SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – VULNERABILITY ASSESSMENT AND PENETRATION TESTING ANALYST				
Sector	Infocomm Technology			
Track	Cyber Security			
Sub-track	Vulnerability Assessment and Penetration Testing			
Occupation	ICT Security Specialist			
Job Role	**Vulnerability Assessment and Penetration Testing Analyst**			
Job Role Description	The Vulnerability Assessment and Penetration Testing Analyst designs and performs tests and check cases to determine if infrastructure components, systems and applications meet confidentiality, integrity, authentication, availability, authorisation and non-repudiation standards. He/She translates requirements into test plan, writes and executes test scripts or codes in line with standards and procedures to determine vulnerability from attacks. He certifies infrastructure components, systems and applications that meet security standards. The Vulnerability Assessment and Penetration Testing Analyst is well versed with cyber security standards, protocols and frameworks, has a creative and analytical mind, and deploys new and innovative methods to perform penetration tests. He works well in a team and communicates findings and implications effectively to relevant stakeholders.			
Critical Work Functions, Key Tasks and Performance Expectations	**Critical Work Functions**	**Key Tasks**	**Performance Expectations**	
	Establish cyber security policies	Assist in the development of cyber security standards, policies and best practices	In accordance with: • Cyber Security Act 2018 by the Cyber Security Agency of Singapore	
		Assist in establishing certification based policies for maintaining compliance to cyber security standards		
		Conduct reviews and assessment of existing security policies, procedures, standards and exceptions		
	Oversee vulnerability assessment and penetration testing (VAPT) activities	Carry out scoping activities to identify systems components which require testing		
		Define and translate requirements into test plans, scenarios, scripts or procedures		
		Conduct VAPT, black box and code reviews, and reverse engineering		
		Perform on-site security assessments of infrastructure components and computer systems		
		Propose recommendations for continuous improvement of testing processes and methodologies		
		Identify emerging security and risk management trends, issues, and alerts in VAPT activities		
	Manage VAPTs	Prepare reports on VAPT results based on established guidelines		
		Provide inputs on security penetration testing in the development of software and applications		
		Review software designs, source codes and deployment to address cyber security issues		
		Prepare documentation to facilitate certification of software		
		Maintain repositories for certification documentation and modifications		
Skills and Competencies	**Technical Skills and Competencies**		**Generic Skills and Competencies**	
	Audit and Compliance	Level 3	Digital Literacy	Advanced
	Cyber Risk Management	Level 4	Computational Thinking	Advanced
	Emerging Technology Synthesis	Level 4	Sense Making	Advanced

Effective date: January 2020, Version 2.1

	Learning and Development	Level 4	Transdisciplinary Thinking	Intermediate
	Network Security	Level 4	Problem Solving	Advanced
	Security Assessment and Testing	Level 4		
	Security Strategy	Level 4		
	Stakeholder Management	Level 3		
	Strategy Implementation	Level 3		
	Strategy Planning	Level 4		
	Test Planning	Level 4		
	Threat Analysis and Defence	Level 4		
Programme Listing	For a list of Training Programmes available for the ICT sector, please visit: www.skillsfuture.sg/skills-framework/ict			

The information contained in this document serves as a guide.

Effective date: January 2020, Version 2.1