SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
SKILLS MAP – PRODUCT SECURITY ENGINEERING MANAGER

Sector	Infocomm Technology
Track	Product Development
Sub-track	Quality, Risk and Security
Occupation	Product Security Specialist
Job Role	**Product Security Engineering Manager**

Job Role Description	The Product Security Engineering Manager guides the assessment of information and cyber risks associated with product development and provides recommendations on control requirements by risk policy and standards. He/She manages and coordinates responses to regulatory inquiries, inspections, audits and ensures cyber security standards and policies are established and implemented. He oversees the development of reports and implements policies and standards, as well as provide strategic direction on the monitoring and maintenance of security operations and incident response. He manages employees and is held accountable for the performance and results of a team. He guides security measures and protocols to stakeholders. He is familiar with cyber security standards, protocols, and frameworks, and ensures the organisation's compliance with the Cyber Security Act 2018. He uses various cyber security monitoring and analysis tools and techniques depending on the organisation's needs and requirements. He also uses cyber risk mitigation strategies and protocols to solve cybersecurity issues in products The Product Security Engineering Manager is sharp, analytical and anticipates cyber security risks in products to mitigate them ahead of time. He is an excellent communicator and promotes a cooperative working environment and relationships within and beyond his team.

	Critical Work Functions	Key Tasks	Performance Expectations
Critical Work Functions, Key Tasks and Performance Expectations	Implement cyber security risk strategy for products	Manage the strategic development and improvement of risk frameworks, methodologies, and requirements for products	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
		Recommend strategies to address key risk areas in cyber security for each product	
		Assess business needs for product launch against cyber security concerns and legal and/or regulatory requirements	
		Provide strategic risk guidance to stakeholders in the implementation and execution of cyber risk strategies for products pre-launch and post-launch	
		Manage the strategic development and improvement of cyber security risk frameworks, methodologies and requirements	
	Establish cyber security standards and policies for products	Formulate governance procedures for documenting and updating security policy, standards, guidelines and procedures for products	
		Plan the implementation of information systems and cyber security policies on products	
		Develop the organisation's Cyber Risk Maturity model in application to product launches	
		Develop policies and frameworks for conducting cyber security risk assessments and compliance audits on products	
	Manage cyber risks and assessments	Advise the development of techniques and procedures for the conduct of cyber risk assessments on products	
		Develop plans for cyber risk assessment activities on products	
		Coordinate the ongoing cyber risk assessment activities for existing and new products	
		Provide strategic and technical recommendations following identification of vulnerabilities in operating systems	

		Incorporate emerging security and risk management trends, issues, and alerts into the risk assessment framework into product upgrades and new products
		Advise the development of techniques and procedures for the conduct of cyber risk assessments on products
	Mitigate cyber security risks and respond to cyber security incidents	Develop programmes and initiatives to strengthen the capability to mitigate risks in existing products and new launches
		Oversee prioritisation of alerts and resources for incident responses on products
		Oversee the planning and conduct of organisational cyber security exercises for products
		Act as a subject matter expert in cyber security incident and breach investigations and post-breach remediation work
		Propose procedures to prevent future incidents and improve cyber security in products
	Manage people and organisation	Review operational strategies, policies and targets across teams and projects
		Develop strategies for resource planning and utilisation
		Review the utilisation of resources
		Oversee the development of learning roadmaps for teams and functions

	Technical Skills and Competencies		Critical Core Skills	
Skills and Competencies	Audit and Compliance*	Level 4	Decision Making	Intermediate
	Cyber and Data Breach Incident Management*	Level 4	Developing People	Intermediate
	Cyber Risk Management*	Level 5	Problem Solving	Advanced
	Data Analytics*	Level 4	Sense Making	Intermediate
	Data Governance*	Level 4	Transdisciplinary Thinking	Intermediate
	IT Governance*	Level 5		
	Learning and Development*	Level 4		
	Manpower Planning*	Level 4		
	Network Security*	Level 5		
	Networking*	Level 4		
	Partnership Management*	Level 4		
	People and Performance Management*	Level 4		
	Security Administration*	Level 4		
	Security Education and Awareness*	Level 5		
	Security Governance*	Level 5		
	Security Programme Management*	Level 4		
	Agile Software Development	Level 4		
	AI Ethics and Governance	Level 3		
	Applications Development	Level 4		
	Budgeting	Level 5		
	Business Continuity	Level 5		

	Business Needs Analysis	Level 4
	Cyber Forensics	Level 3
	Process Improvement and Optimisation	Level 4
	Product Management	Level 3
	Quality Standards	Level 4
	Software Design	Level 4
	Software Testing	Level 4
	Stakeholder Management	Level 4
	Strategy Implementation	Level 4
	Strategy Planning	Level 5
	Test Planning	Level 4
	Threat Analysis and Defence	Level 3
	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.

*Note: Technical Skills and Competencies (TSCs) with an asterisk (*) refer to Priority Skills (i.e., TSCs to be prioritised for this role).