SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY
SKILLS MAP – CYBER RISK MANAGER

Sector	Infocomm Technology
Track	Cyber Security
Sub-track	Governance Risk and Control
Occupation	ICT Security Specialist
Job Role	**Cyber Risk Manager**
Job Role Description	The Cyber Risk Manager guides the assessment of information and cyber risks associated with technology initiatives 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. He manages employees and is held accountable for the performance and results of a team. He provides guidance on security measures and protocols to stakeholders. He is familiar with cyber security standards, protocols and frameworks, and ensures the organisation's compliance to the Cyber Security Act 2018. He is knowledgeable in using various cyber security monitoring and analysis tools and techniques depending on the organisation's needs and requirements. He also has expertise in cyber risk mitigation strategies and protocols. The Cyber Risk Manager has a sharp, analytical mind and is able to anticipate problems and risks to mitigate them ahead of time. He is an excellent communicator who works well with others 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**	Manage the strategic development and improvement of risk frameworks, methodologies and requirements	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
		Recommend strategies to address key risk areas in cyber security	
		Assess business needs against cyber security concerns and legal and/or regulatory requirements	
		Anticipate internal and external business challenges and legal or regulatory issues	
		Provide strategic risk guidance to stakeholders in the implementation and execution of cyber risk strategies across the organisation	
	Establish cyber security standards and policies	Formulate governance procedures for documenting and updating security policy, standards, guidelines and procedures	
		Plan the implementation of information systems and cyber security policies	
		Develop the organisation's Cyber Risk Maturity model	
		Develop policies and frameworks for conducting cyber security risk assessments and compliance audits	
	Manage cyber risks and assessments	Advise the development of techniques and procedures for the conduct of cyber risk assessments	
		Develop plans for cyber risk assessment activities across the organisation	
		Coordinate the on-going cyber risk assessment activities across the organisation	
		Provide strategic and technical recommendations following identification of vulnerabilities in operating systems	
		Incorporate emerging security and risk management trends, issues, and alerts into risk assessment framework	
		Develop cyber risk mitigation strategies and policies for the organisation	
	Develop cyber risk documentation	Oversee the development of documentation on methodologies and tools to mitigate cyber risks	
		Establish guidelines for reporting outcome of cyber risk assessments	

		Oversee the development of internal threat awareness reports	
		Present threat awareness reports to technical and non-technical staff	
	Mitigate cyber security risks	Develop programmes and initiatives to strengthen the capability of the organisation to mitigate risks	
		Oversee the planning and conduct of organisational cyber security exercises	
		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	
		Monitor the maintenance of the cyber security operations training plans for all security staff	
		Manage responses to regulatory inquiries, inspections or audits	
	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	
		Establish performance indicators to benchmark effectiveness of learning and development programmes against best practices	
		Implement succession planning initiatives for key management positions	

Skills and Competencies	**Technical Skills and Competencies**		**Generic Skills and Competencies**	
	Audit and Compliance	Level 4	Computational Thinking	Advanced
	Budgeting	Level 5	Digital Literacy	Advanced
	Business Needs Analysis	Level 4	Global Mindset	Advanced
	Business Performance Management	Level 5	Sense Making	Advanced
	Cyber and Data Breach Incident Management	Level 4	Creative Thinking	Advanced
	Cyber Forensics	Level 4, Level 5		
	Cyber Risk Management	Level 5		
	IT Governance	Level 5		
	Learning and Development	Level 4, Level 5		
	Manpower Planning	Level 4		
	Networking	Level 4		
	People and Performance Management	Level 4		
	Security Administration	Level 4		
	Security Architecture	Level 4		
	Security Education and Awareness	Level 5		
	Security Governance	Level 5		
	Security Programme Management	Level 5		
	Security Strategy	Level 5		

	Stakeholder Management	Level 4, Level 5	
	Strategy Implementation	Level 4	
	Strategy Planning	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.