SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
SKILLS MAP – CHIEF INFORMATION SECURITY OFFICER

Sector	Infocomm Technology
Track	Cyber Security
Occupation	ICT Security Specialist
Job Role	**Chief Information Security Officer**
Job Role Description	The Chief Information Security Officer develops and drives the vision for the information security function. He/She acts as the authority for the development and enforcement of organisation security strategy, standards and policies, and has ultimate responsibility for ensuring the protection of corporate information. He guides the design and continuous improvement of the IT security architecture and Cyber Risk Maturity Model that balances business needs with security risks. He advises the board and top executives on all security matters and sets directions for complying with regulatory inquiries, legal and compliance regulations, inspections and audits. He is an expert in cyber security compliance standards, protocols and frameworks, as well as the Cyber Security Act 2018. He is keeps abreast of cyber-related applications and hardware technologies and services, and is constantly on the look-out for new technologies that may be leveraged on to enhance work processes, or which may pose as potential threats. The Chief Information Security Officer is an inspirational and influential leader, who displays sound judgement and decisiveness in ensuring that corporate information is well protected and secured. He is strategic in his approach toward resource management and capability development among his teams.

	Critical Work Functions	**Key Tasks**	**Performance Expectations**
Critical Work Functions, Key Tasks and Performance Expectations	**Formulate information security strategy**	Establish the organisational cyber security vision, strategy and underlying cyber security initiatives or programmes	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
		Align information security and information risk management strategy with business strategy	
		Provide strategic, budgetary and administrative advice for implementation of information security strategy	
		Drive security awareness and education on information security throughout the organisation	
		Advise senior management and key stakeholders on information security matters	
	Establish security architecture	Oversee the development of information security and risk management policies, disaster recovery and business continuity plans	
		Evaluate current information security practices to ensure compliance with IT standards and industry norms	
		Oversee the implementation of appropriate plans to ensure compliance with regulatory, industry and regional mandates	
		Establish and implement cyber security legal risk rules and guidelines in line with industry norms and standards	
		Drive information security and risk management awareness training programmes	
	Establish security architecture	Oversee the design of cyber security architecture and the overall Cyber Risk Maturity Model	
		Establish Key Performance Indicators (KPIs) to assess the effectiveness of the security architecture	
		Facilitate the development of a framework to measure the effectiveness of security programmes	
		Review security architecture to ensure that it addresses technology shifts and threats	
	Manage cyber security incidents	Act as a subject matter expert in cyber security investigations and analysis	
		Drive resolution of large scale security incidents	
		Lead the development of plans to address system vulnerabilities	
		Advise on responses to regulatory inquiries, inspections or audits	

		Present evidence for legal action arising from cyber security incidents	
	Manage cyber security risks	Oversee the development of cyber security risk assessment frameworks	
		Advise business stakeholders on the different types of cyber risks and incidents along with the cyber security compliance standards	
		Oversee the development and testing of disaster recovery and business continuity plans	
		Drive compliance with international and national information security and privacy regulations	
		Act as the organisation's liaison with external agencies in cyber security risk matters	

Skills and Competencies	**Technical Skills and Competencies**		**Generic Skills and Competencies**	
	Audit and Compliance	Level 5	Leadership	Advanced
	Budgeting	Level 6	Global Mindset	Advanced
	Business Continuity	Level 6	Decision Making	Advanced
	Business Needs Analysis	Level 5	Transdisciplinary Thinking	Advanced
	Business Performance Management	Level 6	Sense Making	Advanced
	Business Risk Management	Level 6		
	Cyber Forensics	Level 6		
	Cyber and Data Breach Incident Management	Level 6		
	Cyber Risk Management	Level 6		
	Disaster Recovery Management	Level 6		
	Emerging Technology Synthesis	Level 6		
	IT Standards	Level 6		
	Learning and Development	Level 6		
	Manpower Planning	Level 5		
	Network Security	Level 5		
	Networking	Level 5		
	Partnership Management	Level 6		
	People and Performance Management	Level 5		
	Security Architecture	Level 5		
	Security Governance	Level 6		
	Security Strategy	Level 6		
	Stakeholder Management	Level 6		
	Strategy Planning	Level 6		
	Threat Analysis and Defence	Level 6		
	Threat Intelligence and Detection	Level 6		

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.