SKILLS FRAMEWORK FOR FINANCIAL SERVICES
SKILLS MAP - HEAD OF TECHNOLOGY, INFORMATION AND CYBERSECURITY RISK MANAGEMENT

Sector	Financial Services
Track	Risk, Compliance and Legal
Occupation	Technology, Information and Cybersecurity Risk Management Officer
Job Role	**Head of Technology, Information and Cybersecurity Risk Management**
Job Role Description	The Head of Technology, Information and Cybersecurity Risk Management develops and drives risk management efforts for technology, information and cybersecurity within the organisation. He/She leads the enforcement of technology, information and cybersecurity risk models, standards and policies in collaboration with Information Technology (IT) personnel. He works with stakeholders to define risk appetites, identify risk exposure, and ensure preparedness for technology, information or cyber risk incidents. He manages risk control and incident resolution activities and independently challenges front line defence activities. The Head of Technology, Information and Cybersecurity Risk Management may be required to be contactable after work hours. He has sound judgement and is decisive, ensuring the organisation is protected and secured. He thinks strategically and keeps abreast of the latest technology trends and their impact. He is comfortable working with various stakeholders and communicating with them in a non-technical manner.

Critical Work Functions and Key Tasks	**Critical Work Functions**	**Key Tasks**
	Maintain technology, information and cybersecurity risk policies and frameworks	Oversee the development of technology, information and cybersecurity risk management policies, governance, disaster recovery and business continuity plans
		Oversee the implementation of plans to ensure compliance with regulatory, industry and regional mandates
		Define procedures for technology, information system and/or cybersecurity breach incidents and post-breach activities
		Incorporate emerging security and risk management trends, issues, and alerts in risk assessment frameworks
		Direct the design of risk maturity models and accompanying risk frameworks and policies for control measures
	Monitor and assess technology, information and cybersecurity risk exposure and preparedness	Plan and oversee the conduct of stress-testing and organisational risk assessments
		Critique existing security architecture to address technology shifts and threats
		Assess the effectiveness of risk maturity models and frameworks based on assessment findings
		Plan and oversee routine monitoring activities for organisational technology, information and cybersecurity risks
		Identify critical assets and core systems for risk management
		Ensure identified risk deviations, risk exposures and vulnerabilities in Information Technology (IT) systems are addressed
		Identify and drive periodic updates to risk monitoring mechanisms to reflect changing trends, regulations and industry best practices
	Manage technology, information and cybersecurity risks	Oversee the implementation of technology risk mitigation and risk management activities
		Drive compliance with international and national technology, information and cybersecurity and privacy regulations
		Collaborate with industry stakeholders and experts on methods for managing technology risks within the industry
		Develop training and awareness strategies to upskill and guide the organisation on managing technology, information and cybersecurity risks
		Ensure sufficient insurance coverage as part of the organisation's technology risk assurance mechanisms
	Facilitate technology, information and cybersecurity incident resolution	Plan technology, information security and/or cybersecurity breach crisis management processes
		Manage risk incident resolution activities based on identified scenarios
		Provide subject matter expertise in technology management and incident resolution processes
		Lead the development of plans to address system vulnerabilities and deficiencies in technology risk controls
		Guide and draft responses to regulatory inquiries, inspections and/or audits in relation to technology, information and cybersecurity incident resolution
		Act as key liaison for external-facing large-scale technology, information and/or cybersecurity breach incidents
		Gain senior management's buy-in and support for change management activities for managing incident resolution

	Technical Skills and Competencies	**Generic Skills and Competencies (Top 5)**

Effective Date: August 2019, Version 1.1

Skills and Competencies	Business Continuity Planning	Level 5	Digital Literacy	Advanced
	Business Risk Assessment	Level 5	Leadership	Advanced
	Contract and Vendor Management	Level 5	Communication	Advanced
	Crisis Management	Level 5	Decision Making	Advanced
	Cybersecurity	Level 5	Lifelong Learning	Advanced
	Data Collection and Analysis	Level 5		
	Data Governance	Level 5		
	Data Storytelling and Visualisation	Level 4		
	Emerging Technology Synthesis	Level 5		
	Ethical Culture	Level 5		
	People Performance Management	Level 5		
	Policy Implementation and Revision	Level 5		
	Risk Appetite and Goals Setting	Level 5		
	Risk Management	Level 5		
	Risk and Compliance Reporting	Level 5		
	Scenario Planning and Analysis	Level 5		
	Security Governance	Level 6		
	Stakeholder Management	Level 5		
	Standard Operating Procedures Development	Level 5		
	Strategy Planning	Level 5		
	Technology Application	Level 4		
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.