETENCIES (TSC) REFERENCE DOCUMENT

TSC Category	Development and Implementation					
TSC Title	Security Assessment and Testing					
TSC Description	Conduct threat modelling, vulnerability assessment and penetration testing to reveal vulnerabilities or lapses in the existing systems or security mechanisms and evaluate the extent to which systems are able to protect the organisation's data and maintain functionality as intended					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		ICT-DIT-2012-1.1	**ICT-DIT-3012-1.1**	**ICT-DIT-4012-1.1**	**ICT-DIT-5012-1.1**	
		Execute vulnerability scans and conduct research on exploitation of system vulnerabilities, and interpret findings to identify security lapses	Conduct authorised penetration testing of systems and to expose threats, vulnerabilities and potential attack vectors in systems	Design security testing plan, and perform advanced, authorised penetration testing as well as intelligence analysis on cyber attack incidents	Authorise and establish organisation guidelines and strategies for security testing, and determine the future-readiness of the organisation's security posture	
Knowledge		• Application and usage of basic vulnerability assessment tools and tests • General process and technical requirements of penetration testing • System security vulnerabilities and threats • Internal and external security standards	• Process and techniques for secured source code review • Threat modelling techniques • Penetration testing techniques and methodologies • Penetration testing tools and their usage • Network monitoring tools and their usage • Vulnerability assessment tests and interpretation of results • Range and types of security loopholes and threats	• Organisational objectives of vulnerability assessment and penetration testing • Key components and methodologies in the design of security testing activities • Advanced threat modelling, hacking, penetration testing and source code review techniques • Data and trend analysis in cyber attacks	• Design guidelines and best practices for threat modelling, vulnerability assessment, penetration tests and source code review • Organisation priorities and IT security objectives • New and emerging trends in cyber attacks, hacking techniques and security threats	
Abilities		• Perform technical coordination of vulnerability assessments and penetration testing according to test plan templates • Execute vulnerability scans on smaller systems, using basic	• Carry out threat modelling and secured source code review • Conduct authorised penetration testing of systems consisting of a range of penetration testing methodologies, tools and techniques	• Design security testing plan and evaluation criteria for vulnerability assessments and penetration testing activities • Manage the implementation of vulnerability assessments and	• Establish organisation guidelines and methodologies for the design and conduct of vulnerability assessments and penetration testing activities • Lead security reviews, specifying the IT	

		vulnerability assessment tools and tests • Document the results of security assessments and tests, according to test plan guidelines • Identify security lapses in the system or security mechanisms, based on issues documented from vulnerability scan results • Record evidence of controls which are inadequate or not duly enforced • Conduct research on threat actors, their techniques and ways in which vulnerabilities in security systems can be exploited	• Use a suite of network monitoring and vulnerability scanning tools to assess the threats and vulnerabilities in a system • Identify vulnerability exploitations and potential attack vectors into a system • Analyse vulnerability scan results to size and assess security loopholes and threats • Evaluate if current systems can overcome emerging threats and hacking techniques • Assess current security practices and controls against expected performance parameters or guidelines • Develop a vulnerability assessment and penetration testing report, highlighting key threats and areas for improving system security	penetration testing activities, in line with the organisation-wide strategy • Implement advanced threat modelling and source code review techniques • Conduct advanced, authorised penetration testing of highly complex and secure systems • Analyse patterns in incident data to identify new and emerging trends in vulnerability exploitation and hacking techniques • Lead advanced analysis of intrusion signatures, techniques, and procedures associated with cyber attacks • Determine hacking techniques and attacks that the organisation's systems are most vulnerable to • Refine test plan templates to model after new and advanced hacking actions	systems, applications, processes, people to be assessed • Develop comprehensive criteria for assessing the effectiveness of security mechanisms and controls • Develop implementation strategies for vulnerability and penetration testing activities to ensure organisation-wide consistent of information security plans • Authorise penetration testing activities on organisation's systems, in line with business priorities and security requirements • Synthesise key organisational implications from vulnerability assessment and penetration testing reports • Evaluate the future-readiness of the organisation's security posture in light of the organisation's mission and the changing technological environment	
Range of Application						