SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
SKILLS MAP – SECURITY OPERATIONS ANALYST

Sector	Infocomm Technology
Track	Cyber Security
Sub-track	Security Operations
Occupation	ICT Security Specialist
Job Role	**Security Operations Analyst**
Job Role Description	The Security Operations Analyst performs real-time analysis and trending of security log data from various security devices and systems. He/She maintains data sources feeding the log monitoring system, develops and maintains detection and alerting rules. He responds to user incident reports and evaluates the type and severity of security events. He documents incidents and develops reports. He identifies recurring security issues and risks to develop mitigation plans and recommends process improvements. He interprets and applies security policies and procedures. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays. He is familiar with cyber security standards, protocols and frameworks, and works in accordance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security monitoring and testing tools and techniques. The Security Operations Analyst is diligent and takes an analytical approach to perform real-time analyses. He is skilled in synthesising trends and insights, and is confident in putting forth creative mitigation plans and solutions to security incidents.

Critical Work Functions, Key Tasks and Performance Expectations	**Critical Work Functions**	**Key Tasks**	**Performance Expectations**
	Monitor cyber security systems	Carries out audits, reviews, security control assessments, and tests of security operations based on established schedules and protocols	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
		Perform real-time analysis and trending of security log data from cyber security systems	
		Analyse security event data to identify suspicious and malicious activities	
		Provide inputs to improve security monitoring rules and alerts	
		Document processes related to cyber security monitoring	
	Maintain cyber security operations	Implement cyber security protocols	
		Formulate emergency response procedures	
		Maintain data sources feeding the log monitoring system	
		Schedule security checks in accordance with reporting schedules	
		Prepare periodic status reports for presentation to management	
	Manage response to cyber security incidents	Review security incident reports	
		Analyse the type and severity of cyber security incidents	
		Assist in establishing procedures for handling detected cyber security incidents	
		Provide status updates during the lifecycle of a cyber security incident	
		Prepare final incident report detailing the events of the cyber security incident	
		Support the maintenance and update of business recovery, contingency plans and procedures	

Skills and Competencies	**Technical Skills and Competencies**		**Generic Skills and Competencies**	
	Audit and Compliance	Level 3	Communication	Intermediate

	Business Continuity	Level 4	Creative Thinking	Intermediate
	Cyber and Data Breach Incident Management	Level 3	Problem Solving	Intermediate
	Cyber Risk Management	Level 4	Sense Making	Intermediate
	Disaster Recovery Management	Level 4	Teamwork	Intermediate
	Network Security	Level 3		
	Security Administration	Level 3		
	Security Programme Management	Level 4		
	Stakeholder Management	Level 3		
	Threat Analysis and Defence	Level 4		
	Threat Intelligence and Detection	Level 3		
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.