SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – THREAT ANALYSIS MANAGER			
Sector	Infocomm Technology		
Track	Cyber Security		
Sub-track	Threat Analysis		
Occupation	ICT Security Specialist		
Job Role	**Threat Analysis Manager**		
Job Role Description	The Threat Analysis Manager plans out strategies to pre-empt potential threats in an organisation's cyber related systems. He/She is responsible for identifying the IT assets that are prone to cyber threats and attacks. He proactively monitors the open web and identifies potential threats and groups or individuals capable of attempting cyber-attacks. He runs tests and analyses different areas of the IT assets to ensure they are safe from cyber-attacks. He is familiar with cyber security standards, protocols and frameworks. He is knowledgeable in using various cyber security analysis tools and techniques to monitor and identify potential incidents. The Threat Analysis Manager is alert and vigilant in performing monitoring activities, and is able to analyse and identify potential security-related issues, which may have critical impact on security and operational systems. He communicates clearly in his interactions with others and coordinates effectively with his team to perform security operations.		
Critical Work Functions, Key Tasks and Performance Expectations	**Critical Work Functions**	**Key Tasks**	**Performance Expectations**
	Assess organisational assets for potential cyber threats	Develop and implement strategies to identify assets prone to cyber threats and attacks	In accordance with: • Cyber Security Act 2018 by the Cyber Security Agency of Singapore
		De-construct the architecture of applications to uncover potential threats and vulnerabilities in the design, implementation, deployment or configuration of the application and systems	
		Conduct in-depth analysis of existing threats and identify existing gaps in the current cyber security set-up	
		Provide advice on the design and implementation of security policy and controls on identified assets	
		Evaluate and provide feedback to improve intelligence production, intelligence reporting, collection requirements, and operations	
	Research and pro-active monitoring of threats and attacks	Run continuous scans and monitor threats that may exist in the dark web and external web-based applications	
		Conduct research on new and existing threats that may impact existing IT systems	
		Identify potential attacker groups or individuals and take preventive measures	
		Recommend and develop approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists	
		Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives related to designated cyber operations warning problem sets	
	Classifying threats and simulating attacks on systems and applications	Identify potential threats that may affect applications and systems using the knowledge of the application and system vulnerabilities	
		Run test attacks and simulations on the systems to identify the possibilities of threats and extent of damage it could cause	
		Prioritise and rate identified threats based on its severity	

		Provide timely notice of imminent or hostile intentions or activities which may impact organisation objectives, resources, or capabilities	
		Use existing database of threats and attack histories to pre-empt and classify potential new threats	
	Implement and document threat mitigation strategies and protocols	Document new threats based on a core set of attributes to develop threat mitigation protocols	
		Provide guidance on threat mitigation strategies and potential threats and cyber-attacks to ensure current cyber security standards and set-up are updated	
		Analyse intelligence and support designated exercises, planning activities, and time-sensitive operations	
		Provide evaluation and feedback to improve intelligence production, reporting, collection requirements and operations.	
	Manage people and organisation	Manage the budget expenditure and allocation across teams and projects	
		Monitor and track the team's achievements and key performance indicators	
		Propose new operational plans, including targeted budgets, work allocations and staff forecasts	
		Acquire, allocate and optimise the use of resources	
		Develop learning roadmaps to support the professional development of the team	
		Manage the performance and development process, including providing coaching and development opportunities to maximise the potential of each individual	

Skills and Competencies	**Technical Skills and Competencies**		**Generic Skills and Competencies**	
	Audit and Compliance	Level 4	Virtual Collaboration	Intermediate
	Budgeting	Level 5	Transdisciplinary Thinking	Advanced
	Business Performance Management	Level 4, Level 5	Problem Solving	Advanced
	Cyber and Data Breach Incident Management	Level 5	Leadership	Advanced
	Cyber Risk Management	Level 5	Global Mindset	Advanced
	Emerging Technology Synthesis	Level 5		
	IT Standards	Level 5		
	Learning and Development	Level 5		
	Manpower Planning	Level 4, Level 5		
	Network Security	Level 4		
	Networking	Level 4		
	People and Performance Management	Level 4		
	Security Architecture	Level 4		
	Security Assessment and Testing	Level 5		
	Security Programme Management	Level 5		
	Security Strategy	Level 5		
	Stakeholder Management	Level 5		

	Strategy Implementation	Level 4	
	Strategy Planning	Level 5	
	Threat Analysis and Defence	Level 5	
	Threat Intelligence and Detection	Level 5	
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 1.1