SKILLS FRAMEWORK FOR FINANCIAL SERVICES SKILLS MAP - TECHNOLOGY, INFORMATION AND CYBERSECURITY RISK MANAGER		
Sector	Financial Services	
Track	Risk, Compliance and Legal	
Occupation	Technology, Information and Cybersecurity Risk Officer	
Job Role	**Technology, Information and Cybersecurity Risk Manager**	
Job Role Description	The Technology, Information and Cybersecurity Risk Manager guides the assessment of technology, information and cybersecurity risks associated with technology initiatives and provides recommendations for risk controls. He/She manages and coordinates the ongoing monitoring of technology initiatives, ensures sufficient risk preparedness activities are conducted and facilitates incident resolution. He acts as a technical non-financial risk expert within the organisation to ensure regulatory compliance and risk coverage is in place. The Technology, Information and Cybersecurity Risk Manager's duties may require him to be contactable after work hours. He has a keen understanding of current and emerging technology and digital developments. He has a sharp and analytical mind, and is able to anticipate problems and risks 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 and Key Tasks	**Critical Work Functions**	**Key Tasks**
	Maintain technology, information and cybersecurity risk policies and frameworks	Develop programmes and initiatives to strengthen the organisation's capabilities in technology, information and cybersecurity and to mitigate risks
		Set governance procedures for documenting and updating technology policies, standards, guidelines and procedures
		Document and implement procedures for technology, information system or cybersecurity breach incidents and post-breach activities
		Facilitate Information Technology (IT) personnel's operational implementation of technology, information and/or cybersecurity frameworks
		Recommend strategies to address key risk areas based on assessments of business needs against security concerns and legal/regulatory requirements
	Monitor and assess technology, information and cybersecurity risk exposure and preparedness	Lead the conduct of risk and control assessments, system assessments and stress testing to identify organisational risk profiles
		Review organisational assessments and augment security controls and internal security systems with vendors and internal Information Technology (IT) personnel
		Analyse technology, information and cybersecurity risk metrics to address emerging risks
		Implement routine technology, information and cybersecurity risk monitoring activities
		Assess risks in new digital initiatives and business units' technology usage
		Provide strategic and technical recommendations following identification of vulnerabilities within IT systems
		Review existing risk monitoring mechanisms to reflect changing trends, regulations and industry best practices
	Manage technology, information and cybersecurity risks	Develop operationalisation plans for technology, information and cybersecurity risk management and mitigation activities
		Provide subject matter expertise regarding technology, information and cybersecurity incidents, breach investigations and post-breach corrective activities
		Review and refine cybersecurity risk management activities carried out by cybersecurity operations centres
		Propose procedures to prevent future incidents and improve technology, information and cyber risk management
		Ensure continual training and conduct of initiatives to increase awareness on technology, information and cybersecurity risk topics
		Identify and implement technology assurance mechanisms through obtaining adequate insurance coverage
	Facilitate technology, information and cybersecurity incident resolution	Oversee and operationalise technology, information security and/or cybersecurity breach crisis management processes
		Develop risk incident scenarios to guide resolution planning
		Engage with IT personnel to align technical processes with technology management strategies
		Provide suggestions to address system vulnerabilities and deficiencies in technology, information and cybersecurity risk controls
		Draft organisational responses to regulatory inquiries, investigations and/or audits
		Support legal and/or regulatory investigations into large-scale technology, information and cybersecurity risk breach incidents
		Facilitate change management activities and prepare for incident resolution activities

Effective Date: August 2019, Version 1.1

	Technical Skills and Competencies		Generic Skills and Competencies (Top 5	
Skills and Competencies	Business Continuity Planning	Level 4	Problem Solving	Intermediate
	Business Risk Assessment	Level 4	Digital Literacy	Advanced
	Contract and Vendor Management	Level 4	Computational Thinking	Advanced
	Crisis Management	Level 4	Communication	Intermediate
	Cybersecurity	Level 4	Sense Making	Intermediate
	Data Collection and Analysis	Level 4		
	Data Governance	Level 4		
	Emerging Technology Synthesis	Level 4		
	Ethical Culture	Level 4		
	People Performance Management	Level 4		
	Policy Implementation and Revision	Level 4		
	Risk Appetite and Goals Setting	Level 4		
	Risk Management	Level 4		
	Risk and Compliance Reporting	Level 4		
	Scenario Planning and Analysis	Level 4		
	Security Governance	Level 5		
	Stakeholder Management	Level 4		
	Standard Operating Procedures Development	Level 4		
	Strategy Planning	Level 4		
	Technology Application	Level 3		
Programme Listing	For a list of Training Programmes available for the Financial Services sector, please visit: www.skillsfuture.sg/skills-framework/financial-services			

The information contained in this document serves as a guide.