OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY COMPETENCY FRAMEWORK

OCTOBER 2021

Effective Date: 8 October 2021 version 1.1

CONTENTS

Effective Date: 8 October 2021 version 1.1

1 INTRODUCTION

The Operational Technology Cybersecurity Competency Framework (OTCCF) aims to guide key stakeholders in the following ways:

- OT and IT system owners can refer to the OT cybersecurity capabilities required to attract the right people, train them adequately, and map out their career pathways;
- Training providers can refer to the technical competencies required by different job roles and be guided to develop best-in-class courses and certifications that cater to local training needs; and
- OT professionals or potential jobseekers can identify skillsets for cross- and up-skilling for a meaningful career in the OT cybersecurity domain. The career pathways could apply to job roles inclusive of vertical and lateral advancement opportunities.

The OTCCF - jointly developed by CSA and Mercer Singapore, and supported by SkillsFuture Singapore (SSG) and Infocomm Media Development Authority (IMDA) - maps out the various OT cybersecurity job roles and the corresponding technical skills and core competencies required. It also captures the possible career pathways showing the options for vertical and lateral progression. It is made up of three key components:

a) Career Pathways
The Career Pathways show the possible options for vertical and lateral progression for advancement and growth.

b) Skills Maps
The Skills Maps cover the job roles, critical work functions, key tasks and skills and competencies.

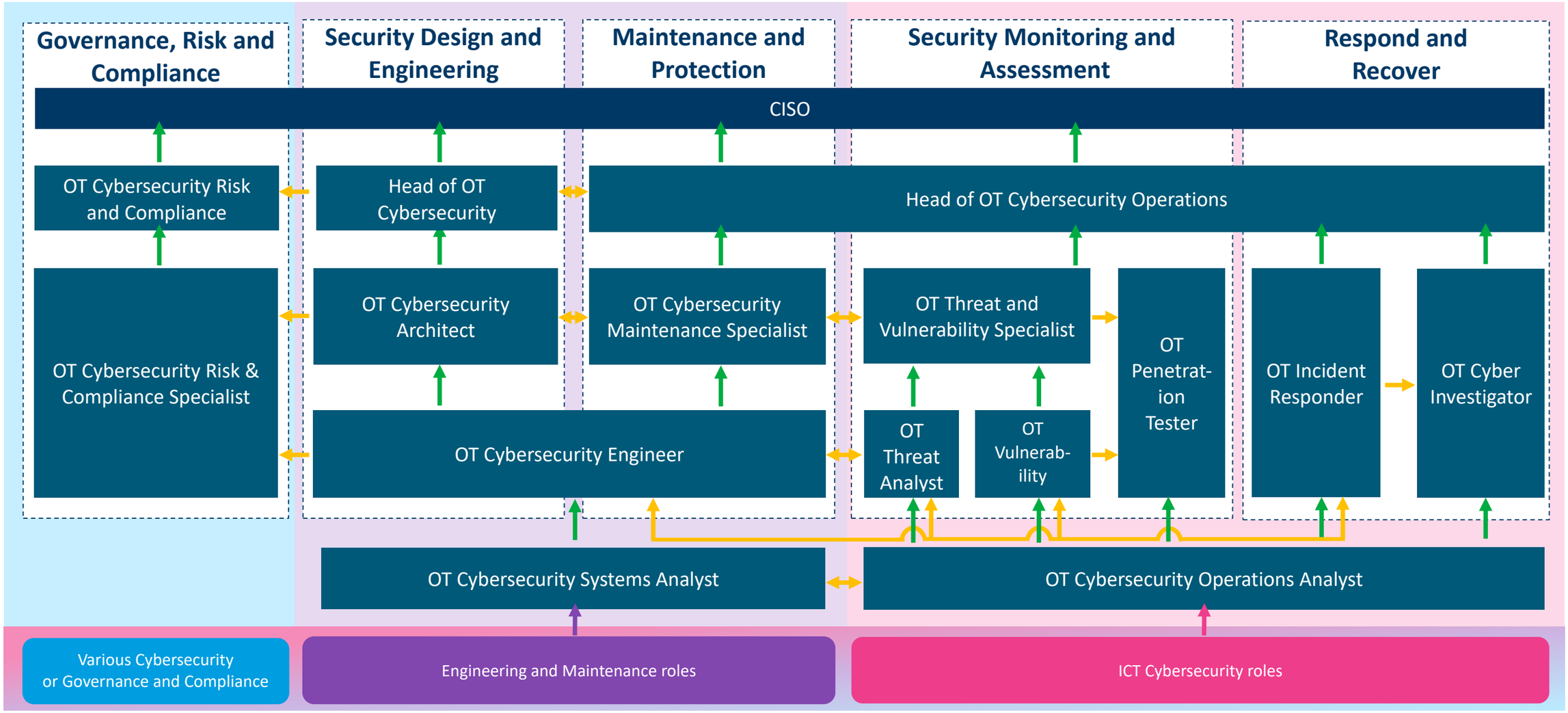
c) Skills and Competencies
Competencies identified for each of the job roles fall under two broad classifications:

(i) Technical Skills and Competencies; and

(ii) Critical Core Skills (previously known as Generic Skills and Competencies) *.

*See https://www.skillsfuture.gov.sg/skills-framework/criticalcoreskills

2 Career Map



Examples*:
- Governance
- Risk Analysts
- Compliance
- Audit

Examples*:
- Maintenance Engineer
- Network Engineer
- Systems Engineer
- Product Security Engineer
- R&D Engineer

Examples*:
- Vulnerability Testing
- Forensic Investigation
- Incident Investigation
- Threat Analysis

**The examples shown above are some of the potential job functions or job roles which serve as advantageous entry points for upskilling and/or cross-training in the OT cybersecurity sector.*

3 Skills Map

Track	**Maintenance and Protection**		
Occupation	**OT Cybersecurity Maintenance Specialist**		
Job Role	**OT Cybersecurity Maintenance Specialist**		
Job Role Description	OT Cybersecurity Maintenance Specialists lead maintenance and administration efforts across OT systems by utilising their strong understanding of OT systems and environment. They work with cybersecurity and operational personnel to develop and/or deploy mitigation techniques in order to effectively defend against cyber threats and vulnerabilities within the OT environment. They have deep understanding of security technologies such as firewall logs, IDS, endpoint security solutions, access control systems, and other related security technologies within the OT environment. They also work with the cybersecurity team to conduct research to develop or deploy new capabilities and solutions.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Discover and manage organisation's OT assets	Verify OT assets discovery process and asset inventory, commissioning and decommissioning.	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Outline OT assets and network diagram to ensure visibility	
		Develop change management processes to authorise and validate OT system changes	
		Work with cybersecurity personnel to identify appropriate asset management solutions for deployment and implement security controls to mitigate associated risks	
		Establish security validation processes and assessment on OT assets for compliance against established baselines	
		Establish, review or update configuration baselines for inventoried assets in order to drive cybersecurity objectives	
	Improve and maintain cybersecurity posture of OT systems	Define the patching and control needs of the organisation's OT system and perform prioritisation of activities	
		Oversee implementation of controls or patches and ensure minimisation of disruption within acceptable limits of risks	
		Partner with operational and cybersecurity personnel to plan and monitor periodic maintenance of OT security infrastructure	

		Implement encryption of OT assets for data in transit and data in rest		
		Conduct OT security posture assessment and upkeeping		
		Establish authentication and identification rules across devices and users to drive cybersecurity objectives within the OT environment		
		Monitor third party and vendor's access and activities in the OT environment		
	Enhance IT-OT alignment and collaboration	Promote knowledge sharing in both the IT and OT cybersecurity teams		
		Develop standardised vocabulary for IT and OT cybersecurity teams based on the identified standards and framework		
		Articulate potential pain points and solutions in aligning IT and OT departments		
		Manage cross-team strategic projects according to guidance from the senior leadership		
		Work with the cybersecurity team to conduct research to develop or deploy new capabilities and solutions.		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Access and Control Management	4	Communication	Advanced
	Application Security Management	4	Developing People	Advanced
	Asset Identification and Inventory	4	Problem Solving	Advanced
	Budgeting	4	Sense Making	Advanced
	Cryptography and Encryption	4		

	Emerging Technology Synthesis	4	Building Inclusivity	Basic
	Network Administration and Maintenance	4	Communication	Basic
	Network Security and Segmentation	4	Creative Thinking	Intermediate
	OT Compliance and Assurance	3	Collaboration	Advanced
	OT Cybersecurity Education and Awareness	3	Transdisciplinary Thinking	Advanced
	OT Cybersecurity Governance and Programme Management	4		
	OT Cybersecurity Risk Assessment and Mitigation	4		
	OT Vulnerability and Patch Management	4		
	Stakeholder Management	4		
	Supply Chain Management	4		

The information contained in this document serves as a guide.

Track	**Security Design and Engineering / Maintenance and Protection**		
Occupation	**OT Cybersecurity Engineer**		
Job Role	**OT Cybersecurity Engineer**		
Job Role Description	OT Cybersecurity Engineers are responsible for performing activities with relevance to OT cybersecurity administration and maintenance in order to establish a secure OT environment. They work with cybersecurity personnel, systems owners and operational staff to implement secure system architectures, mitigate cyber threats and vulnerabilities, and perform routine activities related to the periodic review of OT systems and maintenance of security standards and procedures documentation. They are well-versed with security technologies such as firewall logs, IDS, endpoint security solutions, access control systems, and other related security technologies within the OT environment.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Develop OT cybersecurity architecture and maintain oversight	Work with architects to shape security controls, systems, remote access and architecture for the organisation's OT infrastructure according to defined requirements	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Implement and configure the IT/OT network controls to protect the OT environment	
	Maintain OT cybersecurity system integration	Perform integration activities such as design, install, configure, test, commission and handover to OT asset owners	
		Facilitate the partition of systems under considerations into zones and conduits	
	Manage quality and continuous improvement of OT cybersecurity architecture	Conduct testing and evaluation of new cybersecurity technologies and controls	
		Recommend security products, services and procedures to enhance OT system architecture designs	
	Improve and maintain cybersecurity posture of OT systems	Partner with cybersecurity and operational personnel to deploy vulnerability mitigations and patches on OT systems or compensating controls	
		Identify potential risks (operational, safety, business etc.) of implementing patches	
		Perform periodic maintenance of OT security infrastructure	
		Perform network segmentation and relevant activities to ensure network integrity is protected	

	Respond to OT cybersecurity incidents	Provide inputs to support the fulfilment of incident response processes		
		Partner with other stakeholders to shape mitigation strategies for cybersecurity threats		
	Discover and manage organisation's OT assets	Deploy appropriate asset management solutions to assist in asset discovery		
		Escalate non-compliance of configuration of assets for against established baselines throughout the assets' life cycle		
		Verify that all connected IT and OT assets in the organisation are taken into account and categorized according to criticality		
		Partner with cybersecurity and operational personnel to test or evaluate cybersecurity impact of changes to assets		
		Communicate potential vulnerabilities and attack surfaces and work with cybersecurity and operational personnel to identify and recommend security controls for mitigation		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Access and Control Management	3	Communication	Intermediate
	Application Security Management	3	Computational Thinking	Intermediate
	Asset Identification and Inventory	3	Problem Solving	Intermediate
	Business Needs Analysis	3	Sense Making	Intermediate
	Cryptography and Encryption	3	Teamwork	Intermediate
	Cyber Incident Response and Management	3		

	Emerging Technology Synthesis	3	Problem Solving	Intermediate
	Network Administration and Maintenance	3	Transdisciplinary Thinking	Intermediate
	Network Security and Segmentation	3	Communication	Intermediate
	OT Cybersecurity Governance and Programme Management	3	Sense Making	Intermediate
	OT Cybersecurity Risk Assessment and Mitigation	3	Customer Orientation	Intermediate
	OT Vulnerability and Patch Management	3		
	OT Security Design and Architecture	3		
	OT Products and Solutions Security Evaluation	3		
	Supply Chain Management	3		

The information contained in this document serves as a guide.

Track	**Maintenance and Protection / Security Monitoring and Assessment / Respond and Recover**		
Occupation	**Head of OT Cybersecurity Operations**		
Job Role	**Head of OT Cybersecurity Operations**		
Job Role Description	Heads of OT Cybersecurity Operations lead various functions of OT cybersecurity: managing system control, and system hardening as well as developing frameworks and strategies for vulnerability management, incident response and cyber forensics in the OT environment. They have deep expertise in various OT systems and processes of the organisation as well as their cybersecurity infrastructure. They also have insights on cyber response, investigation and operation recovery. They display strong leadership attributes in guiding, developing and managing resources within and across the team. They are also decisive in their nature and are able to manage senior stakeholders well.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Manage OT system control and remote access	Manage, verify and audit identities and credentials	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Evaluate logs of access and attempts to access	
		Set protocols on removable storage media usage in the OT environment	
		Define standards and guidelines on third-party and vendor and remote access	
		Collaborate with the operations team to define minimum and essential functions of OT systems	
	Improve and maintain cybersecurity posture of OT systems	Strategise and outline the vulnerability management framework for the OT environment	
		Establish and review security baseline configuration standards for operating systems, applications and network devices	
		Partner the operations team to define needs and initiatives of cryptography and encryption	
	Perform vulnerability assessment and penetration testing	Outline penetration testing strategies, plans and playbook for the organisation	

		Ensure certifications and accreditations requirement are met	
		Provide resources and improve team capabilities in conducting penetration testing and vulnerability assessments in the OT environment	
		Oversee penetration testing and vulnerability assessment activities, focusing on maintaining operations without disruption	
		Approve and track remediation plan status for identified vulnerabilities	
		Recommend policy changes based on the findings from the penetration testing and vulnerability assessment exercise	
	Respond to OT cybersecurity incidents	Develop incident response framework, threshold and plans for OT cybersecurity incidents	
		Establish structure, roles and responsibilities for OT cybersecurity incidents response activities	
		Establish the chain of events and processes to be followed for OT cybersecurity incidents	
		Correlate OT cyber incidents to network and system activities	
		Collaborate with legal department and authorities for prosecution and investigation processes where necessary	
	Manage business continuity and recovery	Establish the organisation's recovery time and point objectives	
		Tailor recovery solutions based on organisation's needs	
		Define the organisation's OT system back up needs and protocols	
		Endorse the development of business continuity frameworks in relation to OT cybersecurity threats perspective	
		Evaluate business continuity and recovery plans to ensure they are updated	

		Assign roles and responsibilities in implementing business continuity and recovery plans	
		Spearhead the execution of business continuity and recovery plans	
	Enhance IT-OT alignment and collaboration	Champion cross skilling and collaboration programmes across IT and OT teams	
		Define the cybersecurity standards and frameworks to be used by both IT and OT cybersecurity teams	
		Streamline policies, tools and processes for OT and IT cybersecurity team	
		Anticipate resistance to changes in work processes and develop solutions to address	
		Identify areas or strategic projects that improve IT-OT alignment, cross skilling and improve the organisation cybersecurity capability	
	Lead people and organisation	Collaborate with broader cybersecurity stakeholders and teams to create optimal 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	
	Build a cybersecurity culture in the organisation	Drive cybersecurity awareness and training programmes across the organisation, focusing on the OT cybersecurity angle	
		Advise the organisation's senior leadership to endorse the design and implementation of cybersecurity strategies for the OT environment	
		Lead the endorsement of cybersecurity initiatives according to expertise and required regulations	
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**

	Access and Control Management	5	Communication	Advanced
	Application Security Management	4	Developing People	Advanced
	Budgeting	5	Problem Solving	Advanced
	Business Continuity and Recovery	5	Sense Making	Advanced
	Business Needs Analysis	4		
	Cryptography and Encryption	4	Decision Making	Advanced
	Cyber Forensics	5	Communication	Advanced
	Cyber Incident Response and Management	5	Developing People	Advanced
	Failure Analysis	5	Problem Solving	Advanced
	Learning and Development	5	Transdisciplinary Thinking	Advanced
	Manpower Planning	4		
	Network Security and Segmentation	5		
	OT Cybersecurity Education and Awareness	5		
	OT Cybersecurity Governance and Programme Management	5		
	OT Cybersecurity Risk Assessment and Mitigation	5		

	Penetration Testing	3		
	People and Performance Management	4		
	Stakeholder Management	4		
	Supply Chain Management	5		
	Threat Analysis and Defence	5		
	Threat Intelligence and Detection	5		
	Vulnerability Assessments	4		

The information contained in this document serves as a guide.

Track	**Security Monitoring and Assessment**		
Occupation	**OT Threat Analyst**		
Job Role	**OT Threat Analyst**		
Job Role Description	Threat Analysts perform threat hunting activities by proactively scanning logs, network traffic, SIEMs and other channels for suspicious behaviours and indicators of compromise. They identify OT assets prone to cyber threats and attacks and work with cybersecurity personnel to mitigate these threats. They monitor for potential threats actors/groups/individuals capable of attempting cyber-attacks.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Conduct threat hunting in the OT environment	Research and perform pro-active monitoring or scans of threats and attacks within the OT environment	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Search proactively for early indicators of compromise in the OT environment	
		Analyse historical information and data to identify early indicators or potential threats	
		Identify potential threat actor groups or individual activities	
		Utilise existing database of threats and attack histories to pre-empt and classify potential new threats	
		Prepare threat hunting reports and propose escalation steps or mitigation actions	
		Conduct research on new and existing threats that may impact existing OT systems	
	Provide threat intelligence	Document new threats and establish threat profile based on a core set of attributes to assist in development of threat mitigation protocols	
		Provide evaluation and feedback to improve intelligence production, reporting, collection requirements and operations.	
	Enhance IT-OT alignment and collaboration	Promote knowledge sharing of threats in both the IT and OT cybersecurity teams	
		Develop standardised vocabulary for IT and OT cybersecurity teams based on the identified standards and framework	

		Articulate potential pain points and solutions in aligning IT and OT teams or stakeholders		
		Manage cross-team strategic projects according to guidance from the senior leadership		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Emerging Technology Synthesis	3	Communication	Intermediate
	OT Cybersecurity Education and Awareness	3	Creative Thinking	Intermediate
	OT Cybersecurity Risk Assessment and Mitigation	3	Problem Solving	Advanced
	Stakeholder Management	5	Sense Making	Advanced
	Supply Chain Management	3	Collaboration	Advanced
	Threat Analysis and Defence	3		
	Threat Intelligence and Detection	3		

The information contained in this document serves as a guide.

Track	**Security Monitoring and Assessment**		
Occupation	**Threat and Vulnerability Specialist**		
Job Role	**OT Threat and Vulnerability Specialist**		
Job Role Description	OT Threat and Vulnerability Specialists oversee the OT cybersecurity monitoring activities and maintain oversight on cybersecurity threats within the OT environment, including the associated risks. They work with Penetration Testers to assess the security levels of the OT systems in the organisation without disrupting operations. They define the testing needs and environment and present the findings and remediation plans to the relevant stakeholders.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Monitor OT systems for cybersecurity incidents	Establish and update OT cybersecurity monitoring manuals, operation procedures and documentation based on organisation's and regulatory needs	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Oversee OT cybersecurity monitoring activities and propose improvements	
		Develop and maintain artificial intelligence to detect cyber attacks	
	Perform vulnerability assessments and penetration testing	Anticipate the needs and limitations of vulnerability assessments or penetration activities in the organisation's OT environment	
		Oversee security reviews, penetration testing and red team activities	
		Deliver technical presentations and recommendations to the management	
		Maintain oversight on OT cybersecurity threat landscape and identify the needs for new vulnerabilities management standards based on emerging risks	
	Conduct threat hunting in the OT environment	Develop cyber indicators to maintain awareness of the status of the OT environment	
		Work with cybersecurity personnel to run test attacks and simulations on the systems to identify the possibilities of threats and extent of damage it could cause on OT systems	
		Provide subject matter inputs on cyber threats in the OT environment	
	Provide threat intelligence	Analyse intelligence and shape designated exercises, planning activities, and time-sensitive operations to develop cyber-resiliency	

		Identify and assess the capabilities and activities of cybersecurity criminals or foreign intelligence entities, and produce findings to help initialise or support law enforcement and counterintelligence investigations or activities		
	Improve and maintain cybersecurity posture of OT systems	Present threat hunting reports and work with cybersecurity personnel to establish mitigation actions		
		Provide guidance on threat mitigation strategies and potential threats and cyber-attacks to ensure current cyber security standards and set-up are updated		
	Enhance IT-OT alignment and collaboration	Promote knowledge sharing in both the IT and OT cybersecurity teams		
		Develop standardised vocabulary for IT and OT cybersecurity teams based on the identified standards and framework		
		Articulate potential pain points and solutions in aligning IT and OT teams or stakeholders		
		Manage cross-team strategic projects according to guidance from the senior leadership		
	Lead people and organisation	Collaborate with broader cybersecurity counterparts to create optimal utilisation of resources		
		Contribute to the development of learning roadmaps for teams and functions		
		Establish performance indicators to benchmark effectiveness of learning and development programmes against best practices		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skill**	
	Emerging Technology Synthesis	4	Digital Fluency	Advanced
	Failure Analysis	4	Global Perspective	Advanced
	Learning and Development	4	Sense Making	Advanced

	Manpower Planning	4	Creative Thinking	Advanced
	OT Cybersecurity Education and Awareness	4		
	OT Cybersecurity Risk Assessment and Mitigation	4	Transdisciplinary Thinking	Intermediate
	People and Performance Management	4	Sense Making	Intermediate
	Stakeholder Management	4	Communication	Intermediate
	Supply Chain Management	4	Global Perspective	Intermediate
	Threat Analysis and Defence	4	Creative Thinking	Intermediate
	Threat Intelligence and Detection	4		
	Vulnerability Assessments	4		

The information contained in this document serves as a guide.

Track	**Security Design and Engineering**		
Occupation	**OT Cybersecurity Architect**		
Job Role	**OT Cybersecurity Architect**		
Job Role Description	OT Cybersecurity Architects lead the design, development and implementation of secure system architectures for the OT environment. This includes identification of OT cybersecurity needs of the organisation and translating them into security designs and principles. They also recommend and lead the adoption of new technological advances and best practices in OT systems to mitigate security risks. They are well-versed in OT systems and networks within the organisation, and cybersecurity standards and frameworks, and are knowledgeable of various applications and hardware technologies and services.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Develop OT cybersecurity architecture and maintain oversight	Partner with engineering and business teams to identify and develop security design requirements across different OT systems	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Analyse the current OT security design against the organisation's requirements	
		Ensure that security products, services and procedures are compatible with the current OT systems and met the organisation's requirement	
		Support the development of enterprise security architecture	
		Coordinate with multiple parties to identify technical and business attributes on the design, approval and implementation of OT security controls	
		Delegate control, ownership and authentication of OT assets	
		Design the IT/OT network controls and protocols	
	Manage quality and continuous improvement of OT cybersecurity architecture	Analyse the current architecture to identify weaknesses	
		Conduct research on OT cybersecurity emerging technology and regulations concerning on the sector the organisation is operating in	
		Identify and propose changes to organisation's OT security design and architecture	

		Identify future risk on designs considering total operating life and possible opportunities to upgrade cyber safeguards		
		Execute plans to reduce architectural weakness		
		Lead testing and evaluation of security technologies and control		
	Maintain OT cybersecurity system integration	Oversee and advise on system integration activities		
		Review the policies and standard requirement of system integration		
		Partner with the rest of the cybersecurity team to identify improvement opportunities		
	Enhance IT-OT alignment and collaboration	Facilitate knowledge sharing in both the IT and OT cybersecurity teams		
		Develop standardised vocabulary for IT and OT cybersecurity teams based on the identified standards and framework		
		Identify and summarise pain points in aligning IT and OT departments		
		Manage cross-team strategic projects according to guidance from the senior leadership		
		Complete and architect level of understanding of IT-OT demarcation, DMZ and communication flows between IT-OT		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Application Security Management	4	Communication	Intermediate
	Business Needs Analysis	4	Creative Thinking	Intermediate

	Emerging Technology Synthesis	4	Developing People	Intermediate
	Network Security and Segmentation	3	Problem Solving	Intermediate
	OT Cybersecurity Education and Awareness	4	Sense Making	Intermediate
	OT Cybersecurity Risk Assessment and Mitigation	4		
	OT Security Design and Architecture	4	Problem Solving	Intermediate
	OT Products and Solutions Security Evaluation	4	Creative Thinking	Advanced
	Stakeholder Management	5	Transdisciplinary Thinking	Advanced
	Supply Chain Management	4	Sense Making	Intermediate
			Building Inclusivity	Basic

The information contained in this document serves as a guide.

Track	**Security Design and Engineering**		
Occupation	**Head of Cybersecurity Architecture**		
Job Role	**Head of OT Cybersecurity Architecture**		
Job Role Description	The Heads of OT Cybersecurity Architecture work closely with the senior leadership of the organisation to identify goals, objectives and risk appetites and formulate the cybersecurity needs and security design principles that balances and suit these needs. They lead a team of OT cybersecurity architects and provide technical guidance during the design and implementation of secure system architectures for the OT environment. They also champion the IT/OT alignment in the organisation. They have deep expertise on the various OT systems and networks and are strongly familiar with the cybersecurity standards and frameworks used globally. They keep abreast of cyber-related applications and hardware technologies and services and are constantly on the look-out of new technologies which could enhance the security architectures of the OT environment. They display strong leadership attributes in guiding, developing and managing resources within the team. They are also decisive in their nature and are able to manage senior stakeholders well.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Manage quality and continuous improvement of OT cybersecurity architecture	Champion the adoption of new technologies and drive the implementation to improve OT security design and architecture	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Review OT security architecture to ensure that it addresses technology shifts, threats and changes in regulation	
		Develop strategic roadmaps and tactical remediation plans to address OT cybersecurity architectural weaknesses	
		Establish key performance metrics to assess the effectiveness of the OT security architecture	
	Formulate the organisation’s OT cybersecurity architecture based on the organisation's standards	Derive OT security architecture requirements from organisation's strategy, business requirement and external environment	
		Lead the process of identifying the organisation’s OT security architectural requirements	
		Lead, approve and evaluate the development and implementation of OT security design	
		Champion the security-by-design concept in the organisation	

		Provide leadership and domain expertise in OT cybersecurity on networking, operating systems hardening and cyber security tooling		
	Enhance IT-OT alignment and collaboration	Champion the cross-skilling and collaboration programmes across IT and OT teams		
		Define the cybersecurity standards and frameworks to be used by both IT and OT cybersecurity teams		
		Streamline policies, tools and processes for OT and IT cybersecurity team		
		Develop tactical solutions to address resistance to change		
		Identify areas or strategic projects that improve IT-OT alignment, cross skilling and improve the organisation cybersecurity capability		
	Lead people and organisation	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		
	Build a cybersecurity culture in the organisation	Drive cybersecurity awareness and training programmes		
		Facilitate and advise the organisation's senior leadership in deciding cybersecurity strategy in the OT environment		
		Lead various cybersecurity exercises according to expertise and required regulations		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Application Security Management	4	Communication	Advanced

	Business Needs Analysis	5	Creative Thinking	Advanced
	Emerging Technology Synthesis	5	Developing People	Advanced
	Learning and Development	5	Problem Solving	Advanced
	Manpower Planning	4	Sense Making	Advanced
	Network Security and Segmentation	4		
	OT Cybersecurity Education and Awareness	5	Problem Solving	Advanced
	OT Cybersecurity Governance and Programme Management	5	Creative Thinking	Advanced
	OT Cybersecurity Risk Assessment and Mitigation	~~4,~~5	Transdisciplinary Thinking	Advanced
	OT Security Design and Architecture	5	Sense Making	Advanced
	Partnership Management	5	Building Inclusivity	Intermediate
	People and Performance Management	4		
	OT Products and Solutions Security Evaluation	~~4,~~5		
	Stakeholder Management	5		
	Supply Chain Management	5		

The information contained in this document serves as a guide.

Sector	**OT Cybersecurity**		
Track	**Security Design and Engineering / Maintenance and Protection**		
Occupation	**OT Cybersecurity Systems Analyst**		
Job Role	**OT Cybersecurity Systems Analyst**		
Job Role Description	The OT Cybersecurity System Analysts support various activities in the design, maintenance and protection functions within the OT environment. They perform activities with relevance to OT cybersecurity administration and maintenance in order to establish a secure OT environment. This includes performing asset discovery, managing vulnerabilities in existing OT systems, as well as performing access control management across OT systems and devices. They are familiar with security technologies such as firewall logs, IDS, endpoint security solutions, access control systems, and other related security technologies within the OT environment.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Improve and maintain cybersecurity posture of OT systems	Conduct system hardening and cybersecurity administration for identified OT systems	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Audit identities and credentials for authorised devices, users and processes in order to protect physical or remote access to OT systems or devices	
		Assist in OT system vulnerability mitigation and patches by working with relevant personnel to deploy regular post-patching update and perform testing of patches	
		Support the implementation of agreed security system changes and maintenance routines	
		Maintain documentation of all maintenance procedures and tests on OT systems	
		Assist with vulnerability assessments and identification	
	Establish OT cybersecurity architecture and controls	Assist in performing security reviews on existing controls and identify cybersecurity gaps	
		Assist in development of cybersecurity requirement specifications for new systems or devices	
		Reference architectural guidelines and validate designs against requirement specification	

	Establish and drive cybersecurity strategies, policies, standards and guidelines according to organisation's needs and legislation	Assist with the implementation of cybersecurity policies, standards and procedures on OT systems
		Monitor third party compliance with organisational cyber security policies, standards and procedures
		Monitor users' adherence to cyber security policies, standards and procedures
	Manage OT cybersecurity risk and compliance	Assist in performing risk analysis or security reviews on OT systems and environment
		Support the proposal of possible recommendations for inclusion in the risk mitigation strategy
	Discover and manage organisation's OT assets	Perform asset discovery or deploy asset management solutions to establish inventory of all connected IT and OT assets that exist within the OT environment
		Establish dependencies, inventory attributes and information across assets in order to support cybersecurity activities
		Maintain and update inventory of all connected IT and OT assets and devices within the organisation
		Document change logs and include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)
		Monitor configuration of assets for consistency against established baselines throughout the assets' life cycle

Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Access and Control Management	3	Communication	Basic
	Application Security Management	2	Creative Thinking	Basic
	Asset Identification and Inventory	2	Problem Solving	Intermediate
	Business Needs Analysis	2	Sense Making	Intermediate

	Network Administration and Maintenance	2	Collaboration	Intermediate
	Network Security and Segmentation	3		
	OT Cybersecurity Risk Assessment and Mitigation	2	Sense Making	Basic
	OT Vulnerability and Patch Management	3	Problem Solving	Basic
	OT Security Design and Architecture	3	Transdisciplinary Thinking	Intermediate
	Stakeholder Management	2	Collaboration	Intermediate
	Supply Chain Management	3	Digital Fluency	Intermediate

The information contained in this document serves as a guide.

Track	**Governance, Risk and Compliance**		
Occupation	**OT Cybersecurity Risk and Compliance Specialist**		
Job Role	**OT Cybersecurity Risk and Compliance Specialist**		
Job Role Description	OT Cybersecurity Risk & Compliance Specialists drive OT cybersecurity policies, standards and guidelines aligned to the organisation's enterprise risk management framework as well as legislation requirements. They work with internal and external stakeholders to conduct risk assessment in the OT environment to help identify related cybersecurity risks and determines appropriate controls to ensure that OT systems perform within acceptable limits of risks. They monitor, track and manages risk mitigations and exceptions to ensure compliance with cyber security standards and policies.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Establish and drive cybersecurity strategies, policies, standards and guidelines according to organisation's needs and legislation	Communicate and drive adoption of new policies or amendments to existing OT cybersecurity policies, standards and guidelines across all relevant internal or external stakeholders	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Support review of policies, standards and guidelines against the current cyber operating environment and cybersecurity threat landscape	
		Provide inputs to shape OT cybersecurity policies, standards and guidelines	
		Support necessary compliance and audit activities as required	
		Report on metrics and identified outcomes to track compliance across the OT environment	
		Follow-up on deviations from compliance activities and audit findings with relevant business teams to address compliance gaps and remediation plans	
		Work with relevant stakeholders to ensure successful implementation and functionality of security requirements and appropriate OT policies and procedures that are consistent with the organisation's enterprise risk management framework	
		Monitor procedures and controls to ensure regulatory and compliance for OT environment	
		Address technical queries and issues on OT cybersecurity policies, standards and guidelines	
	Manage OT cybersecurity risk	Communicate acceptable level of risk tolerance to internal or external stakeholders	

		Maintain awareness and documentation of all cybersecurity risks identified for OT systems through risk registers			
		Analyse and classify identified cyber risks in the OT environment based on severity and assign risk owner			
		Execute documentation, monitoring and assessment processes necessary to assure that existing and new OT systems meet the organisation's cybersecurity and risk requirements			
		Work with system owners and relevant internal or external stakeholders to perform risk analysis or security reviews on OT systems and environment resulting in recommendations for inclusion in the risk mitigation strategy.			
		Ensure appropriate treatment of risk, compliance, and assurance from internal and external stakeholders in order for OT systems to perform within acceptable limits of risks			
		Partner with relevant internal or external stakeholders to implement corrective actions or remediation plans in order to mitigate vulnerabilities identified during risk assessments or audits			
	Enhance IT-OT alignment and collaboration	Provide inputs to overall Enterprise Risk Management Framework processes and activities			
		Drive awareness of OT cybersecurity related risks			
		Develop standardised vocabulary for IT and OT cybersecurity teams based on the identified standards and framework			
		Articulate potential pain points and solutions in aligning IT and OT departments			
		Manage cross-team strategic projects according to guidance from the senior leadership			
Skills & Competencies	**Technical Skills & Competencies**			**Critical Core Skills**	
	Business Needs Analysis	4		Transdisciplinary Thinking	Intermediate
	OT Compliance and Assurance	3		Digital Literacy	Advanced
	OT Cybersecurity Education and Awareness	4		Sense Making	Advanced

	OT Cybersecurity Governance and Programme Management	5	Problem Solving	Advanced
	OT Cybersecurity Risk Assessment and Mitigation	4		
	Stakeholder Management	3	Sense Making	Intermediate
	Supply Chain Management	3, 4	Communication	Intermediate
	Vulnerability Assessment	2	Problem Solving	Intermediate
			Transdisciplinary Thinking	Intermediate
			Global Perspective	Intermediate

The information contained in this document serves as a guide.

Track	**Governance, Risk and Compliance**		
Occupation	**OT Cybersecurity Risk & Compliance Manager**		
Job Role	**OT Cybersecurity Risk and Compliance Manager**		
Job Role Description	OT Cybersecurity Risk & Compliance Managers are responsible for establishing and approving policies, standards and guidelines to effectively manage OT cybersecurity risks. They also work with enterprise risk management and other various stakeholders to integrate and align the OT cyber risk management framework within the organisation's context. They have deep expertise in the governance and compliance domain and are strongly familiar with the sectoral trend and cyber threats in the OT landscape. They also have a strong expertise in risk assessment and analysis framework and methodologies.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Establish and drive cybersecurity strategies, policies, standards and guidelines according to organisation's needs and legislation	Articulate organisation's purpose, strategies and operation priorities and formulate OT cyber risk management framework	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Establish and approve policies, standards and guidelines for managing cybersecurity risks and protecting OT systems against cybersecurity threats	
		Work with critical stakeholders to conduct review of policies, standards and guidelines against the current cyber operating environment and cybersecurity threat landscape	
		Develop procedures and controls to ensure regulatory and compliance within the OT environment	
		Ensure alignment of OT cybersecurity policies with other policies and operational standards	
	Manage OT cybersecurity risk	Define organisation's OT cyber risk appetite aligned with organisation's enterprise and business risks	
		Define roles and responsibilities in managing OT cybersecurity risk, including reporting lines and accountabilities across organisation, including identification and prioritisation of OT assets	
		Present findings on deviations from compliance activities and audit findings with relevant senior management stakeholders to drive implementation of corrective actions or remediation plans	
		Develop or update risk assessment techniques to ensure comprehensive coverage across the OT environment	
		Develop relevant policies and procedures to verify that security postures or controls are implemented, document deviations, and recommend required actions to correct those deviations	

		Provide advisory on tactical measures to address and mitigate OT cyber risk		
		Monitor cyber regulatory compliance findings and engage stakeholders with immediate follow-up actions if required		
	Enhance IT-OT alignment and collaboration	Build organisation's awareness on the risks in the OT environment and identify need for OT cybersecurity awareness and training programmes		
		Champion the cross skilling and collaboration programmes across IT and OT teams		
		Streamline policies, tools and processes for OT and IT cybersecurity team		
		Anticipate resistance to changes in work processes and develop solutions to address		
		Identify areas or strategic projects that improve IT-OT alignment, cross skilling and improve the organisation cybersecurity capability		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Budgeting	5	Digital Fluency	Advanced
	Business Needs Analysis	4	Global Perspective	Advanced
	Learning and Development	5	Sense Making	Advanced
	Manpower Planning	4	Creative Thinking	Advanced
	OT Compliance and Assurance	4		
	OT Cybersecurity Education and Awareness	5	Problem Solving	Advanced
	OT Cybersecurity Governance and Programme Management	5 6	Decision Making	Advanced

	OT Cybersecurity Risk Assessment and Mitigation	5,6	Collaboration	Advanced
	People and Performance Management	4	Transdisciplinary Thinking	Advanced
	Stakeholder Management	4	Communication	Advanced
	Supply Chain Management	5		
	Vulnerability Assessment	2		

The information contained in this document serves as a guide.

Track	**Security Monitoring and Assessment / Respond and Recover**		
Occupation	**OT Cybersecurity Operations Analyst**		
Job Role	**OT Cybersecurity Operations Analyst**		
Job Role Description	OT Cybersecurity Operations Analysts support various activities in driving cybersecurity operations on OT systems. This includes performing comprehensive surveillance and monitoring on OT systems and assets, supporting in the identification of threats or vulnerabilities, and providing incident response and remediation support. They collect and document information based on established standards and guidelines and assist in preparing performance reports. They are familiar with various cyber security standards, protocols and frameworks and are knowledgeable in using various cybersecurity tools to perform their job accordingly.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Monitor OT systems for cybersecurity incidents	Maintain data sources feeding cybersecurity or monitoring systems to facilitate analysis and trending of security log data	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Perform continuous security monitoring, analysis and reporting of cybersecurity events or incidents affecting OT systems	
		Maintain incidents and security data logs on OT systems and prepare regular documentation for reports	
		Support identification and analysis of security events and incidents against indicators of compromise to detect attacks on OT systems	
		Provide inputs to shape development and maintenance of security monitoring rules and activities	
	Improve and maintain cybersecurity posture of OT systems	Execute vulnerability scans on OT systems and components	
		Provide recommendations to maintain and improve OT cybersecurity posture in alignment with monitoring and assessment outcomes	
		Prepare OT system vulnerability mitigation and patch deployment report to escalate to systems and asset owners	
		Execute and support the implementation of OT cybersecurity programme	
		Prepare routine performance and metrics reports for OT cybersecurity operations	

	Respond to OT cyber incidents	Facilitate incident response activities according to incident response protocols and plans		
		Provide information to support triaging, analysis and eradication of cybersecurity incidents		
		Assist Incident Response personnel in containment and mitigation of incidents to recover compromised systems to acceptable levels of confidentiality, integrity, and availability		
		Follow the crisis management plan according to organisation's guidelines		
		Support OT cybersecurity investigation activities through collection of relevant data during cyber incidents		
	Discover and manage organisation's OT assets	Assist in OT asset discovery and identification of attack surfaces		
		Maintain visibility and monitor OT asset inventory, devices and networks within the organisation		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Asset Identification and Inventory	2	Communication	Basic
	Business Continuity and Recovery	3	Creative Thinking	Basic
	Business Needs Analysis	2	Problem Solving	Intermediate
	Cyber Forensics	2	Sense Making	Intermediate
	Cyber Incident Response and Management	2	Collaboration	Intermediate
	Failure Analysis	2		
	Network Administration and Maintenance	2	Sense Making	Basic

	OT Cybersecurity Governance and Programme Management	3	Problem Solving	Basic
	OT Cybersecurity Risk Assessment and Mitigation	2	Transdisciplinary Thinking	Intermediate
	OT Vulnerability and Patch Management	3	Collaboration	Intermediate
	Stakeholder Management	2	Digital Fluency	Intermediate
	Threat Intelligence and Detection	2		
	Vulnerability Assessments	2		

The information contained in this document serves as a guide.

Track	**Security Monitoring and Assessment**		
Occupation	**OT Penetration Tester**		
Job Role	**OT Penetration Tester**		
Job Role Description	OT Penetration Testers design and perform penetration testing and security assessments on live or simulated environments to determine if OT systems, components and applications meet confidentiality, integrity, authentication, availability, authorisation and non-repudiation standards. They translate and scope test requirements or environments in alignment with pre-approved standards and procedures to evaluate vulnerabilities. They outline findings and propose remediation plans. They work with relevant OT personnel to ensure no operational disruption to systems are caused as a result of testing and assessments. They are well versed with the tools, standards, protocols and frameworks to conduct penetration testing in the OT environment without causing operational disruption and putting the physical safety at risk.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Perform Vulnerability Assessments and/or Penetration Testing	Enable continued or new exploitation operations in support of organisation objectives and target requirements.	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Collaborate with other internal and external partners on target access and operational issues.	
		Conduct analysis of physical and logical digital technologies to identify potential avenues of access to OT systems and networks	
		Conduct in-depth target and technical analysis including target-specific information (e.g., cultural, organisational, political) that results in access	
		Perform comprehensive exploitation activities that identify exploitable technical or operational vulnerabilities.	
		Conduct or support authorised penetration testing on OT systems or simulated environments	
		Propose remediation measures and security posture improvements	
		Stay abreast of possible threats that impact operation criticality and physical safety of OT systems	
		Prepare penetration testing reports highlighting risk to business operations	
	Enhance IT-OT alignment and collaboration	Communicate new developments, breakthroughs, challenges and lessons learned on outcomes of testing and assessments across OT and IT cybersecurity teams	

	Develop standardised vocabulary for IT and OT cybersecurity teams based on the identified standards and framework	
	Articulate potential pain points and solutions in aligning IT and OT departments	
	Manage cross-team strategic projects according to guidance from the senior leadership	

Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Application Security Management	2,3	Digital Fluency	Advanced
	Threat Analysis and Defence	3, 4	Sense Making	Advanced
	OT Cybersecurity Education and Awareness	3	Transdisciplinary Thinking	Intermediate
	Penetration Testing	3, 4	Problem Solving	Advanced
	Threat Intelligence and Detection	3		
	Emerging Technology Synthesis	4	Communication	Intermediate
	Stakeholder Management	3	Sense Making	Intermediate
	OT Cybersecurity Risk Assessment and Mitigation	3	Problem Solving	Intermediate
	Vulnerability Assessments	3	Transdisciplinary Thinking	Advanced
	OT Cybersecurity Governance and Programme Management	3	Creative Thinking	Advanced
	OT Products and Solutions Security Evaluation	3, 4		

The information contained in this document serves as a guide.

Track	**Security Monitoring and Assessment**		
Occupation	**OT Vulnerability Assessor**		
Job Role	**OT Vulnerability Assessor**		
Job Role Description	OT Vulnerability Assessors perform vulnerability or security assessment across the OT environment to determine if OT systems, components and applications meet confidentiality, integrity, authentication, availability, authorisation and non-repudiation standards. They obtain critical information and data with regards to vulnerabilities and work with relevant cybersecurity personnel to prioritise threats and implement mitigation action. They are well versed with the tools, standards, protocols and frameworks of vulnerability management. They also have in-depth knowledge of threat actors relevant to the organisation. They are systematic and analytical in performing their duties and are able to reveal threats and articulate the risks and impact to the organisation.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Perform Vulnerability Assessment and/or Penetration Testing	Perform technical risk and vulnerability assessments or scans across the OT environment	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Perform discovery of missing patches, misconfiguration and lack of hardening	
		Analyse software and configuration snapshot of endpoints for possible exploitation points	
		Prioritise vulnerabilities based on risk and impact to the OT environment	
		Define attack vector, severity and complexity of affected OT systems based on vulnerabilities identified	
		Manage and operate vulnerability management systems and tools for OT cybersecurity	
		Provide inputs to improve assessments or scans based on emerging security and risk management trends and issues	
	Improve and maintain cybersecurity posture of OT systems	Identify vulnerability gaps in existing security controls	
		Communicate the outcome of assessment initiatives and results to the stakeholder groups	

		Provide recommendations or mitigating controls mitigate risks and improve OT cybersecurity posture in alignment with monitoring and assessment outcomes		
	Discover and manage organisation's OT assets	Identify potential attack surfaces across OT assets and devices		
	Enhance IT-OT alignment and collaboration	Communicate new developments, breakthroughs, challenges and lessons learned on outcomes of testing and assessments across OT and IT cybersecurity teams		
		Develop standardised vocabulary for IT and OT cybersecurity teams based on the identified standards and framework		
		Articulate potential pain points and solutions in aligning IT and OT departments		
		Support the management of cross-team strategic projects according to guidance from the senior leadership		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Application Security Management	2	Communication	Intermediate
	Emerging Technology Synthesis	4	Creative Thinking	Intermediate
	Learning and Development	3	Problem Solving	Advanced
	OT Cybersecurity Education and Awareness	3	Sense Making	Advanced
	OT Cybersecurity Governance and Programme Management	3	Collaboration	Advanced
	OT Cybersecurity Risk Assessment and Mitigation	3		
	OT Products and Solutions Evaluation	3, 4		
	Stakeholder Management	3	Communication	Intermediate

	Threat Analysis and Defence	3	Sense Making	Intermediate
	Threat Intelligence and Detection	3	Problem Solving	Intermediate
	Vulnerability Assessments	4	Transdisciplinary Thinking	Advanced
			Creative Thinking	Advanced

The information contained in this document serves as a guide.

Track	**Respond and Recover**		
Occupation	**OT Incident Responder**		
Job Role	**OT Incident Responder**		
Job Role Description	OT Incident Responders promptly respond to cyber incidents in order to mitigate immediate and potential threats within the OT environment. They perform proactive coordination with appropriate departments in the containment and mitigation of incidents, as well recovery processes. They work with cybersecurity personnel to identify and define cyber threats and root causes, investigate into the cause and impact of the incident, and develop detailed reports on incident timeline, evidence, findings, conclusions and recommendations. They are responsible for managing cyber incidents and resolving the incidents in a timely manner. They are familiar with cyber security standards, incident response plans, procedures and protocols of the organisation, and work in compliance with them.		
Critical Work Functions and Key Tasks / Performance Expectations	**Critical Work Functions**	**Key Task**	**Performance Expectations (for legislated/regulated occupations)**
	Respond to OT cybersecurity incidents	Receive incident escalations and activate incident response procedures as per established incident response plan and protocols	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Work with relevant cybersecurity or operations personnel to understand threat scenario and security issues	
		Analyse security issues and perform triaging of OT cybersecurity incidents to enact relevant identification, containment, and eradication measures while supporting recovery efforts of OT systems	
		Coordinate with relevant personnel such as operations team to implement procedures for the containment of cybersecurity incidents, activation of recovery processes, and investigation processes	
		Advise senior leadership with information to facilitate critical decision-making and alignment in incident response and handling approach	
		Implement procedures for the preservation of evidence or artefacts prior to the initiation of recovery process to support investigation activities	
		Engage and liaise with external parties such as vendors for forensic/recovery activities or law enforcement personnel to carry out required incident response protocols	
		Prepare accurate and detailed cyber incident reports in the OT environment to facilitate after-action review processes	
	Improve and maintain cybersecurity posture of OT systems	Organise or participate in cybersecurity exercises to ensure readiness and preparedness across critical teams	
		Present findings of cyber incidents to identify and recommend mitigation actions to prevent recurrences	

	Enhance IT-OT alignment and collaboration	Participate and contribute to the development of incident response plans and identification of responsibilities across the organisation		
		Act as subject matter experts to provide insight and guidance to colleagues engaging in incident response activities or prevention measures		
		Support the development of standardised vocabulary to align IT and OT cybersecurity teams		
		Articulate potential pain points and solutions in aligning IT and OT departments		
		Support the management of cross-team strategic projects or joint cybersecurity exercises according to guidance from the senior leadership		
Skills & Competencies	**Technical Skills & Competencies**		**Critical Core Skills**	
	Business Continuity and Recovery	3, 4	Communication	Intermediate
	Cyber Forensics	2	Creative Thinking	Intermediate
	Cyber Incident Response and Management	3, 4	Problem Solving	Intermediate
	Failure Analysis	2	Sense Making	Intermediate
	OT Cybersecurity Risk Assessment and Mitigation	3, 4	Teamwork	Intermediate
	Supply Chain Management	3		
	Stakeholder Management	4		
			Problem Solving	Intermediate
			Sense Making	Intermediate

			Communication	Intermediate
			Creative Thinking	Intermediate
			Decision Making	Intermediate

The information contained in this document serves as a guide.

<table>
<tr><td>Track</td><td colspan="3">Respond and Recover</td></tr>
<tr><td>Occupation</td><td colspan="3">OT Cyber Investigator</td></tr>
<tr><td>Job Role</td><td colspan="3">OT Cyber Investigator</td></tr>
<tr><td>Job Role Description</td><td colspan="3">OT Cyber Investigators carry out investigation processes and protocols in the OT environment after a cyber-threat or incident.

They are familiar with different types of threats, cyber security standards, protocols and frameworks with regards to forensic investigation. They are knowledgeable of hardware and software applications to analyse threat data from various sources.</td></tr>
<tr><td rowspan="9">Critical Work Functions and Key Tasks / Performance Expectations</td><td>Critical Work Functions</td><td>Key Task</td><td>Performance Expectations (for legislated/regulated occupations)</td></tr>
<tr><td rowspan="5">Conduct Forensic Investigation on OT systems</td><td>Identify, collect, examine, and preserve evidences and artefacts for the purpose of conducting cyber forensic investigation on OT systems</td><td rowspan="9">Cyber Security Act 2018, Cyber Security Agency of Singapore</td></tr>
<tr><td>Analyse evidence and artefacts to investigate cyber incidents and examine root causes</td></tr>
<tr><td>Identify attacker tools, tactics, and procedures and develop indicators of compromise</td></tr>
<tr><td>Develop and implement remediation plans and investigative reports in conjunction with incident response</td></tr>
<tr><td>Present reports and outcomes in investigations or legal proceedings to senior management and stakeholders</td></tr>
<tr><td rowspan="4">Improve and maintain cybersecurity posture of OT systems</td><td>Recommend threat and vulnerability mitigation actions based on investigation findings</td></tr>
<tr><td>Contribute to the development of digital forensic investigation policies and standards for the organisation</td></tr>
<tr><td>Suggest improvements to cyber forensic investigation techniques and methodologies for the OT environment</td></tr>
<tr><td>Skills & Competencies</td><td colspan="2">Technical Skills & Competencies</td><td>Critical Core Skills</td></tr>
</table>

	Cyber Forensics	3, 4	Communication	Advanced
	Business Continuity and Recovery	4	Developing People	Advanced
	Emerging Technology Synthesis	4	Problem Solving	Advanced
	Failure Analysis	3, 4	Resource Management	Advanced
	OT Cybersecurity Risk Assessment and Mitigation	4	Sense Making	Advanced
	Stakeholder Management	3		
			Problem Solving	Intermediate
			Communication	Intermediate
			Sense Making	Intermediate
			Transdisciplinary Thinking	Intermediate
			Collaboration	Intermediate

4 Technical Skills & Competencies (TSC)

TSC Category	Protect					
TSC Title	Application Security Management					
TSC Description	Detect, mitigate and prevent vulnerabilities to protect applications that have been deployed					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Perform application code review, application testing and unit testing to identify security lapses	Examine associated vulnerabilities in applications to deploy mitigation measures	Integrate best practices to drive secure software development practices throughout an application lifecycle, in consideraration of evolving threats and trends		
Knowledge		• Organisation operational technology security standards • Techniques for application and unit testing • Types of vulnerabilities that exist in applications used in organisation • Methods to perform source code review • List of applications used in the organisation	• Types of threats to organisational technology security posed by applications • Operational technology security standards • Types of operational technology security controls and mitigation procedures • Implementation process and considerations for appropriate measures to address vulnerabilities that exist in applications	• Best practices for application security • Secure software development lifecycle practices • Types of mitigation strategies • Implications of technical changes on applications		
Abilities		• Identify the need to perform application code review prior to application testing • Provide technical assistance to users for the installation and maintenance of applications, in-line with application security standards and secure software development lifecycle practices • Perform functional application testing or unit testing to review cybersecurity capabilities	• Facilitate efforts with relevant subject matter experts to assess and address source code defects prior to application testing • Inspect adherence of applications and its components to application security standards and baselines • Develop processes, methods and technologies to facilitate application testing across varying	• Oversee the maintenance and update of the list of approved applications for usage in OT systems required to drive operations and cybersecurity • Lead implementation of patches or compensating controls for applications in consultation with relevant stakeholders • Evaluate criticality of the applications and specifics of the vulnerabilities to		

		across all installed applications • Assess lapses in security standards or issues that exist in applications which would endanger operations security and integrity • Collate user feedback on existing applications • Perform troubleshooting to determine if the root-cause stems from a cybersecurity lapse • Consolidate list of applications and softwares which conflicts with or poses potential risk to existing OT cybersecurity systens • Facilitate blacklisting and whitelisting of softwares to prevent system conflict and unauthorised usage	applications that exist in OT systems • Examine security risks, threats and vulnerabilities associated with existing applications utilising appropriate tools and techniques • Deploy mitigation actions to address application security gaps and facilitate alignment with operations security standards • Implement follow-up reviews or regression tests to validate the effectiveness of the mitigation actions • Identify list of software or applications to be blacklisted or whitelisted to prevent access from unauthorised software	prioritise mitigation action to undertake • Collaborate with relevant stakeholders to integrate best practices into an application life cycle in order to uncover and address vulnerabilities before usage of applications • Define processes to manage and maintain an application from its design phase to its decommission and manage application defects • Establish processes to incorporate controls or non-repudiation actions to verify the usage of applications • Review and update approvals for existing applications to ensure that only applications required for the operation and cybersecurity of OT systems are whitelisted for usage and installation • Evaluate OT cybersecurity landscape for evolving threats and trends and identify implications on existing application security measures		

The information contained in this document serves as a guide.

TSC Category	Identify					
TSC Title	Asset Identification and Inventory					
TSC Description	Identify and manage the organisation's OT assets and inventory to enable the organisation in delivering cybersecurity activities across different functions					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Facilitate implementation of asset identification, change management and configuration processes	Improve asset identification process to deliver a robust asset inventory	Drive asset identification, practices and configuration standards across varying OT assets	Spearhead collaboration with relevant departments and stakeholders to drive asset identification across OT and IT assets	
Knowledge		• Asset identification tools and techniques • Metadata required for asset inventory • Baseline configuration standards • Proper asset handling, maintenance and storage procedures • Types of OT assets and systems that exist in the organisation	• Lifecycle stages and management of OT assets • Asset identification process • Asset change management practices • Impact of asset identification tools and techniques • Potential cyber security risks from OT assets • Vendors for OT assets	• Industry best practices in configuration standards • Elements of an organisation asset management plan and procedures • Industry standards and best practices in asset identification and management • Mitigation strategies to deal with vulnerabilities and weaknesses of OT assets	• Components of OT and IT asset management plans • Impact of change management practices on cybersecurity operations • Industry best practices for strategies and techniques in asset performance and maintenance • Emerging threats and trends in the OT cybersecurity landscape • Regulatory requirements or standards for asset management	
Abilities		• Perform identification of assets and maintenance of inventory utilising identified asset identification tools and techniques • Maintain and update data points in alignment with asset identification requirements • Consolidate configuration and information on OT assets from existing network maps, historical data or other documentation	• Review comprehensiveness of asset inventory and recommend additional tools for effective and continuous monitoring of assets • Assess risk and implications on implementing IT or OT-specific asset identification tools and techniques • Provide recommendations and mitigation strategies on asset identification approach when utilising	• Define scope and approach for asset identification to drive comprehensiveness and efficiency of asset identification process • Establish information or additional data points required to drive delivery of OT cybersecurity • Oversee utilisation of ongoing identification tools and ensure that proper measures are in place to mitigate threat vulnerabilities	• Guide integration of asset identification updates into change control processes to ensure that processed changes are aligned with asset inventory • Liaise with relevant IT stakeholders to leverage IT networks and protocols to assist in asset identification • Articulate value of asset identification in reducing recovery times and lowering organisational risk to gain buy-in from relevant stakeholders	

		• Perform logging of changes that impact the availability, integrity, confidentiality of OT assets • Identify owners of OT assets to facilitate assignment of responsibilities across asset management practices and processes	IT asset identification tools on OT assets • Monitor configuration of OT assets against established baselines throughout the assets' lifecycle and escalate issues where necessary • Review OT assets and perform identification of end-of-support or end-of-life assets and systems	• Endorse changes and updates to asset identification processes • Establish configuration baselines for inventoried and deployed assets in alignment with cybersecurity objectives • Plan mitigation of risks posed by end-of-support or end-of-life assets systems in consultation with asset owners • Maintain oversight on the presence and efficiency of major technical controls across OT assets, determining where controls may be missing or malfunctioning	• Spearhead consolidated reporting and management by keeping up-to-date with OT asset identification program and identifying implications on IT asset management programs, vice versa • Anticipate future OT assets requirements of the organisation and impact on existing OT assets based on emerging trends and evolving needs • Lead review and updates of configuration baselines or changes at an organisation-defined frequency	

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	Cryptography and Encryption					
TSC Description	Implement cryptography and encryption to mitigate threat vectors posed to unsecured OT systems					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Support cryptography and encryption testing, and storage and providing support to stakeholders for decryption of relevant data for operations	Execute and implement cryptography and encryption initiatives and evaluating potential threat vectors posed to existing OT systems	Assess the effectiveness of existing mix of cryptography and encryption initiatives in securing OT systems and ensuring proper storage of decryption keys	Drive creation of new frameworks, guidelines and processes to strike a balance between encrypting information while minimising disruption to operations for cryptography and encryption initiatives in the organisation	
Knowledge		• Techniques for acccessing confidential data flowing through different types of OT systems (SCADA, PLCs, etc.) • Audit and monitoring techniques • Internal guidelines for storage of encryption keys • Cryptography and encryption techniques and skills	• Vulnerability points and threat vectors posed for OT systems • Understanding of varied algorithm creation techniques and application • Cryptography and encryption techniques • Cryptography and encryption frameworks (IPsec, etc.), standards (IEC62351, etc.) and techniques • Industry guidelines and best practices for storage and securing encryption keys	• Strength and weaknesses of various cryptography and encryption techniques • Impacts of encryption on business operations, continuity, safety and recovery from OT cybersecurity incidents • Business processes utilising encrypted information • Vulnerabilities of OT systems during the integration process	• Impacts of emerging threats and best practices affecting organisational initiatives • Differentiating levels of impact to business operations, continuity, safety and recovery from OT cybersecurity incidents • Flows of confidential information throughout organisational OT systems	
Abilities		• Support the testing of encrypted algorithms prior to the execution of cryptography and encryption initiatives • Support requests from other stakeholders to decrypt information • Consolidate data on security logs in order to monitor effectiveness of	• Identify the need to execute suitable algorithms for cryptography and encryption initiatives • Review security logs to identify unauthorised activity • Analyse potential threat vectors on various	• Create cryptography algorithms to encrypt OT systems • Facilitate cryptography and encryption initiatives in-line with OT security requirements • Identify the appropriate encryption technique to provide expected level of	• Establish requirements for identification and communication of confidential data between OT systems to drive encryption activities, in alignment with relevant industrial standards • Design guidelines and processes for the	

		existing cryptography initiatives • Monitor storage and usage of decryption keys to ensure alignment with guidelines and processes	cryptography and encryption techniques • Identify appropriate storage channels for encryption keys • Assess effectiveness of existing modifications to cryptography and encryption initiatives	protection on OT systems • Recommend further improvements for cryptography and the encryption of OT systems • Identify key stakeholders to possess appropriate user rights and decryption keys • Evaluate impact, relevance and effectiveness of encryption on internally shared information	identification of threat vectors and allocation of critical OT assets into different cryptography and encryption layers • Prioritise decisions on encrypting information by assessing operation disruption or safety risks on existing OT systems • Cultivate relationship with stakeholders internally and externally to incorporate cryptography and encryption best practices and trends into organisational initiatives	

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	Network Security and Segmentation					
TSC Description	Design and configure network systems to ensure integrity and reliability of network infrastructure of OT systems through segmentation of network infrastructure, incorporating uses of apprioriate protection, detection and response mechanisms to confine and detect security incidents					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Monitor, review and execute operational requirements to ensure the integrity of OT network infrastructure	Manage, identify and analyse functional and performance security requirements of networks involved in OT systems	Design frameworks to assess differentiating network security requirements across varying OT systems and develop policies to mitigate threats	
Knowledge			• Security requirements of the organisation • Virtual Private Network (VPN)- types, functions and operation, limitations, bandwidth and dynamic security environment • Configuration of routers and switches • Hardware and software security products, features and capabilities • Network protocols and operating systems • Security perimeters, functions, protocols, standards and data encryption	• OT network zones and their configuration • Types of network attacks, vulnerabilities and related weaknesses of installed infrastructure • Types and techniques of OT security network and security measures • Network security implementation and procedures • Network segmentation • Wireless security impacting OT systems	• Frameworks, guidelines and regulatory requirements • Industry trends of best practices and threats in the landscape • OT assets and OT security network segmentation requirements	

Abilities			• Monitor security network for incidents and identified operational threats affecting OT systems • Propose recommendations to address network security deficiencies • Implement perimeter security, network hardening measures and authentication and user account controls according to identified network security requirements • Conduct testing to verify the key functions and performance measures of network security • Monitor packets and information to facilitate diagnosing of network problems, investigating security or policy violations, and aiding in security incident response and network forensics activities • Assess if identified alerts are false positives • Debug network security according to test results • Perform collection, storing and correlation of logs utilising appropriate security information and event management Review logs and audit reports of security incidents, intrusions and attempts	• Assess need for network security segmentation in order to ensure secure OT systems • Collaborate with relevant stakeholders to keep up to date with current security posture of networks in critical OT systems • Identify threats to OT systems based on network security requirements in consultation with relevant stakeholders • Assess feasibility for unidirectional gateway implementation in highly critical environments • Deploy and configure firewalls to control network traffic and run inspection, on abnormal protocol behaviour, search for patterns of compromise, and verify traffic signatures against known malware and exploit traffic • Deploy security measures and controls across network components and zones to reduce risk of compromises and increase network visibility • Analyse and recommend configurations aligned with incident response procedure designs • Identify gap between expected and actual performance for VPNs and firewalls to optimise troubleshooting, response practices and forensic practices • Execute recovery plan for false positives identified	• Define planning, building and management phases for network security design on OT systems • Determine perimeters, boundaries and trust levels for network security zones in order to limit broadcast domain, restrict bandwidth usage and reduce attack surfaces • Define security requirements for network security zones to drive availability, integrity and confidentiality of critical OT systems • Establish planning, building and management phases for network security design on OT systems • Conduct research and evaluate organisational, regulatory and security policies used to benchmark acceptable network security standards • Prioritise recommendations to address current and future security network gaps • Evaluate degree of integration between end-to-end OT security solutions with wireless networks • Formulate policies concerning VPNs and firewalls implementation • Collaborate with relevant stakeholders to formulate network intrusion detection and recovery processes OT systems	

				• Monitor network traffic to ensure that there is no unauthorised access on OT systems	• Implement device profiling framework for devices that are connected to the organisational OT network • Define rules of communications across network security zones and facilitate efforts to drive resiliency and redundancy best practices for network zones • Assess need to identify cell area zones in alignment with goal of the security efforts for networks involved in OT systems	
Range of Application	Types of networks may include but are not limited to: • LAN network (e.g., SOHO network, WLAN) • Telecommunications network • Next generation network (NGN) • Wide area network (WAN) Types of zones may include but are not limited to: • Indutrial zones • Enterprise Zones • Industrial Demilitarised Zones • Cell Area Zones Log mangement: • Firewall logs • Network intrusion detection logs • Router and switch logs • Operating system logs • Application logs					

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	OT Compliance and Assurance					
TSC Description	Facilitate compliance and assurance processes by reviewing adherence to regulations and standards involving OT systems; assess and enhance the thoroughness of compliance and/or governance processes and organisation's internal controls to align with changing compliance standards and ensure audit's readiness.					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Conduct audits on various OT systems in the organisations, highlighting findings and implementing changes to address identified gaps	Develop and enhance compliance processes for the OT environment based on an evaluation of gaps in business and operations.	Establish OT systems compliance and assurance strategy and objectives for the organisation.	
Knowledge			• OT systems' processes and principles • Principles of auditing • Methodologies and tools for the conduct of compliance and assurance acitivites in the OT environment • Attributes of compliance findings • Techniques to interpret and analyse of compliance results • Techniques and processes to identification of non-compliance and good practices • Internal and external compliance and regulatory guidelines	• Range of OT systems in the organisation and how they are connected • Elements and considerations in development of compliance processes • External standards relevant to organisation's context and application implications • Organisation's historical OT system compliance or audit findings and patterns • Process gaps and non-compliance analysis techniques in the operations or OT environment	• Types of factors and concepts which influence compliance strategy development for OT systems in the organisation • Operational, safety and business priorities and considerations and their impact to compliance • Evolving statutory and regulatory standards for the OT environment • Emerging trends, approaches and industry best practices of compliance and assurance in the OT environment • Root cause evaluations strategies for cases of non-compliance	
Abilities			• Perform compliance or inspection readiness activities in line with the organisation's compliance processes and guidelines • Review audit or compliance findings to identify relevant security controls, areas of	• Develop compliance and assurance processes in accordance with the organisation's strategy and internal and external guidelines • Evaluate inspection or compliance results, and liaise with stakeholders	• Establish OT systems compliance strategy considering emerging trends, approaches and industry best practices • Oversee alignment of OT system compliance strategy with operation and safety requirements	

			process gaps or key instances of non-compliance in the OT environment • Collaborate with stakeholders and asset owners to propose improvement measures to align with organisational internal and external requirements • Propose changes in in alignment with internal compliance standards or external regulatory guidelines to drive security on OT systems	and asset owners to identify reasons for gaps or non-compliance • Analyse findings to determine systemic and recurring compliance findings • Evaluate adequacy and effectiveness of existing controls against identified business objectives and requirements • Recommend enhancements to compliance processes or security controls to strengthen cybersecurity governance in the OT environment	and business priorities as well as external regulations and standards • Evaluate compliance and inspection findings and highlight root causes and potential organisational impact • Determine adequacy, alignment with internal and external regulations and standards, and effectiveness of OT asset owner's control and governance • Prioritise areas that have matured further and require further enhancement • Endorse enhancements to critical compliance processes	

TSC Category	Identify					
TSC Title	OT Cyber Risk Assessment and Mitigation					
TSC Description	Develop and implement cyber risk assessment and mititgation strategies across the systems' life-cycle, taking into considerationthe organisation's OT environment and external threats					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Support risk assessment exercises across OT assets and systems and documenting results	Conduct OT cyber risk assessment according to techniques and framework endorsed by the organisation	Develop OT cyber risk assessment techniques as well as analyse the risks in terms of likelihood and impacts and roll-out endorsed measures to address identified cyber risks	Assess and direct enhancements to OT cyber risk assessment techniques, and develop strategies to address and mitigate OT cyber risks	Authorise OT cyber risk assessment activities and define operational, business and safety implications of the risks, as well as evaluating the preparedness level to manage such risks
Knowledge		• Techniques to perform cyber risk assessment in the OT environment • Methods to identify OT assets and categorise them based on risk criticality • Risk analysis methodology • Methods to categorise risk and build risk matrix • Methods to document risk analysis results	• Interconnectivity and communication paths of assets in the OT environment • Processes of OT systems in the organisation • Cyber threat libraries and stages of cyber attacks • Elements of risk assessment and risk scenarios • Risk analysis methodology • Methods to categorise risk and build risk matrix	• Cyber risk assessment techniques for the OT environment • Security risks, threats and vulnerabilities in the organisation's OT environment • Operational, safety and business risks and implications from cyber security loopholes • Possible treatments of OT cyber risks	• Design of cyber risk assessment techniques for the OT environment • Projection of cyber risks, threats and vulnerabilities in the OT environment • Key requirements and objectives of various OT cyber risk assessments • Pros and cons of various risk mitigation treatment approaches	• Evolving cybersecurity landscape and emerging threats for the OT landscape • Measures of organisational readiness and preparedness against OT cyber threats
Abilities		• Identify OT assets and owners of the organisation and create assets inventory within the OT environment • Document threat events that are relevant to each asset • Document outputs from the risk assessment exercise and update them in a risk register	• Perform a cyber risk assessment on organisation's OT environment • Develop threat models or risk scenarios based on key risk indicators, business context, system environment and pertinent threats for the OT environment, monitor risk register updates • Collaborate with relevant stakeholders to	• Consolidate insights from various departments and stakeholders for the purpose of designing OT cyber risk assessment techniques • Develop cyber risk assessment techniques to identify loopholes and vulnerabilities in the OT environment and across a system's life cycle • Review the implementation of OT cyber risk assessments	• Guide the development of OT cyber risk assessment techniques • Collaborate with relevant stakeholders to implement relevant policies and processes in order to mitigate OT cyber risks • Evaluate effectiveness of current OT cyber risk assessment techniques • Drive improvements or modifications to OT cyber risk assessment techniques	• Establish organisation's position and strategy for assessing and managing OT cyber risk aligned to overall enterprise risk approach • Define roles and responsibilities for OT cyber risk assessment and mitigation exercises • Formulate risk assessments and testing policies and authorise related activities within the organisation

			implement endorsed treatments and measures to address and mitigate risk	• Analyse the likelihood of OT cyber risk impacting creating operational, safety or business impacts • Assess effectiveness of risk mitigation treatments against organisational policies, processes, procedures and key risk indicators	• Lead the implementation of OT cyber risk assessment activities throughout organisation • Weigh potential operational or safety risks associated with cyber security risks • Evaluate options and determine treatment approaches for OT cyber risks • Develop key risk indicators or indicators of compromise in collaboration with key stakeholders and asset owners to categorise severity of risk and potential impact to organisation and operations	• Articulate implications of potential OT cyber risks and threats and translate them into a business case • Assess overall strength and preparedness of the organisation's existing defences in light of identified OT cyber risks • Endorse strategies to effectively address and mitigate the OT cyber risks identified and evaluate potential costs to the organisation to implement the strategies • Formulate strategies and plans to address current and future risks gaps in consultation with relevant stakeholders

TSC Category	Protect					
TSC Title	OT Products and Solutions Security Evaluation					
TSC Description	Develop test strategy and procedure to verify and ensure that OT solutions and products are in line with cybersecurity requirements; this includes the ability to define and verify the cybersecurity requirements across the product life stages, the tools used to perform the test, the data and/or resources needed to conduct the test.					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Conduct evaluation of OT products and solutions in line with defined framework and processes	Design evaluation plan and analyse test results in alignment with cybersecurity standards	Define frameworks, processes and standards to guide cybersecurity evaluation of OT vendors, products and solutions	
Knowledge			• Testing tools and processes • Documentation requirements of software and hardware testing • Methodologies to implement and assess OT products and solutions	• Different types and levels of testing over product life stages • Range of tests, testware and applications • Optimal scheduling times for different tests • Functional and performance requirements of OT products and solutions	• Testing objectives and scope • Range of tests and their pros, cons, applicability and compatability • Key resources, data and tools required to implement product security • Key components of OT products • OT industry and landscape trends	

Abilities			• Conduct evaluation and testing of OT products and solutions in accordance to established timelines, and functional requirements • Draft functional and performance test scenarios for OT products and solutions • Prepare reports on operational security incidents for OT products and solutions • Conduct network and end-point security testing of OT products and solutions • Coordinate efforts with end-users to identify potential cybersecurity vulnerabilities for implementation of OT products and solutions • Draft report of observed outcomes evaluations of OT products and solutions	• Identify types of evaluations and testings required by OT products and solutions throughout the product life cycle • Configure functional and performance test scenarios for OT products and solutions to ensure that they are not exposed to varying cybersecurity vulnerabilities • Monitor evaluation process to ensure alignment with requirements and standards • Evaluate results against cybersecurity requirements and standards and assess effectiveness of products and solutions in delivering cybersecurity to OT systems • Identify anomalies and vulnerabilities of OT products and solutions and recommend mitigation strategies • Monitor updates of OT product and solutions updates from vendors and identify implications	• Define product and solution requirements in alignment with cybersecurity standards and processes • Establish evaluation framework to facilitate systematic test procedures and approaches across varying OT products and solutions • Spearhead review of existing evaluation processes and frameworks against emerging trends or cybersecurity threats in the industry landscape and assess implications on OT products and solutions • Establish escalation procedures for OT products and solutions that do not comply with cybersecurity requiements • Collaborate with relevant stakeholders to mitigate cybersecurity risks posed by OT products and solutions based on security evaluation results • Cultivate partnerships with vendors or clients to facilitate effective performance and security evaluation of OT products and solutions	

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	OT Security Design and Architecture					
TSC Description	Embed security principles into the design and specification of security architectures and controls for OT systems to meet defined OT cybersecurity needs					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Design secure OT systems and define security specifications of components, integrating appropriate security controls	Develop a security blueprint and direct the design of a robust and coherent OT security architecture, based on a suite of security solutions and key design principles	Establish organisational guidelines and principles for the design of OT security architecture and controls, and drive the enhancement of organisation-wide OT security systems	
Knowledge			• Security threats and vulnerabilities facing OT systems • Levels of security assurance and functional requirements • OT security system components • Elements and workings of security controls • Objectives and purpose of security controls • Common specifications and designs for secure OT systems • Types of models for OT secuirty (such as Incoporation of Purdue Model for ICS Security (PERA)) • Methods to acess OT systems	• Emerging security threats and impacts on OT systems • Key components of OT security system blueprints • Principles of security system integration • Range of OT system security tests and interpretation of results • Evaluation guidelines for OT system secuirty architectures • Interdependencies between OT systems	• Industry best practices in OT security architectures and systems design • Emerging trends and potential impacts on enterprise architecture and security controls • Key criteria for determining required level of security controls • New and emerging OT security system design methodologies, tools and techniques • Interdependencies and impact of changes on OT systems	
Abilities			• Identify security risks and problems posed by new technologies integrating with OT systems and assets • Design secure systems and controls based on OT architectural guidelines and	• Evaluate potential security threats and articulate implications on OT systems design • Define security system blueprint for relevant OT systems or infrastructure, including	• Establish organisational guidelines and principles for the design of OT security system architectures and controls • Evaluate OT security system architecture against industry best	

			requirements aligned with business priorities • Define security specifications of system components, that address security objectives and functional requirements • Incorporate controls into OT security system components to minimise security breaches or lapses • Assess the level of security robustness in OT system designs	protection profile and security targets • Integrate security solutions and design principles to develop a robust and coherent OT security architecture • Lead design of new or enhanced OT security systems and architectures • Plan and embed security controls for OT systems architecture based on understanding of system interdepedencies, organisational guidelines and security principles • Lead the review of OT system architecture against security requirements • Recommend modifications to OT security control designs to boost the protection of organisation assets	practices and business requirements • Define the level of security controls needed for the organisation's OT systems, information and assets • Plan the design and integration of organisation-wide IT-OT security systems • Endorse new, modified or strengthened security controls that are in line with the organisation's security strategy • Introduce new security system design methodologies, tools and techniques to the organisation • Evaluate OT systems' security plans and interdependencies between systems in view of potential evolution of the enterprise strategy and architecture	

The information contained in this document serves as a guide.

TSC Category	Identify					
TSC Title	OT Cybersecurity Governance and Programme Management					
TSC Description	Develop and implement OT cybersecurity enterprise programs, policies and standards to govern the organisation's approach towards protecting OT systems in alignment with regulations, organisation's context, operating environment and cyber threats					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Facilitate efforts in implementing and tracking of OT cybersecurity programmes and conformance to policies, standards and protocols	Assess adherence of OT cybersecurity policies, standards and protocols, driving the OT cybersecurity programme implementation and monitoring effectiveness	Develop OT cybersecurity policies, standards, protocols and develop plans and resources to implement the programmes	Develop OT cybersecurity programmes at an enterprise level, defining organisation's risk appetite and providing direction for OT cybersecurity policies, standards and protocols
Knowledge			• Organisation cybersecurity policies, standards and protocols • OT cybersecurity programmes and indicators of good practices • Common tools and methodologies in OT security programme development • Maintenance procedures for OT security programmes	• Various OT threats and system vulnerabilities in the OT environment • Implementation process and considerations for cybersecurity policies, standards, protocols and programmes • Types of security controls in the OT environment of the organisation • Methods to assess processes against policies, standards and protocols • Objectives and plans for OT cybersecurity programmes • Metrics to evaluate OT cybersecurity programmes	• Critical elements of corporate security policies, standards and protocols • International OT cybersecurity frameworks • Geographical and sectoral regulations and codes of practices for OT cybersecurity • Policy, standard and protocol writing techniques • Methods to communicate organisation's policies, standards, and protocols • Related operational or business policies, standards, protocols and programmes	• Emerging trends and developments in OT cybersecurity management and practices • Industry standards, regulations and best practices for OT cybersecurity • Key business and operation implication of changes in policies, standards and protocols concerning the OT environment • Methods to analyse cost and benefits of implementing an OT cybersecurity programme
Abilities			• Coordinate efforts with appropriate stakeholder to drive or maintain ongoing cybersecurity programmes • Support the roll out and communication of OT	• Validate compliance of cybersecurity policies, standards and protocols • Highlight areas for improvement and propose solutions or revisions to	• Develop OT cybersecurity policies, standard, and protocols based on the frameworks, regulations, OT cyber threats and	• Define and articulate the organisation's risk appetite and tolerance • Set direction for the organisation's cybersecurity policies, standards, protocols and

			cybersecurity policies, standards, protocols and programmes • Monitor existing process on a daily basis and ensure conformance to OT cybersecurity standards and protocols • Monitor ongoing OT cybersecurity programme and highlight implementation hurdles • Consolidate feedback and concerns of end-users with regards to ongoing OT cybersecurity programmes	cybersecurity policies, standards and protocols • Identify lapses in or potential issues that may endanger the OT environment • Propose specific action plans for different OT area or business units to improve conformance and programmes' effectiveness • Evaluate technologies and tools that can address gaps and facilitate compliance with security policies • Introduce and review adequacy of security controls in line with corporate cybersecurity policies • Implement and partner stakeholders on implementation of new or updated cybersecurity policies, standards, protocols and programme • Drive implementation of OT cybersecurity programmes with other stakeholders • Regularly monitor impact and metrics to determine effectiveness of OT cybersecurity policies, standards, protocols and programmes	risks and organisation's context • Establish internal processes to regularly review the adequacy of security controls • Introduce suitable technologies, processes and tools to maximise compliance and programmes implementation • Communicate and educate the organisation on new or updated policies, standards or protocols and cybersecurity programmes • Develop plans, schedule and resources to implement OT cybersecurity programmes • Collaborate with senior stakeholders to ensure that OT cybersecurity policies, standards , protocols and programme are executable and aligned with other enterprise-level initiatives	programme in line with business requirements and the external environment • Review and endorse proposals for updates or enhancements to organisation's policies, standards, protocols and programmes • Assess overall effectiveness of OT cybersecurity programme and set priorities and improvement activities • Establish benchmarks and targets with regards to OT cybersecurity governance and set processes to be regularly reviewed against • Establish and regularly review OT cybersecurity programmes' strategy and objectives in alignment with organisation's strategic priorities and risk tolerance for OT systems • Lead communication of business case to key leadership roles and ensure buy-in for OT cybersecurity policy changes and programme management

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	OT Vulnerability and Patch Management					
TSC Description	Deploy vulnerability mitigations and patches in phases to minimise operation disruption during testing, deployment and validation to mitigate vulnerabilities in OT systems					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Perform patch testing, deployment and post-deployment validation of patches to identify potential vulnerabilities and conflict with other systems	Analyse and combine various vulnerability and patch management configurations to correct threats and mitigate adverse effect through phased deployment of patches	Establishing patch management strategy through collaboration with other stakeholders to manage testing and deployment of patches while balancing security and operations	
Knowledge			• Vulnerability and patch management configuration tools and techniques • Analysis and verfication process, tools and techniques for testing effectiveness of patch • Internal guidelines for managing vulnerability and patch deployment, validation and user-access • Types of system conflicts created when implementing external vendor patches and resources	• Range of patch mangement configuration techniques • Internal stakeholders requirements and guidelines for patching of OT systems or embedded devices • Threats posed by relevant stakeholders provided with access and privilege to OT systems or embedded devices • Types of interactions and possible conflict during patch deployment by internal and external stakeholders • Tools and techniques for safe deployment of patches in OT systems or embedded devices	• Host architectures (Appliances, mobile devices, laptops, firmwares) and interdependencies with OT systems for patch updates • Vulnerability and patch management techniques and strategies and their implications on OT system operations and legacy systems • Industry best practices, frameworks and developments in vulnerability and patch management • Tradeoffs between patch security, usability and availability of OT systems	
Abilities			• Monitor environment to ensure OT systems are up-to-date and are in compliance with internal patch processes	• Develop change management plan and procedures to facilitate systematic and timely approach to reduce vulnerability exposure	• Spearhead collabaration with stakeholders in prioritising and planning vulnerability and patch deployment efforts in	

			• Consolidate and group OT systems in the organisation according to the different configuration methods and highlight legacy systems that are no longer supported by vendors • Coordinate with vendors, asset owners or relevant stakeholders to ensure smooth deployment of patches or other modifications to OT assets and systems • Evaluate severity of vulnerabilities and weaknesses and prioritise actions to undertake • Execute patch testing and implementation in line with identified phased roll-out • Conduct post-patch verification through further testing of vulnerabilities • Monitor feedback from other stakeholders to determine possible unintended side-effect from patch updates	while ensuring ongoing operations to OT systems • Evaluate legacy OT systems exposed to potential vulnerabilities • Propose and prioritise alternative patch solutions • Define roles and responsibilities for involved parties across the industrial environment to facilitate patch management processes • Manage guidelines on vulnerability and patch management configuration to standardise efforts to mitigate conflict and disruption • Conduct vulnerability and exposure reviews of OT assets and identify preventative action when threat vulnerabilities and weaknesses are detected • Execute planning, testing and implementation of patches in phases for safe deployment and to minimise disruption and unauthorised traffic • Analyse post-patch validation data to determine if further actions are required	phases on a combination of platforms and systems to prevent overloading of resources and other networks • Lead creation of alternative vulnerability and patch management strategies for legacy OT systems that are no longer actively patched by vendors • Asses industry trends and emerging threats to inform ongoing patch management strategies • Establish internal policies for the management, optimisation and protection of the organisation's assets in alignment with business priorities and industry standards • Plan appropriate tools and techniques for the safe deployment of patches to reduce unauthorised interaction between control and operation servers • Evaluate data from existing systems to determine if additional follow-up patches are required	

The information contained in this document serves as a guide.

TSC Category	Identify					
TSC Title	Supply Chain Management					
TSC Description	Manage OT cybersecurity risks associated with services or systems that are dependent on vendors or external entities through formulation of frameworks, guidelines and processes					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Monitor service levels, review and report service delivery deviations	Analysing the effectiveness of existing initiatives in evaluating the cybersecurity compliance of vendors	Design processes in conjunction with various stakeholders to ensure OT cybersecurity compliance to mitigate risk posed	Spearhead the creation of frameworks, processes and guidelines to develop a secure and agile supply chain
Knowledge			• Methods for data collection and analysis • Organisational procedures for escalation and reporting of service level agreements (SLAs) breaches • Service performance, conformance testing and assessment measures • Key performance indicators to measure supply chain systems	• Types of cybersecurity risks and vulnerabilities impacting OT sysetems • Types of supply chain interdependencies • Organisational standards and guidelines for service delivery • Communication channels and methods • Diagnostic methods and tools • Service resolution procedures and techniques	• Organisation's OT cybersecurity risk assessment and prioritisation frameworks and processes • Types of threats posed by interdependencies and variability in the supply chain • Service recovery policies and methods • Stakeholder relationship development concepts and techniques	• OT cybersecurity emerging trends and threats • OT cybersecurity frameworks, legislation and requirements • Various types of OT system vulnerabilities and potential threats • Alternative suppliers of specialised and sensitive OT equipment
Abilities			• Monitor service delivery in accordance to established service level agreements and compliance with contractual obligations • Evaluate vendors' performance against conformance testing, assessment, performance standards and benchmarks • Assess gaps in service delivery and identify potential issues or breaches that would	• Communicate roles, responsibilities and expectations to vendors or external dependencies in delivering associated products or services in alignment with cybersecurity requirements • Identify critical depdencies and associated risks across the end-end supply chain management process of OT systems	• Establish supplier risk profile to assess overall security posture of vendors and dependencies • Lead evaluation and prioritisation of supplier risk profile and dependency risk in line with organisation's risk criteria and frameworks • Define clear parameters and expectations of vendors' roles and responsibilities in alignment with establish cybersecurity requirements and	• Spearhead review of existing vendor management and selection framework to formulate consideration of abilities to meet cybersecurity requirements against internal or regional standards • Formulate supply chain OT cybersecurity risk management framework to guide procedures and information sharing on OT cybersecurity incidents, threats or mitigation measures • Lead communication of cybersecurity risks

			impact cybersecurity on OT systems • Consolidate feedback from end-users and external depencdencies to analyse future demands and needs to deliver secure OT systems and assets • Facilitate information sharing on relevant OT cybersecurity information or incidents	• Establish key performance indicators for assessment of vendor service delivery, conformance testing, assessment and performance levels • Review dependencies' ability to continually meet cybersecurity requirements for delivery of services and identify actions for improvement of service levels • Evaluate the impact of contractual issues and problems on cybersecurity of OT systems, and determine if a major contractual breach has occurred • Identify stakeholders to be involved in information-sharing processes based on shared interest in risk to OT systems and assets	controls to protect the organisation against cybersecurity threats • Establish processes to enable the monitoring of service performance and validate compliance with cybersecurity requirements • Collaborate with relevant stakeholders to build OT cybersecurity awareness for external dependencies on prevailing OT cybersecurity threats, impacts and mitigations • Develop contractual provisions to pre-empt and address significant OT cybersecurity risks associated with varying dependencies • Evaluate overall performance of vendors to review and endorse decisions on future contract renewals, changes or termination • Assess the proportion and type of clients served by the vendors for potential conflict of interest and threats • Establish alternative sourcing plans in the event of operation disruptions	posed by supply chain dependencies and gain buy-in for proposed mitigation or actions to from key stakeholders • Establish organisational cybersecurity requirements across OT systems and dependencies in consultation with key stakeholders • Establish benchmarks against regulatory standards to guide the development of supply chain framework from a OT cybersecurity perspective • Formulate detection strategy for critical components in the supply chain to detect for early signs of compromise • Assess need to renegotiate the terms of SLAs or outsourcing contracts in the event of new legal or regulatory requirement
Range of Application	• Suppliers • Customers • Single-source or other essential dependencies					

The information contained in this document serves as a guide.

TSC Category	Respond and Recover					
TSC Title	Business Continuity and Recovery					
TSC Description	Plan, design and test contingency plans to ensure organisational resilience and maintenance of the availability, stability and integrity of OT systems in the events of cybersecurity incidents					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Implement business continuity and contingency procedures and exercise, and management of alternative resourcing of critical OT systems	Develop business continuity plans for OT systems, and direct resources to establish and maintain business continuity processes	Define the optimal business continuity strategy and objectives for business continuity and contingency plans for OT systems to minimise disruption and threats to stakeholders	
Knowledge			• Data information processes and procedures • Steps required to implement and test business continuity plans and procedures	• Interlinkages between OT systems and stakeholders involved • Potential long-term and short-term risks to the availability, stability and integrity of OT systems • Business continuity and recovery procedures • Techniques to analyse continuity plan tests	• Regulatory requirements and industry best practices for business continuity and recovery strategy and plans • Potential risks posed to stakeholders in the events of a disruption • Potential disruption and adverse impact during the testing of contingency plans • Strategies to analysis risk of disruptions to operations and stakeholders	

Abilities			• Collate information to identify critical OT systems to be considered for business continuity • Facilitate the identification of the interdependences that exist in driving availability, stability and integrity of OT systems • Coordinate efforts to execute business continuity, recovery and contingency procedures for OT systems based on organisational strategies • Facilitate OT cybersecurity or business continuity exercises based on defined objectives, action plans and criteria • Document test results and propose follow-up actions to achieve desired levels of business continuity	• Assess interdependencies that exist among the critical OT systems and stakeholders to guide formation of continuity plans • Evalute the relative impact of potential risks to the availability, integrity and reliability of key OT components • Develop business continuity procedures outlining tasks, responsibilities and schedules in alignment with the organisation's security strategy • Recommend process enhancements to achieve improved levels of business continuity • Develop a business continuity test or exercise plan, including its objectives, procedures, assessment criteria and roles and responsibilities of involved personnel	• Lead formulation of business continuity and recovery plans for critical OT systems in consultation with relevant stakeholders • Segregate business operations into key components of business operations to determine priority areas with cascading levels of acceptable OT system performance • Assess and identify key interdependencies and reliances across external stakeholders beyond the organistion • Guide the definition of the organisation's system and data recovery objectives based on organisation needs, industry best practices and regulatory standards • Guide the definition of continuity assessment benchmarks to ensure that plans are relevant, adequate and closely aligned with the	

				• Analyse the long-term outage and short-term outage of critical OT systems implications on business operations • Define frequency of change for critical data and configuration and requirements for ensuring completeness of back-ups	organisation's needs and priorities • Evaluate overall result of OT systems business continuity exercise and effectiveness of contingency plan to determine implicationsand prioritise areas for further review and improvements • Evaluate the need to source for critical alternative components or to develop alternative processes while balancing costs to achieve desired level of business continuity • Formulate backup and restoration policy considering criticality of OT systems and frequency of change for critical data and configuration	

TSC Category	Respond and Recover					
TSC Title	Failure Analysis					
TSC Description	Examine the root cause of OT system failures and execute appropriate analysis and mitigation techniques for both physical and digital incidents to ensure compliance with organisational and regulatory requirements					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Support and respond to failure incidents and initiate process of failure analysis	Conduct failure analysis to determine cause of defect and impact to OT assets	Lead failure analysis and review the results to determine root causes	Outline procedures, guidelines and plan failure analysis activities and lead communication and remediation plans	
Knowledge		• Organisation's OT system and network • Organisational procedures and processes for safety and failure analysis in the OT environment • Allowable down-time of OT systems for failure analysis	• Types of OT cyber incidents and failures • Physical attributes of OT system • Physical safety guidelines of the organisation • Procedures to conduct physical failure analysis • Failure analysis tools and techniques for OT systems	• Potential root causes of failure in the OT systems • Root cause analysis • Failure analysis tools and techniques for OT systems • Types of failure analysis techniques and procedures for OT systems • Stakeholders mapping with regards to OT failure incidents	• Regulatory and organisational requirements for OT system failure • Risks and operation implication of conducting failure analysis in the OT systems • Industry best practices and emerging trends in OT failure analysis	
Abilities		• Respond to failure incidents and initiate appropriate process for failure analysis according to organisation guidelines and procedures • Draft failure report and incident log for review • Support communications with asset owners and other stakeholders in preparation for failure analysis	• Evaluate incidents and identify appropriate failure analysis technique • Execute failure analysis on OT systems in line with organisational guidelines and procedures • Review failure reports • Conduct physical failure analysis on OT systems, keeping abreast of organisation's safety guidelines • Prepare communication materials and conduct communication session	• Review failure incident to determine appropriate failure analysis procedures for physical and digital assets • Identify and segregate list of possible failure techniques for potential physical and cyber incidents and appropriate • Define time-frame for failure analysis to minimise operation disruption • Analyse result of failure reports and develop remediation plans	• Create process and guidelines to document and conduct failure analysis activities • Incorporate and update organisational and regulatory requirements into failure analysis process • Set the depth and level of analysis standards required for compliance with regulatory and organisational requirements • Identify best practices and emerging technology in the failure analysis field • Assess and approve changes to existing processes and	

			with internal stakeholders	• Assess root causes of failure outlining lesson learnt and and recommend remediation actions • Supervise the failure analysis activities • Communicate findings to asset owners and other stakeholders • Collaborate with stakeholders and key asset owners to develop failure analysis processes	procedures to improve failure analysis activities • Engage operation team, asset owners and other key stakeholder in planning failure analysis activities balance and minimise operational disruption and risk • Lead communication efforts of findings and remediation plan	

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	Network Administration and Maintenance					
TSC Description	Monitor to provide for optimum levels of network performance and minimisation of downtime. This includes detection, isolation, recovery and limitation of the impact of failures on the network as well as provision of support to system users through ongoing maintenance information sharing and training					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Monitor network performance, investigate and resolve network faults or downtime	Review, optimise and align network performance with operation needs, and ensure adherence to configuration rules	Assess network capabilities and set network rules to support OT networks and systems, as well as and optimise performance in changing environments		
Knowledge		• Purposes of OT systems and their dependencies on network • OT network performance indicators and methods to assess them • Detection, identification, isolation and limitation techniques of network faults and failures in the OT environment • Potential causes and impacts of network faults or downtime • Resolution techniques for a range of different network issues in the OT environment • Critical information to be communicated to the organisation regarding network updates	• OT network visualisation and modelling • Impact of network performance on OT operations • Best practices in network administration and maintenance in the OT environment • Priorities, audience and dependencies with regards to communicating network updates in the OT environment • Relevant programming languages for applications • Indicators of network performance	• Industry best practices in fault detection, isolation and recovery in the context of network administration in the OT environment • Resources and capability requirements to support software-defined infrastructure in the OT environment • Network virtualisation management and monitoring tools and methods • Scope of multi-tier networking in OT environment • Range of network rules and programming codes • Semantics of different networks and network types in the OT environment		
Abilities		• Monitor network performance in the OT environment • Highlight areas for further review to optimise network performance	• Conduct review and evaluation on network performance in the OT environment and determine areas for improvement	• Establish guidelines and Standard Operating Procedures (SOP) to detect and recover network faults and failures in the OT environment		

		• Identify potential impact of network faults and failures • Take appropriate action to isolate or limit network faults and failures in the OT environment • Resolve network faults and failures in the OT environment • Investigate the causes for unresolved faults and propose solutions to address them • Develop required communication materials for information sharing	• Optimise and align network performance with operation and business needs • Assess incidents of network faults, failures or downtime in the OT environment and determine recovery and resolution efforts • Determine network updates and maintenance information and customisation for different audiences • Ensure adherence to established configuration baselines or rules for network security • Monitor performance and health status of applications, controllers and components in the OT environment • Implement adjustments to network-wide traffic flow to meet changing needs	• Establish OT network maintenance processes to ensure performance is stable and optimal for the operation • Assess the readiness of equipment and capabilities in the OT environment for emerging software-defined infrastructure • Determine network rules and desired behaviours to be programmed in to meet the OT network requirements • Establish configuration baselines or rules for network security across the OT environment • Direct overall network programming activities and performance, determining adjustments to be made in light of changing contexts and environments		

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	Access Control Management					
TSC Description	Manage access controls to ensure authorised access for OT assets and systems in accordance with the organisation's policies, including creating and managing identities					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Apply access control policies by following the access limitation and responsibilities granted	Develop access control policies in alignment with the organisation's policies and cybersecurity advisories	Develop organisational access control frameworks to determine granting and revocation of user access control rights	
Knowledge			• Access enforcement methods • Remote access methods • Wired and/or wireless authentication methods • Least privilege principles • Account management principles • Access control technologies • Troubleshooting tools and techniques • Access control methods • Wired and/or wireless access restrictions • Authorisation methods	• Types of access control systems • Access control rogue connection audit techniques • Access control risk mitigation techniques • System interfacing • Investigative techniques • Root cause analysis techniques	• Organisational access control needs • Financial costs for access control changes • Laws and regulations related to cybersecurity • Stakeholder communication channels • Policy-based and risk adaptive access controls • Best practices, industry standards and emerging trends for access control	
Abilities			• Establish and maintain identities through provisioning and de-provisioning for personnel and other entities who require access to OT systems or assets • Perform troubleshooting for verified users with access control issues • Grant users access control rights according to defined frameworks and best practices • Manage access control lists • Maintain audit logs and ensure ensuring proper	• Review and update identity repositories and credentials to ensure validity • Define time threshold for provisioning and de-provisioning of identities • Deploy appropriate control systems utilising appropriate models based on understanding of OT systems and needs • Solve system interfacing issues or problems • Perform audits on access control systems to identify rogue connections	• Formulate requirements for identity credentials in alignment with organisation’s risk criteria • Establish policies and procedures specifying the usage of system resources by only authorized users, programs, processes, or other systems • Define organisational access control frameworks for managing system accounts, including establishing, activating, modifying, reviewing,	

			access habits are enforced	• Analyse and recommend mitigation measures to reduce access control breaches • Design group policies and access control lists to ensure compatibility with organisational standards and needs • Assess adequacy of access controls based on principles of least privilege and need-to-know	disabling, and removing accounts in alignment with relevant industry standards • Define controls for addressing the use of portable and remote devices and personally owned information systems to access the OT systems as well as the use of remote access capabilities and the implementation of wireless technologies • Determine communication plans with relevant stakeholders on access control breaches • Develop access control audit frameworks • Evaluate and adopt new access control technologies • Champion best practices on access controls to protect OT systems and assets from unauthorised access and are put into place	

The information contained in this document serves as a guide.

TSC Category	Respond and Recover					
TSC Title	Cyber Forensics					
TSC Description	Perform forensics investigations on cyber-related incidents on OT systems through preservation of digital evidence					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Coordinate the cyber forensics execution of collection and preservation of evidence	Gather and preserve digital evidence from different systems and sources following authorised procedures and provide preliminary analysis from consolidated digital evidence	Perform in-depth investigation activities and forensic analysis	Establish forensics policies and procedures to effectively manage forensic investigations and recovering of operations	
Knowledge		• Procedures used to acquire, preserve and maintain integrity of evidence • Safe handling techniques for physical safety and to prevent contamination or tampering of evidence for different OT systems	• Potential types of data from physical and digital assets, found internally and externally • Range of analytical techniques to examine digital evidence • Conflicts with integration of broad range of OT systems, computer, network and mobile forensic tools and techniques • Statistical analysis procedures used to identify trends • Legal principles and regulations in relation to forensic investigations	• End-to-end process and procedures in a forensics investigation • Critical asset owners and stakeholders involved in digital evidence gathering • Emerging and specialised forensic tools, solutions and methodologies • Changes and updates to regulatory or legal requirements • Implications of regulatory and legal parameters on forensic investigations	• Live forensics and impacts on OT system networks • New and emerging trends in OT forensic investigation • New and emerging trends in the OT and related fields • Impacts and consequences of OT forensics investigation policies and procedures on organisational operations • Legal and regulatory requirements for OT forensics investigation	

Abilities		• Facilitate collection and preservation of digital evidence in consultation with relevant stakeholders • Coordinate execution of forensic investigation plan in compliance with organisational physical safety guidelines • Monitor a range of internal and external OT data sources to identify relevant information to incident at hand	• Combine digital evidence and identify patterns, or unauthorised access from digital evidence • Combine digital evidence from several sources and methods to analyse forensic evidence, document inferences, patterns and correlation of events to draw evidence • Prepare report on digital forensics finding in compliance with legal regulations and standards • Access and extract evidence from OT systems utilising appropriate forensic tools • Document OT system security incidents including detail, trend and handling • Store original and copied evidence in safe environments with limited access • Extract digital evidence from various sources, in compliance with authorised procedures	• Perform investigation activities and forensic analysis to determine the underlying causes and effects of incidents • Establish processes to facilitate the digital evidence acquisition to minimise impact to OT systems functionality and uptime • Assess suitability of new and emerging forensic tools, given investigation requirements and OT operation requirements • Determine the key tasks, timelines, milestones and accountabilities for a specific forensic investigation • Lead forensic investigations, involving interaction with OT systems involving time-sensitve, critical OT assets, large data sets and networks considerations • Review multi-source evidence and conclusions drawn in light of broader trends and contextual considerations • Identify alternatives and solutions for potential barriers and conflicts for communication between investigative methods, tools, procedures and OT systems that prevents data collection	• Develop forensic investigation plan, including the tools, processes and methodologies to be used • Develop guidelines and Standard Operating Procedures (SOP) for investigation procedures including guidelines for physical and digital interviews, data handling, surveillance etc. • Identify types and time-sensitivity of data gathered from OT systems • Collaborate with external vendors to identify appropriate forensics tools and potential conflict with integration to OT systems • Assess and approve recommendations for changes to minimise impact to OT systems and improve the digital evidence integrity validity • Formulate plans to identify types of data and appropriate methods and tools required to acquire digital evidence from OT systems while minimising impact to digital evidence integrity validity • Lead presentation of reports and outcomes in significant investigations or legal proceedings	

The information contained in this document serves as a guide.

TSC Category	Respond and Recover					
TSC Title	Cyber Incident Response and Management					
TSC Description	Detect and report cyber incidents in the OT environment, identify affected systems and user groups, trigger alerts and announcements to ensure efficient resolution of the situation					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Conduct real-time incident and status reporting in the OT environment and identify affected systems	Troubleshoot incidents, escalate alerts to relevant stakeholder, and analyse root causes and implications of incidents	Develop incident management procedures and synthesise incident-related analyses to distil key insights, resolve incidents and establish mitigating and preventive solutions	Formulate incident response strategies and direct teams in the remediation, resolution, communication and post-mortem of large-scale, unpredictable OT cyber incidents	Drive cross-collaboration efforts to co-develop strategies to manage OT cyber incidents on an industry, national or international scale
Knowledge		• OT systems and network in the organisation • Incident detection and reporting protocols • Types of security incidents • Types of threats, cyber attacks and breach in the OT environment • Categorisation guidelines for incidents • Impact of incidents on systems and operations	• Prioritisation criteria for OT incidents • Procedures and processes to conduct Root cause analysis and timeline analysis of OT incidents • Tools and processes to conduct remediation of OT cyber incidents • Security implications of incidents	• Mechanics of incident alert triggers in the OT system • OT cyber Incident remediation solutions and strategies • OT cyber Incident mitigation strategies	• Industry standards and best practices in incident management in the OT environment • Key components of an incident management playbook for the OT environment • Criteria and requirements of an OT incident response team • Key stakeholders for OT incident management • Post-mortem processes for OT cyber incidents • Communication strategies and protocols • Prosecution processes and requirement related to cyber attack	• Political, national and international sensitivities regarding cyber crimes in OT sectors • Potential impact of incidents to the organisation and stakeholders and community • Best practice and types of OT cyber incident management strategies • Risk mitigation strategies for OT cyber incidents • Procedures to manage OT cyber incidents on an industry, national or international scale
Abilities		• Provide real-time status reporting on affected OT systems • Maintain logs of incidents • Report incidents, in line with incident management protocols • Gather relevant information or collection of evidence from stakeholders and	• Review categorisation of incidents in the OT environment and determine its priority level • Conduct containment of cyber incidents in the OT systems • Escalate alerts to relevant stakeholder groups upon the occurrence of incidents to facilitate execution of information collection plan of evidence	• Define incident alerts mechanisms, processes and relevant parties in the OT environment • Develop a holistic view of OT incidents by integrating information, data, alerts and analysis from detection system logs to • Distil key insights and impact from analyses of incidents	• Establish incident management procedures for the detection, reporting and handling of incidents in the OT environnment • Develop a playbook for OT cyber incident management • Lead the remediation and resolution of cyber and data incidents at the organisational level	• Direct the management of OT cyber incidents on an industry, national or international scale • Manage OT cyber incidents to minimise significant reputational risk to the organisation • Lead collaboration across industries to manage manage OT cyber risk and incident management • Co-develop incident management strategies

		asset owners about incidents • Categorise the importance of incidents based on established guidelines • Identify the OT systems and affected parties by the incident based on information gathered • Assist in mitigation of incidents as directed • Document the modifications made to troubleshoot and resolve problems or incidents in the system • Coordinate efforts to facilitate incident response processes across different stakeholders	• Perform first responder troubleshooting by following pre-determined procedures • Analyse incident reports, log files and affected systems to identify threats and root causes of incidents • Perform incident triage to assess severity of incidents and security implications • Implement plans and processes for remediation	• Manage the containment of incidents within the organisation • Lead recovery and preservation of key evidence in line with organisational needs of contained OT incidents • Establish and drivee the implementation of mitigation and prevention processes and policies	• Resolve large-scale, unpredictable OT cyber incidents • Develop framework and lead the communication activities to different critical stakeholders • Direct post-mortem activities following critical incidents in the OT environment • Develop OT cyber incident mitigation strategies • Support the legal action and prosecution activities where necessary • Collaborate with key internal stakeholders, external stakeholders, OT system vendors and asset owners to create evidence collection and preservation plans	on a national level with external experts and stakeholders for the OT sectors • Lead critical communications to the public, authorities, internal and external stakeholders • Define required standards of preservation of evidence in line with organisational legal or regulatory needs

TSC Category	Detect					
TSC Title	Penetration Testing					
TSC Description	Conduct penetration testing to reveal vulnerabilities or lapses in the existing OT systems					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Conduct authorised penetration testing of OT systems to expose threats	Design security testing plan, and perform advanced, authorised penetration testing	Authorise and establish organisation guidelines and strategies for penetration testingfor OT systems, and determine the future-readiness of the organisation's security posture	
Knowledge			• General process and technical requirement for penetration testing of OT systems • Penetration testing techniques and methodologies for OT systems • Penetration testing tools and their usage for OT systems • Range and types of security loopholes and threats	• Organisational objectives of penetration testing • Key components and methodologies in the design of security testing activities • Types of risk implications of penetration testing for OT systems • Penetration testing techniques, tools and their usage for OT systems • Range and types of security loopholes and threats	• Design guidelines and best practices for penetration tests • Organisation priorities and OT security objectives • New and emerging trends in cyber-attacks, hacking techniques and security threats • Cost-benefit analysis between conducting penetration testing OT systems and maintaining operational uptime	
Abilities			• Perform technical coordination of penetration testing according to test plan templates • Conduct authorised penetration testing of OT systems consisting of a range of penetration testing methodologies, tools and techniques • Assess current security practices and controls	• Design security testing plan involving key stakeholders and asset owners for penetration testing activities • Manage the implementation and scheduling of penetration testing activities, in line with the organisation-wide strategy • Evaluate potential risks and, such as	• Establish organisation guidelines and methodologies for the design and conduct of penetration testing activities • Develop implementation strategies for penetration testing activities to ensure organisation-wide consistency of information security plans	

			performance against expected performance during penetration testing attempts • Develop a penetration testing report, highlighting key threats and areas for improving OT system security	operational or safety risks, of conducting penetration testing on OT systems • Identify alternative penetration testing techniques and methodologies for OT systems which minimise risk of disruption, such as creating system digital twins or back-up air-gapped OT environments • Conduct advanced, authorised penetration testing of highly complex and secure OT systems • Determine possible impact of penetration testing on organisational OT operations to inform penetration testing strategy	• Prioritise different levels of identified potential risks, and key areas of OT systems for specific tests to be conducted to minimise downtime to OT systems • Authorise penetration testing activities on organisation's systems, in line with business priorities and security requirements, partnering with stakeholders across the organisation to evaluate wider risk impacts of penetration testing • Synthesise key organisational implications from penetration testing reports and propose appropriate follow-up actions to relevant stakeholders • Refine and propose penetration test plan templates to model after evolving trends in the landscape	

The information contained in this document serves as a guide.

TSC Category	Analyse and Detect					
TSC Title	Threat Analysis and Defence					
TSC Description	Conduct analysis of new and incoming threats, to examine their characteristics, behaviours, capabilities, intent and interactions with the environment as well as the develop defence and mitigation strategies and techniques to effectively combat such threats					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Perform static, dynamic or behavioural analysis on malicious code and threats, debug malware, thraw attacks and document incidents	Examine threat behaviours and capabilities and circumventing anti-analysis mechanisms, recommending techniques to block and mitigate malicious code and attacks	Define and establish an enterprise threat defence and mitigation strategy, incorporating new techniques to combat emerging threats and attacks	
Knowledge			• Types of threats or malware • Patterns of common malware characteristics • Mechanism of malware • Various file formats of malicious threat types • Programming languages which malware are created from • Types and usage of static, dynamic and behavioural analysis tools • Types and usage of anti-malware tools	• Types and characteristics of new and emerging threats • Range of malware analysis techniques • Core concepts for reverse-engineering malware at the code level • Anti-analysis mechanism in anti-disassembly, anti-debugging and obfuscations mechanisms • Techniques to circumvent anti-analysis mechanisms Malware defence techniques	• Industry developments and trends in threat analysis and defence • New and emerging techniques in threat analysis • Different enterprise threat mitigation strategies, approaches and critical considerations • Principles underlying threat defence and analysis strategies and methodologies • Long-term trends and evolution in the types and perpetrators of threats and attacks	

Abilities			• Debug malware with debuggers and monitoring tools to gather information on malware • Correlate stages, actions or malicious commands in an attack • Perform static and dynamic analysis of malicious code and executables • Implement behavioural analysis tools to understand nature of threats affecting OT systems • Utilise anti-malware and threat gateways to thwart malicious attacks • Generate reports on incidents and threats identified, and highlight newly identified vulnerabilities in OT systems • Draft recommendations to mitigate malware, exploit kits and attacks • Document threat specimen's attack capabilities, propagation characteristics and threat signatures	• Apply countermeasures to circumvent or subvert anti-analysis mechanisms • Unpack protected malicious executables • Evaluate and make recommendations to existing strategies to incorporate lessons learn from incidents • Utilise a combination of analysis techniques and reverse engineering techniques to determine threat characteristics and capabilities • Conduct in-depth examination of malicious threats to understand the behaviour, capabilities, intent and interactions with the environment • Recommend proactive steps to combat and mitigate malicious code, threats and attack • Assess incidents and threats identified by systems and determine if existing mitigation strategies are effective • Identify emerging and complex threats from malicious software and codes and modify existing techniques or develop new ways to block malicious code and attacks	• Evaluate threat analysis, outcomes and reports to identify potential vulnerabilities and impact to the OT systems, building a clear picture of the overall attack surface • Establish organisation threat protection and defence strategy, balancing protection, safety, operations, capability and cost • Approve recommendations to strategies to improve effectiveness in mitigating current and potential threats to OT systems • Lead internal cross-functional communications on threats to OT systems, building awareness across the organisation • Formulate relationships with stakeholders externally to stay abreast of new and emerging threats, attacks and anti-detection mechanisms in the OT landscape • Define threat techniques to combat emerging or emerging forms of attacks • Employ new methods or tools to analyse malicious software and attacks	

The information contained in this document serves as a guide.

TSC Category	Protect					
TSC Title	Threat Intelligence and Detection					
TSC Description	Monitor and anticipate potential threats to OT systems and its components					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Perform security monitoring and interpret logs to detect anomalous activity, intrusions and threats	Implement intrusion detection technology and analyse multi-source information to identify vulnerabilities, potential exploits, methods, motives, and capabilities	Develop strategies to monitor threats and project future technical cyber threat scenarios and present mission reports to key stakeholders	Establish a threat intelligence strategy and direct analysis and integration across various sources to present a robust view on threats, perpetrators, motivations and modus operandi	
Knowledge		• Methods and tools for monitoring network activities, systems and mechanisms • Intrusion detection techniques, software, and their functions • Types of security threats and intrusions affecting OT systems • Security protocols, standards and data encryption • Indicators of attacks • Attack patterns and threat vectors • Techniques, methods and technologies in threat data collection	• Range of intrusion detection and monitoring technologies for OT systems • Applied principles and tools of information security • Techniques for analysis and integration of threat data • Relevant data sources of threat intelligence in the form of firewall logs, intrusion detection system logs, open source internet searches, honeypots • Types and features of exploits and malware	• Mechanisms for threat detection and monitoring for OT systems • Advanced statistical and trend analysis techniques • Emerging trends and developments in OT cybersecurity • Types of impact analyses of cyber threats for OT systems • Range of possible tactics, techniques and procedures used for security attacks • Key components and objectives of intelligence products and mission reports	• Multiple fields in cyber intelligence, including intelligence collection operations and cyber counter-intelligence • Emerging threats, perpetrators, doctrines and methods of operation • Types of business, financial, operational and safety impacts of cybersecurity threats	
Abilities		• Perform security monitoring to detect intrusions utilising appropriate tools and applications • Monitor access control mechanisms, network activities and operating systems • Interpret information from logs and scanners to detect threats and intrusion attempts	• Identify resources and technologies required for intrusion detection according to technical and cost guidelines • Implement intrusion detection and analysis based on key objectives and stakeholders' requirements • Analyse collected information to identify	• Develop strategies for threat monitoring and tracking efforts across enterprise systems • Synthesise multiple information sources and analysis reports into a holistic view of potential threats • Draw insights about the potential impact of	• Formulate mechanisms and processes for detection and identification of cybersecurity events as well as collation and analysis of events, threats or incidents affecting OT systems and its components • Manage the research, analysis, and data integration across a wide	

		• Apply detection technologies, checks and techniques to identify anomalous activity and patterns • Identify indicators of attacks during the detection process • Escalate security threats or intrusions detected with with relevant parties	vulnerabilities and potential for exploitation • Review multiple sources of data and intelligence feeds • Conduct intelligence analysis of OT cyber activities to identify entities of interest, potential methods, motives, and capabilities • Assess and identify critical contextual information for cyber events	estimated cyber threat scenarios for OT systems • Develop threat hunting and intelligence reports so as to present analysis of threat data to key stakeholders • Lead comprehensive evaluation of the capabilities and activities of cyber criminals, foreign intelligence entities or perpetrators • Conduct in-depth research into OT cybersecurity issues of industry-wide or nation-wide significance • Produce findings to help initialise or support law enforcement and counterintelligence investigations or activities	variety of information sources • Determine the tactics, techniques and procedures used for intrusions and attacks on OT systems • Present an informed and robust point of view on both current and anticipated threats, perpetrators, motivations, doctrine and modus operandi • Articulate significance of evolving OT cybersecurity threats to critical decision-makers and senior management in the organisation • Present policy recommendations and impact assessments to critical industry stakeholders and leaders	

TSC Category	Detect					
TSC Title	Vulnerability Assessment					
TSC Description	Conduct threat modelling and vulnerability assessment to reveal vulnerabilities or lapses in the existing OT systems					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Execute vulnerability scans and conduct research on exploitation of OT system vulnerabilities, interpreting findings to identify security lapses	Conduct authorised testing of OT systems to expose threats, vulnerabilities and potential attack vectors in systems	Design security testing plan, and perform advanced, authorised testing as well as intelligence analysis on cyber attack incidents	Authorise and establish organisation guidelines and strategies for security testing for OT systems, and determine the future-readiness of the organisation's security posture	
Knowledge		• Application and usage of basic vulnerability assessment tools and tests for OT systems • Types of OT system security vulnerabilities and threats • Internal and external security standards	• Process and techniques for secured source code review • Threat modelling techniques • Network monitoring tools and their usage • Vulnerability assessment tests and interpretation of results • Range and types of security loopholes and threats	• Organisational objectives of vulnerability assessment • Key components and methodologies in the design of security testing activities • Advanced threat modelling, hacking, and source code review techniques • Data and trend analysis in cyber attacks	• Design guidelines and best practices for threat modelling, vulnerability assessment and source code review • Organisation priorities and OT security objectives • New and emerging trends in cyber-attacks, hacking techniques and security threats	
Abilities		• Perform technical coordination of vulnerability assessments according to test plan templates • Execute vulnerability scans on smaller systems, using basic vulnerability assessment tools and tests • Document the results of security assessments and tests, according to test plan guidelines • Identify security lapses in the system or security mechanisms, based on issues documented from	• Carry out threat modelling and secured source code review • Deploy a suite of network monitoring and vulnerability scanning tools to assess the threats and vulnerabilities in an OT system • Identify vulnerability exploitations and potential attack vectors into an OT system • Analyse vulnerability scan results to size and assess security loopholes and threats • Evaluate if current systems can overcome	• Design security testing plan and evaluation criteria for vulnerability assessments • Manage the implementation of vulnerability assessments activities, in line with the organisation-wide strategy • Implement advanced threat modelling and source code review techniques • Analyse patterns in incident data to identify new and emerging trends in vulnerability	• Establish organisation guidelines and methodologies for the design and conduct of vulnerability assessments • Lead security reviews, specifying the OT systems, applications, processes, people to be assessed • Develop comprehensive criteria for assessing the effectiveness of security mechanisms and controls • Develop implementation strategies for	

		vulnerability scan results • Record evidence of controls which are inadequate or not duly enforced • Conduct research on threat actors, their techniques and ways in which vulnerabilities in security systems can be exploited	emerging threats and hacking techniques • Assess current security practices and controls against expected performance parameters or guidelines • Develop a vulnerability assessment report, highlighting key threats and areas for improving OT system security	exploitation and hacking techniques • Lead advanced analysis of intrusion signatures, techniques, and procedures associated with cyber attacks • Determine hacking techniques and attacks that the organisation's OT systems are most vulnerable to • Refine test plan templates to model after new and advanced hacking actions	vulnerability testing activities to ensure organisation-wide consistency of information security plans • Synthesise key organisational implications from vulnerability assessments • Evaluate the future-readiness of the organisation's security posture in light of the organisation's mission and the changing technological environment	

The information contained in this document serves as a guide.

TSC Category	Identify					
TSC Title	OT Cybersecurity Education and Awareness					
TSC Description	Drive education and awareness of potential risks, mitigation strategies and best practices in OT cybersecurity; this includes facilitation of communication and training to ensure employee capabilities, adoption and adherence to security policies and protocols.					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Support delivery of security activities and programmes to drive education and awareness of OT cybersecurity in existing work practices	Define activities required to bridge gaps in knowledge and capabilities of key personnel to effectively deliver OT cybersecurity functions and processes to the organisation	Develop communication priorities and strategies in alignment with industrial trends and business priorities to drive awareness of OT cybersecurity and capability development in the organisation	
Knowledge			• Critical elements in OT cybersecurity education and awareness programs • Principles of OT cybersecurity • Types of OT security awareness or delivery methods • Methods to measure effectiveness of security education and awareness programs	• OT cybersecurity education needs and imperatives • Potential threats and vulnerabilities encountered by end-users during operations • Job roles and responsibility requirements in OT cyber security	• Trends and threats in the evolving OT cybersecurity landscape • Strategic partnership building strategies in up-and-coming areas in OT • Key business priorities and security implications across OT and IT systems • Best practices and emerging areas in external training programs and research • Matury of organisation OT cybersecurity and possible exposure to cyber-threats	
Abilities			• Coordinate efforts to drive awareness and understanding of basic OT cyber security concepts and importance of OT cybersecurity to users across the organisation • Identify end-users and key responsibilities involved in delivering OT cybersecurity	• Drive communication and awareness of regulatory matters, best practices, standards, methods and tools in assessing and mitigating OT cybersecurity risks • Define priorities and gaps for OT cybersecurity knowledge and	• Lead critical communications of OT cybersecurity education and awareness programmes • Formulate training timeline, plans, procedures and controls to cultivate a culture of safe OT cybersecurity practices in consultation	

			• Consolidate data and feedback to analyse effectiveness on existing OT cybersecurity education and awareness efforts • Suggest content, structure or approach of OT cybersecurity awareness programmes to maximise effectiveness based on feedback and sentiments gathered • Manage employee queries on potential OT cybersecurity threats and risks in their daily work practices • Collaborate with different departments to execute and incorporate OT cybersecurity practices into existing work practices	capabilities required to drive delivery of OT cybersecurity processes • Develop a business case for OT cybersecurity education and awareness programmes in consultation with relevant stakeholders • Determine outcomes and imperatives of education and training programs aligned with organisation's security priorities • Identify active roles in the OT environment to facilitate thedesign of OT cybersecurity education and training programs aimed to drive understanding of the OT cybersecurity risks relevant to their duties • Oversee cross-communication, collaboration and sharing of knowledge between different departments to increase awareness and bridge knowledge gaps resulting from IT and OT convergence • Identify areas for improvement in the organisation's existing OT education and training programs • Collaborate with key stakeholders to address knowledge	with relevant stakeholders • Establish strategic alliances with partners to implement OT cybersecurity training and ensure the ongoing suitability and competence of personnel, commensurate with the risk to OT systems and security objectives • Lead development of new OT cybersecurity materials in consultation with relevant stakeholders to increase awareness of developing trends and industry best practices • Guide development of cybersecurity education and awareness strategies for specific workforce segments with relevance to OT cybersecurity • Formulate processes to communicate new OT cybersecurity insights to end users in the organisation in a timely manner • Evaluate opportunities to enable cross-communication and collaboration to enable integrated IT and OT responses and awareness of convergence • Review the effectiveness of current education plans in light of developments in the OT cybersecurity landscape and regulatory requirements	

				gaps for key roles in delivering OT cybersecurity and facilitate safer adoption of new working responsibilities	• Endorse improvement to the organisation's existing OT cybersecurity practice, policies and education and training programs	

The information contained in this document serves as a guide.

TSC Category	Organisational Management and Support					
TSC Title	Budgeting[#]					
TSC Description	Prepare organisational budgets to support short- and long-term business plans through forecasting, allocation and financial policy setting					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Prepare business unit's operational budgets	Manage budgeting and forecasting for annual financial and business planning within the business unit	Develop long-term financial plans and budget requirements	Endorse organisational financial and treasury management policies, systems, budgets and plans
Knowledge			• Objectives, parameters and types of budgets • Key principles of accounting and financial systems • Types of data sources and data required to prepare a budget • Accounting principles and practices related to budget preparation • Key principles of budgetary control and budget plans, budgetary control techniques • Requirements of Singapore's taxation policies • Functional objectives and key requirements • Organisational financial data • Financial analytical techniques and methodology • Stakeholders to consult on budget calculations	• Analyse business function strategies, functional objectives and operational plans • Carry out forecasting and budgeting for the financial year • Calculate the business unit's cash flow requirements • Determine the business unit's financing needs for the financial year • Compare budget data with estimations to highlight discrepancies • Report budget calculations and discrepancies to organisation management to facilitate decisions on budget allocation • Ensure adherence to financial controls in accordance with relevant organisational corporate governance and financial policies, legislation and regulations	• Recommend parameters and assumptions for budget forecasting in accordance with organisational needs and market conditions • Prepare financial forecasts to facilitate financial and business planning • Implement budget plans to manage resource allocation to business activities • Manage actual budget to enable financial operation n to be measured against forecasted business plans • Monitor budget outcomes to ensure proper utilisation and accounting of resources against their intended purposes • Present financial forecasts, budgets and budget outcomes to immediate supervisors for review and approval	• Determine short- and long-term financial needs to assess current financial situations • Formulate financial plans aligned to overall organisational strategies • Allocate budget resources in accordance with organisational financial plans • Review financial forecasts to anticipate changes in business and operational circumstances • Review draft budgets in accordance with organisational guidelines • Monitor and evaluate actual expense figures against budget to identify and address variances • Report findings, recommendations and options to organisation management for review in accordance with organisational policies

Abilities			• Analyse business function strategies, functional objectives and operational plans • Carry out forecasting and budgeting for the financial year • Calculate the business unit's cash flow requirements • Determine the business unit's financing needs for the financial year • Compare budget data with estimations to highlight discrepancies • Report budget calculations and discrepancies to organisation management to facilitate decisions on budget allocation • Ensure adherence to financial controls in accordance with relevant organisational corporate governance and financial policies, legislation and regulations	• Recommend parameters and assumptions for budget forecasting in accordance with organisational needs and market conditions • Prepare financial forecasts to facilitate financial and business planning • Implement budget plans to manage resource allocation to business activities • Manage actual budget to enable financial operation n to be measured against forecasted business plans • Monitor budget outcomes to ensure proper utilisation and accounting of resources against their intended purposes • Present financial forecasts, budgets and budget outcomes to immediate supervisors for review and approval	• Determine short- and long-term financial needs to assess current financial situations • Formulate financial plans aligned to overall organisational strategies • Allocate budget resources in accordance with organisational financial plans • Review financial forecasts to anticipate changes in business and operational circumstances • Review draft budgets in accordance with organisational guidelines • Monitor and evaluate actual expense figures against budget to identify and address variances • Report findings, recommendations and options to organisation management for review in accordance with organisational policies	• Set direction for organisational budget planning in consultation with stakeholders • Align budget plans with organisation's strategic plans • Review organisational financial and treasury management policies, systems, budgets and plans • Evaluate effectiveness in increasing business value • Evaluate implications of financial and treasury management policies, systems, budgets and plans on the organisation • Advise senior management on refinements to financial and treasury management policies, systems, budgets and plans • Evaluate financial and treasury management policies, systems, budgets and plans for endorsement purposes
Range of Application						

The information contained in this document serves as a guide.
#Extracted from SkillsFuture ICT Framework

TSC Category	Organisational Management and Support					
TSC Title	Business Needs Analysis[#]					
TSC Description	Identify and scope business requirements and priorities through rigorous information gathering and analysis as well as clarification of the solutions, initiatives and programmes to enable effective delivery. This also involves the development of a compelling and defensible business case and the articulation of the potential impact of the solution to the business.					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Document business requirements and identify basic needs as well as potential solutions	Elicit and analyse business requirements from key stakeholders and assess relevant solutions and their potential impact	Investigate existing business processes, evaluate requirements and define the scope for recommended solutions and programmes	Lead comprehensive analysis to understand underlying drivers and present a compelling business case for proposed IT solutions	
Knowledge		• Processes in business requirement documentation • Typical business processes and functional requirements • Existing or standard IT solutions and initiatives	• Business requirements from key stakeholders • Relevant solutions or programmes • Types of business solutions	• End-to-end requirement elicitation process • Business process and priorities analysis • IT programme / solution scoping techniques • Evaluation techniques or processes for IT solutions and initiatives • Business case elements	• Best practice methodologies in business requirement gathering • Strategic planning and prioritisation for IT business requirements • Business modelling techniques and tools • Projection of long term implications of IT solutions or changes • Business case development	
Abilities		• Document requirements from operational management or other stakeholders • Identify basic and immediate business needs and requirements • Conduct exploratory research or information scanning to consolidate relevant information, options or ideas that can be used • Support in the shortlisting or development of options	• Elicit business requirements from operational management or other stakeholders using appropriate techniques • Review documentation to verify accuracy and understanding of business needs • Analyse data gathered to identify the business problems, requirements and opportunities presented • Assist in analysis of stakeholder objectives	• Lead business requirements elicitation effort, conversations and interactive processes with internal or external stakeholders • Analyse existing business processes and information gathered to understand short-mid term business requirements of varying complexity • Define scope and business priorities for small-medium sized	• Design requirement elicitation process, defining analysis and inputs required • Lead complex and comprehensive analysis of business processes and inputs gathered to understand long-term business requirements and their driving factors • Facilitate scoping and business priority setting for strategic and complex IT initiatives with senior stakeholders	

		or solutions for consideration	and their underlying drivers • Explore relevant solutions or programmes, from an existing repertoire, that can address business needs • Present solution options for consideration • Explain how solutions will impact the business and address requirements	initiatives and programmes • Analyse requirements for alignment with business objectives and priorities • Obtain formal agreement by stakeholders or recipients to the scope and establish baseline for commencement of solution delivery • Evaluate potential options and recommend effective solutions and programmes that can be combined or customised to address root of business needs • Present business case for recommended solutions, defining potential benefits, options, associated risks and impact	• Obtain formal agreement from stakeholders and recipients to the scope, prioritised requirements and establishment of a baseline for solution delivery • Manage effective business processes, through changes and enhancements in IT systems, management and processes • Establish the contribution that IT initiatives, programmes and solutions can make to business objectives • Oversee development and implementation of solutions, taking into account the change implications to the organisation and all stakeholders • Utilise in-depth analysis and business models to present a strong, compelling business case for proposed IT changes and solutions • Project long-term costs and benefits, options, risks and impact to senior stakeholders	
Range of Application						

The information contained in this document serves as a guide.
#Extracted from SkillsFuture ICT Framework

TSC Category	Organisational Management and Support					
TSC Title	Emerging Technology Synthesis[#]					
TSC Description	Monitor and integrate emerging technology trends and developments, structured data gathering for the identification of new and emerging technological products, services and techniques. In addition, the performance of cost-benefit analysis and evaluation of their relevance, viability, sustainability and potential value add to the business.					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Conduct research and identify opportunities for new and emerging technology to support the business	Evaluate new and emerging technology and trends against the organisational needs and processes	Establish internal structures and processes to guide the exploration, integration and evaluation of new technologies	Establish an emerging technology strategy and spearhead organisational norms to synthesise and leverage new technologies and trends to propel business growth
Knowledge			• Market scanning and research techniques for emerging technology • Similar or relevant industries • New technologies and IT products and services in the market • Typical business process flows	• Current industry and technology information sources • Industry-accepted hardware and software products • Emerging trends in technological products and services in the IT industry • Cost-benefit analysis and evaluation methods for assessing new technologies • Business process flows and interdependencies	• Key sources of information on new technologies in adjacent, competing or relevant industries • Risk analysis of the new technologies, and implications on legal, ethical or security dimensions of the business • Change management and implementation considerations relating to introduction of new technologies • Business priorities, planning, value chain and key processes • Current and future impact analysis	• Critical elements of an emerging technology blueprint • Short and long-term impact of new and emerging technologies • Trends and developments in adjacent industries • Potential impact and disruptions to process norms in the Infocomm Technology (ICT) industry or field • Strategic partnership and alliance development

Abilities			• Explore relevance of technologies or IT processes in use and under development in other industry sectors • Conduct research on new technologies • Assess potential of emerging technologies to address challenges or enhance processes within the organisation • Identify processes that will be improved by the application of new and emerging technologies and approaches • Put forth recommendations or options of technology models that offer process improvement	• Determine the suitable sources and relevant sectors or industries to explore new technologies in detail • Monitor the market to keep abreast of new technologies that will impact the ICT market • Evaluate emerging technology against the existing business needs and infrastructure in a nimble and iterative manner • Review market research and validate the new technologies against the organisational needs • Provide recommendations with strong rationale for the outcome of the evaluation • Communicate with external partners to obtain and explore emerging technologies	• Lead the identification and evaluation of new and emerging technologies, techniques and models • Decipher impact of new and emerging technologies on business operations • Experiment with the integration of new and emerging technology into the existing business context • Establish internal processes and guidelines to facilitate the research on and evaluation of new technologies • Establish organisational need and selection criteria for new technologies • Articulate the business considerations and parameters relating to the adoption of new technologies • Manage collaborations with external partners to gain access to and explore emerging technologies	• Develop an emerging technology strategy and blueprint • Harness new technologies and trends in moulding business strategy • Decipher the impact of emerging technology on the ICT industry or field • Establish organisational norms of evaluating emerging technologies in a rapid, nimble and iterative manner • Synthesise different emerging technologies and trends into initiatives or products that propel business growth • Establish alliances to facilitate emerging technology exploration across organisations • Build strategic partnerships with organisations and suppliers to optimise access to new and emerging technology • Create thought leadership around emerging technologies and their impact
Range of Application			Contexts in which this skill may be applied includes, but is not limited to: • Overall business operations • New IT products or services • IT operations • Marketing function • Sales function			

The information contained in this document serves as a guide.
#Extracted from SkillsFuture ICT Framework

TSC Category	Organisational Management and Support					
TSC Title	Learning and Development[#]					
TSC Description	Manage employees' learning and development activities to maximise employee' potential and capabilities to contribute to the organisation					
TSC Proficiency Description	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				Support employees to develop their skills and facilitate learning opportunities and coaching junior management employees	Drive employee developmental programmes in alignment to business needs	Mentor successors, support organisational learning and develop and engage employees to develop a strong organisational base
Knowledge				• Legal and ethical considerations relating to identification of individual training requirements • Market trends and developments in relation to business functions which may aid in identifying new and emerging skill requirements • Roles and accountability for identifying appropriate employee skill requirements • Methods of facilitation of individual learning opportunities • Instructional techniques and methods for working with team members to increase performance • Relevant professional or industry codes of practice and standards • Communication techniques and channels relevant for disseminating information regarding	• Legal and ethical considerations relating to the broader development and provision of human resource information and services • Links between human resource and organisational strategies • Communication techniques and channels relevant for disseminating • Facilitation and communication skills for working with stakeholders in the development of human resource activities, services and programmes • Models and methods for evaluating the effectiveness of human resource activities, services and programmes • Legal and ethical considerations relating to consultation and communication with	• Legal and ethical considerations relating to succession planning, and organisational learning and development • Organisational policies and procedures relating to succession planning, and organisational learning and development • Relevant professional or industry codes of practice and standards relating to learning and development • Implications and impact on employees and the organisation arising from succession management processes, learning and development processes, and engagement activities • Relationship between engagement and performance • Concepts and theories of succession planning and employee engagement

				team activities, services and products • Models and methods of training needs analysis • Negotiation techniques for encouraging employees to participate in processes to improve skills • Implications and impact of coaching and mentoring activities on the individuals participating in the process	organisational stakeholders • Relationship between strategies developed at more senior levels and the operational or functional requirements of other areas within an organisation	• Market trends and developments in relation to succession management, employee engagement and learning and development
Abilities				• Review organisational strategies and business plans that impact on the team's competency requirements • Select and use tools to review current skills of employees • Establish employees' learning priorities • Support employees in drafting learning and development plans • Facilitate learning and development opportunities to address skills needs • Provide resources and support for learning and development • Establish clear learning outcomes and timeframes • Review learning outcomes against learning goals	• Identify human resource trends that may impact on organisational performance • Implement identified changes to human resource activities, services and programmes to support the organisation's strategic and business goals • Establish performance indicators and measures for the effectiveness of human resource activities, services and programmes designed to support the organisation's strategic and business goals • Review organisation's strategic and business plans to identify areas impacting on human resource activities, services and programmes • Facilitate involvement of stakeholders to review	• Develop a succession management strategy in consultation with the human resources function and other relevant personnel to facilitate succession planning • Identify critical roles and feeder positions to provide opportunities to groom successors • Work with managers and identified successors to create and implement development and retention plans • Prioritise learning and development programmes to support employees in the development of their professional, technical and managerial competencies • Guide senior managers to demonstrate independence and responsibility for their personal development • Provide engagement strategies to improve

					human resource service effectiveness and clarify future expectations and requirements • Communicate with stakeholders to clarify their needs relating to human resource activities, services and programmes	organisational performance
Range of Application						

The information contained in this document serves as a guide.
#Extracted from SkillsFuture ICT Framework

TSC Category	Organisational Management and Support					
TSC Title	Manpower Planning[#]					
TSC Description	Estimate and fulfil manpower requirements to achieve business goals and targets					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Facilitate recruitment of manpower to meet forecast requirements	Conduct project level manpower forecasts to bridge gaps between manpower demand and supply, and facilitate development of recruitment strategies	Formulate organisational manpower plans to bridge gaps between manpower demand and supply based on current and projected needs of the organisation	
Knowledge			• Elements of organisation-approved job description templates • Organisational and project workflows • Talent needs of the organisation • Job architecture elements	• Factors influencing future manpower demand • Techniques of manpower modelling • Parameters for accurate forecasting • Statistical analysis techniques for reviewing capacity and capability of existing workforce • Methods to identify elasticities of substitution in headcounts and skills • Organisation's human resources capabilities and people strategies	• Organisation's products, policies and processes • Types of links between manpower plans and organisational strategies • Types of workforce trends that impact organisational performance • Legal and ethical considerations affecting manpower policies • Types of Human Resource policies and procedures • Models and methods for evaluating the effectiveness of manpower forecasting and planning	

Abilities			• Determine job roles and positions required • Identify skills needs related to job positions • Develop job descriptions to articulate role and skill requirements • Assist in developing recruitment strategies with Human Resource department • Negotiate with residential contractors (RCs) and common contractors (CCs) on manpower needs	• Review workforce execution plans needed to meet project and/or functional objectives • Adapt mathematical models to conduct statistical analyses of manpower demand • Review productivity metrics of existing residential contractors (RCs) and common contractors (CCs) • Develop manpower forecast based on job roles and positions required	• Gather data to forecast demand of headcount and skills at organisational level • Review internal education and training programmes to verify manpower supply against future demand • Prepare contingency plans to meet the turn of economic and technological change circumstances • Initiate changes to Human Resource activities, services and programmes • Guide key stakeholders with information on how manpower decisions assist in achieving strategic organisational goals	
Range of Application						

The information contained in this document serves as a guide.
#Extracted from SkillsFuture ICT Framework

TSC Category	Organisational Management and Support					
TSC Title	Partnership Management[#]					
TSC Description	Build cooperative partnerships with inter-organisational and external stakeholders and leveraging of relations to meet organisational objectives. This includes coordination and strategising with internal and external stakeholders through close cooperation and exchange of information to solve problems.					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Support the development and coordination of partnerships with external stakeholders and organisations	Propose strategic initiatives with other organisations based on identification of mutual benefits, and analyse their impact	Evaluate and drive inter-organisational initiatives, and negotiate strategic information exchange with key partners	Inspire direction and define key imperatives for inter-organisational partnerships, leading negotiations with senior leaders and on an international scale
Knowledge			• Types of external partnerships • Objectives of external partnerships • Stakeholders involved in external partnerships	• Cost-benefit analysis of external partnerships • Return on Investment (ROI) calculation and assessment for external partnerships and engagements	• Strategic partnership management • Negotiation techniques	• Strategic networking techniques • Inter-organisational strategy and relationship management
Abilities			• Support the identification of potential initiatives, programmes and projects with other organisations • Coordinate partnerships with external stakeholders • Maintain communication channels with inter-organisational stakeholders and partners	• Propose potential strategic initiatives, programmes and projects with other organisations • Identify common issues as well as mutual benefits and potential gains of collaborating with other organisations • Establish communication channels with inter-organisational stakeholders, to coordinate, address needs, queries or concerns, and facilitate consensus-building • Analyse strategic impact or outcomes of external partnerships to determine effectiveness of partnerships	• Manage inter-organisational initiatives, programmes and projects • Evaluate potential organisations and assess the costs and benefits of a shared partnership • Recommend potential organisations with shared or complementary objectives, or which allow for mutual benefits of a shared partnership • Negotiate the strategic exchange of information with key partners or stakeholders • Co-create a robust inter-organisational strategy to effectively address common issues faced	• Inspire direction for inter-organisational partnerships and culture of collaboration • Define key imperatives of partnerships with external organisations and stakeholders for mutual benefits • Leverage broad and deep networks and relations to establish cooperative and strategic partnerships and meet organisational objectives • Lead negotiations for key partnership agreements • Lead communications with top management or senior leaders from other organisations on an international scale

					• Evaluate effectiveness of partnerships and identify room for enhancement	• Define a robust inter-organisational strategy in consultation with partners and organisation representatives
Range of Application						

The information contained in this document serves as a guide.
[#]Extracted from SkillsFuture ICT Framework

TSC Category	Organisational Management					
TSC Title	People and Performance Management[#]					
TSC Description	Establish organisation-wide performance management strategies to facilitate performance management, including identification of key performance indicators and employee performance assessment					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			Implement performance management programmes	Develop performance management programmes	Establish organisation-wide performance management strategies	
Knowledge			• Organisational performance management programmes • Statistical analysis techniques for evaluating current performance management programmes • Key performance indicators (KPIs) used in performance management programmes • Types on competency frameworks in organisation	• Industry codes of practice related to performance management • Best practices in performance management • Market trends pertaining to performance management • Roles and responsibilities of key stakeholders in performance management • Behaviours that influence employees' performance • Statistical analysis techniques for evaluating performance management data	• Organisational strategy and the impact on human resource (HR) strategies • Emerging trends and developments related to performance management • Relationship between performance management programmes and development of business objectives • Stakeholder engagement techniques • Links between performance management and organisational strategy	
Abilities			• Facilitate the identification of KPIs for teams and individuals with managers • Conduct research on the best practices in KPI development • Communicate KPI guidelines to line managers • Implement performance management programmes according	• Review the key performance indicators (KPIs) as identified by line managers • Cascade departmental level KPIs to teams and individuals • Provide guidance on the use of performance management tools and resources available • Engage employees in understanding their	• Cascade organisational level key performance indicators (KPIs) to departments • Engage stakeholders in identifying performance management requirements • Develop performance management strategies aligned to organisational strategies	

			to overall performance management strategies • Communicate performance management programmes to employees using appropriate communication channels • Analyse relationship between performance management and business performance • Evaluate effectiveness of performance management programmes • Refine performance management programmes based on feedback	roles and responsibilities in performance management • Monitor adherence to performance management requirements • Train line managers on the appropriate mindset and behaviours in conducting performance reviews • Develop review systems for obtaining feedback related to performance management systems • Manage grievances related to performance management for junior employees • Review trends on the impact of performance management programmes on businesses • Recommend refinements to performance management programmes based on industry best practices	• Oversee the implementation of the performance management strategies • Facilitate the development of organisational policies that supports the performance management strategies • Manage performance issues for senior leaders • Evaluate the impact of performance management programmes on business performance • Monitor emerging trends that may impact performance management programmes • Endorse refinements to performance management programmes	
Range of Application						

The information contained in this document serves as a guide.
#Extracted from SkillsFuture ICT Framework

TSC Category	Organisational Management and Support					
TSC Title	Stakeholder Management[#]					
TSC Description	Manage stakeholder expectations and needs by aligning those with requirements and objectives of the organisation. This involves planning of actions to effectively communicate with, negotiate with and influence stakeholders.					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		Identify key stakeholder relationships, needs and interests, and coordinate with stakeholders on a day-to-day basis	Serve as the organisation's main contact point for stakeholder communications, clarifying responsibilities among stakholders, and engaging them to align expectations	Develop a stakeholder engagement plan and negotiate with stakeholders to arrive at mutually-beneficial arrangements	Define a strategic stakeholder management roadmap, and lead critical discussions and negotiations, addressing escalated issues or problems encountered	Establish the overall vision for the alignment of organisation's and stakeholders' objectives, co-creating shared goals and strategic initiatives with senior stakeholders.
Knowledge		• Key stakeholder relationships • Basic stakeholder communication techniques	• Stakeholder mapping techniques • Stakeholders' roles and relationships, and their impact on the organisation • Range of communication channels, approaches and techniques • Stakeholder engagement strategies	• Analysis of stakeholder relationships and levels of interest, power and impact • Process of setting and aligning expectations • Negotiation techniques and approaches • Conflict resolution techniques and approaches • Escalation procedures for handling disputes	• Analysis and planning approaches in stakeholder management • Evaluation techniques to prioritise stakeholder relationships • Negotiation styles and skills to gain consensus • Value added from stakeholder relationships	• Key processes and considerations in formulating stakeholder management strategy • Changes and trends in stakeholders' demands and priorities • Senior stakeholder engagement strategies and techniques
Abilities		• Identify key stakeholders and the organisation's relationship with them • Identify stakeholder needs, positions and interests • Coordinate basic activities and processes with stakeholders on a day-to-day basis • Apply knowledge of the organisatisation's position to respond to simple queries from stakeholders	• Conduct stakeholder mapping to identify facets and nature of relationships with and between stakeholders • Manage stakeholders' expectations and needs, based on the organisation's position and resources • Articulate each stakeholder's role and responsibilities • Serve as the organisation's main contact point or representative for communicating with	• Analyse the complexities of stakeholder relationships and determine their level of interest, power and impact on the organisation • Examine stakeholder positions, agendas and priorities which may be explicitly articulated or unspoken • Develop a stakeholder engagement plan to guide communications with different groups of stakeholders	• Prioritise stakeholder relationships based on in-depth analysis and the organisation's strategic objectives and direction • Develop a strategic stakeholder management roadmap, aligned to the organisation's vision • Lead discussions and negotiations to influence key stakeholder decisions • Address escalated issues raised by or encountered with stakeholders	• Establish the overall vision for how the organisation's and stakeholders' objectives can be shared or aligned • Anticipate changes in stakeholders' needs, demands, priorities and expectations • Optimise alignment of stakeholder management strategy with organisational goals • Lead strategic negotiations, discussions and engagement initiatives with key

			stakeholders, addressing queries and providing clarifications • Represent the company's interests when interacting with stakeholders • Engage stakeholders regularly to set and align expectations and activities as well as to exchange feedback	• Set clear parameters and expectations of stakeholders' roles and responsibilities • Negotiate with stakeholders to align interests or goals and arrive at mutually-beneficial arrangements • Investigate problems or issues encountered in stakeholder relationships • Review feedback from stakeholders and affected parties, and recommend improvements to stakeholder management strategy		leaders and senior stakeholders • Represent the organisation to resolve major escalated issues involving critical stakeholders • Deepen relationships with critical senior stakeholders on an ongoing basis • Co-create shared goals, objectives and vision with senior leaders and stakeholders
Range of Application						

The information contained in this document serves as a guide.
#Extracted from SkillsFuture ICT Framework

OPERATIONAL TECHNOLOGY CYBERSECURITY COMPETENCY FRAMEWORK

QUERIES & FEEDBACK

Questions and feedback on this document may be submitted to:

simon_eng@csa.gov.sg

raymond_ung@csa.gov.sg

corrine_peng@csa.gov.sg

Effective Date: 8 October 2021 version 1.1