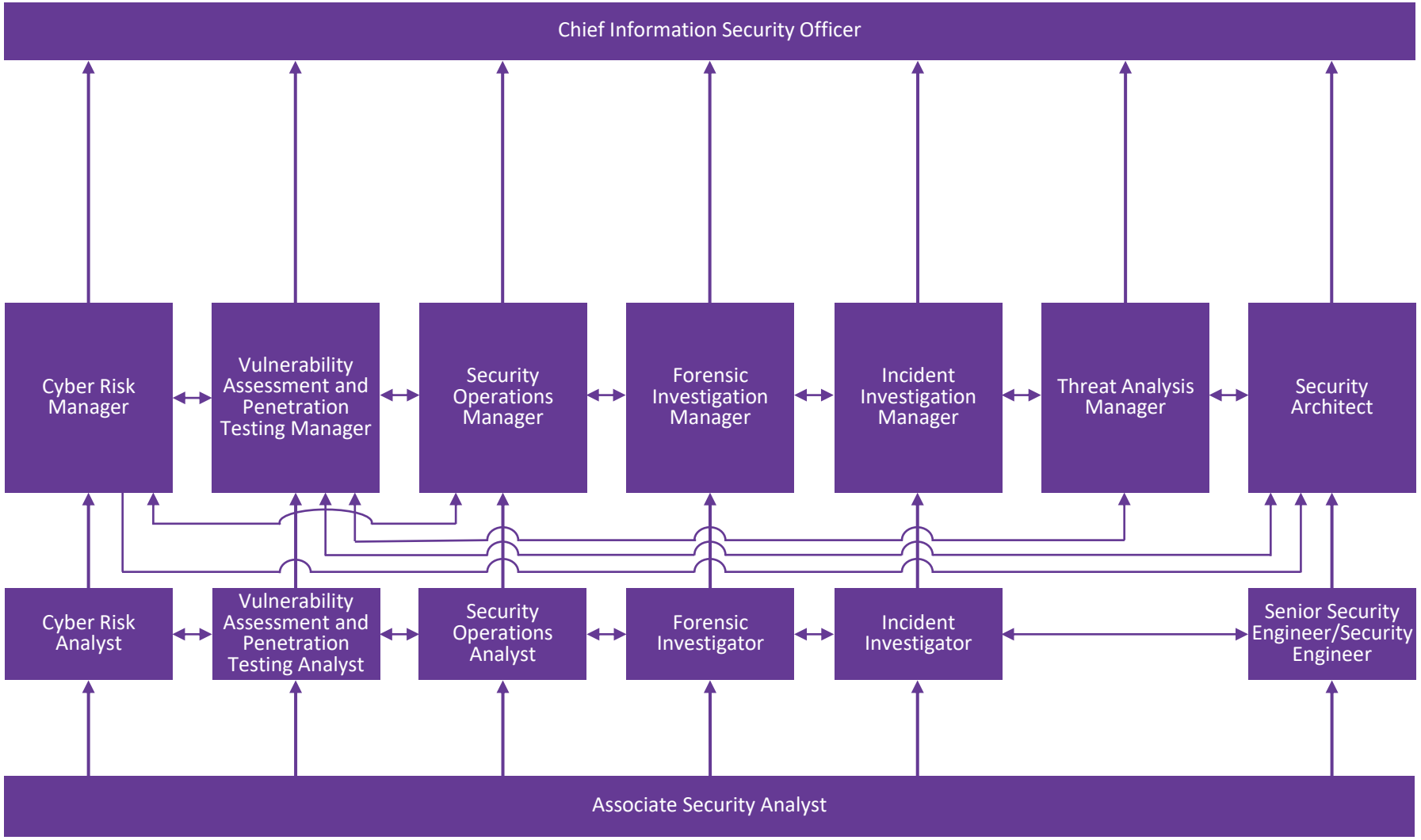
Click on Sub-track names below to view feeder roles and next moves

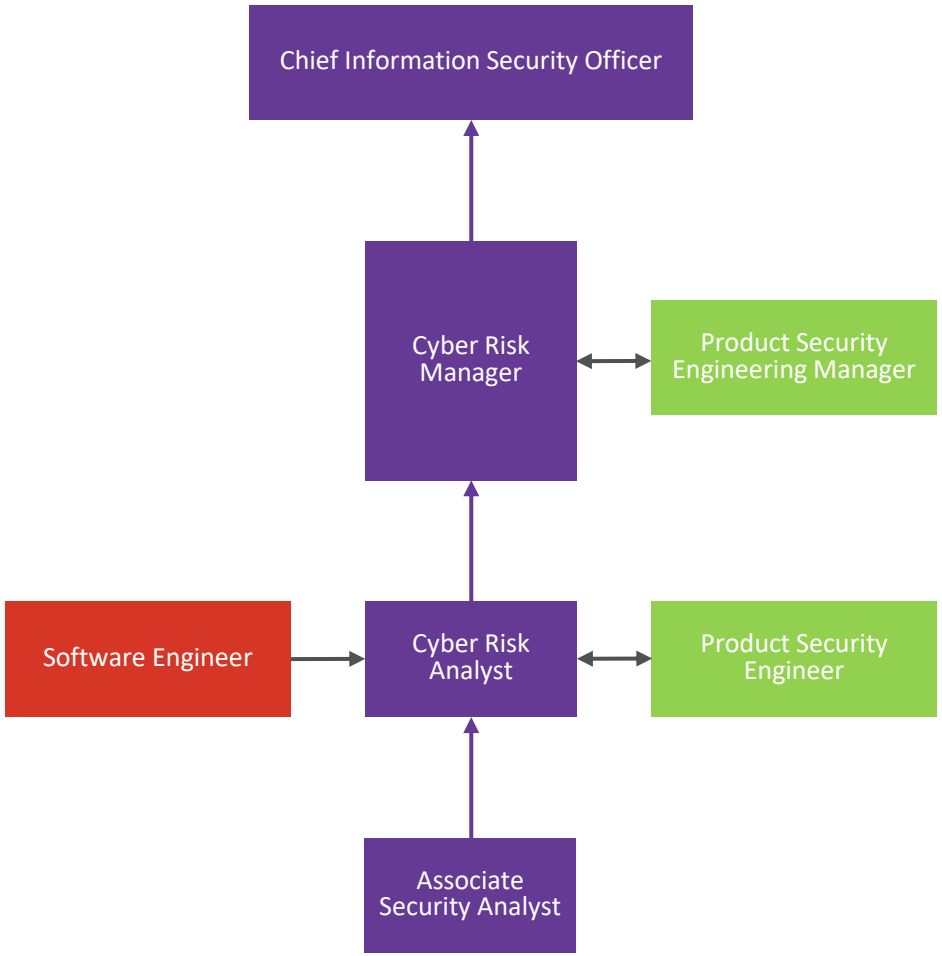
GOVERNANCE RISK AND CONTROL | VULNERABILITY ASSESSMENT AND PENETRATION TESTING | SECURITY OPERATIONS | FORENSICS INVESTIGATION | INCIDENT RESPONSE | THREAT ANALYSIS | SECURITY DESIGN AND ENGINEERING



INFOCOMM MEDIA DEVELOPMENT AUTHORITY
SKILLSFuture SG

Click on Sub-track names below to view feeder roles and next moves

GOVERNANCE RISK AND CONTROL



Lateral Movement | Vertical Progression

BACK TO Career Pathway

ASSOCIATE SECURITY ANALYST

Job Description

The Associate Security Analyst supports security systems, operations administration, monitoring and maintenance of cyber security systems and applications. He/She monitors security alerts and events. He collects and documents information based on established practices and supports the preparation and publishing of security advisories. He assists with the analysis of security-related information and events, escalation of incidents for validation and remediation. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays.

He is familiar with cyber security standards, protocols and frameworks, and is required to act in accordance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security tools and techniques to monitor and resolve incidents.

The Associate Security Analyst is alert and vigilant in performing monitoring activities and is able to analyse and resolve security-related issues critically. He communicates clearly in his interactions with others and coordinates effectively with his team to perform security operations.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Business Needs Analysis	2
Cyber and Data Breach Incident Management	2
Cyber Forensics	2
Infrastructure Support	3
Network Administration and Maintenance	1,2
Problem Management	3
Security Administration	2
Security Assessment and Testing	2
Security Education and Awareness	3
Security Programme Management	3
Stakeholder Management	2
Threat Analysis and Defence	3
Threat Intelligence and Detection	2

Critical Core Skills (Top 5)	Proficiency Level
Communication	Basic
Creative Thinking	Basic
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

ASSOCIATE SECURITY ANALYST

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Monitor cyber security systems	• Perform cyber security monitoring activities on IT systems and applications • Categorise security incidents and breaches that occur • Track and react to security monitoring alerts • Compile reports on the performance of security operations for management reporting	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Maintain cyber security operations	• Assist with the implementation of agreed security system changes and maintenance routines • Assist in the implementation of new cyber security programs • Assist with conducting vulnerability and penetration assessments • Assist in aligning cyber security systems with established service agreement standards • Maintain documentation of all maintenance procedures and tests on cyber security systems	• As above
Respond to cyber security queries	• Assist in responding to cyber security issues • Assist in forensic threat investigations • Assist with resolution of security-related issues • Assist with simulation of user problems to identify drawbacks of cyber security systems • Recommend modifications to cyber security systems to address issues • Maintain logs of cyber security incidents	• As above
Facilitate cyber security compliance	• Assist with the implementation security policies, standards and procedures • Educate users on cyber security policies, standards and practices • Identify improvement areas to existing security policies and procedures • Monitor third party compliance with organisational cyber security policies, standards and procedures • Monitor users' adherence to cyber security policies, standards and procedures	• As above
Optimise cyber security system performance	• Assist with piloting of new cyber security tools, technologies, and processes • Assist with installation of new cyber security related hardware and software • Assist with security system testing and ongoing optimisation or changes such as scheduled upgrades and updates • Maintain documentation of all optimisation activities • Recommend security products, services and/or procedures • Propose improvements to IT operational processes, procedure manuals, and documentation	• As above

BACK TO Career Pathway

CYBER RISK ANALYST

Job Description

The Cyber Risk Analyst conducts cyber risk assessment in support of technology initiatives to help identify IT related risk and determines appropriate controls to mitigate risks. He/She monitors, tracks and manages risk mitigations and exceptions to ensure cyber security standards and policies are established. He applies a defined set of analytical or scientific methods and works independently. He is also responsible for documentation of cyber risk assessment reports.

He is familiar with cyber security standards, protocols and frameworks, and acts in accordance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security monitoring and analysis tools and techniques depending on the organisation's needs and requirements.

The Cyber Risk Analyst is vigilant and systematic in identifying cyber risks and enjoys analysing and investigating such issues. He is a strong team player, and communicates well both verbally and in writing.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	3
Business Needs Analysis	3
Cyber and Data Breach Incident Management	3
Cyber Forensics	3
Cyber Risk Management	4
IT Governance	4
Security Administration	3
Security Education and Awareness	4
Security Governance	4
Security Programme Management	4
Stakeholder Management	3
Strategy Implementation	4
Strategy Planning	4

Critical Core Skills (Top 5)	Proficiency Level
Digital Literacy	Advanced
Computational Thinking	Advanced
Sense Making	Advanced
Transdisciplinary Thinking	Intermediate
Problem Solving	Advanced

CYBER RISK ANALYST

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Establish cyber security standards and policies	• Conduct review of existing security policies, procedures, standards and exceptions • Assist in the development of policies for conducting cyber security risk assessments and compliance audits • Support implementation of information systems and cyber security policies	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Manage cyber risks and assessments	• Perform cyber risk assessment activities based on risk assessment plans • Assess third party security controls and internal security systems • Establish scope of risk analysis for new technology initiatives • Conduct research on emerging cyber security and risk management trends, issues, and alerts • Monitor risks and incidents in accordance with the risk mitigation policies and guidelines	• As above
Develop cyber risk documentation	• Document methodologies and tools to mitigate cyber risks • Prepare reports for cyber risk assessment reporting • Conduct research to develop internal threat awareness reports	• As above
Mitigate cyber security risks	• Determine cause of security violations • Recommend corrective actions or appropriate controls to mitigate technical risks • Assist in the implementation of preventive measures against intrusion, frauds, attacks or leaks • Track remediation efforts for security and audit deficiencies	• As above

BACK TO Career Pathway

CYBER RISK MANAGER

Job Description

The Cyber Risk Manager guides the assessment of information and cyber risks associated with technology initiatives and provides recommendations on control requirements by risk policy and standards. He/She manages and coordinates responses to regulatory inquiries, inspections, audits and ensures cyber security standards and policies are established and implemented. He oversees the development of reports and implements policies and standards. He manages employees and is held accountable for the performance and results of a team. He provides guidance on security measures and protocols to stakeholders.

He is familiar with cyber security standards, protocols and frameworks, and ensures the organisation's compliance to the Cyber Security Act 2018. He is knowledgeable in using various cyber security monitoring and analysis tools and techniques depending on the organisation's needs and requirements. He also has expertise in cyber risk mitigation strategies and protocols.

The Cyber Risk Manager has a sharp, analytical mind and is able to anticipate problems and risks to mitigate them ahead of time. He is an excellent communicator who works well with others and promotes a cooperative working environment and relationships within and beyond his team.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	4
Budgeting	5
Business Needs Analysis	4
Business Performance Management	5
Cyber and Data Breach Incident Management	4
Cyber Forensics	4,5
Cyber Risk Management	5
IT Governance	5
Learning and Development	4,5
Manpower Planning	4
Networking	4
People and Performance Management	4
Security Administration	4
Security Architecture	4
Security Education and Awareness	5
Security Governance	5
Security Programme Management	5
Security Strategy	5
Stakeholder Management	4,5
Strategy Implementation	5
Strategy Planning	5

Critical Core Skills (Top 5)	Proficiency Level
Computational Thinking	Advanced
Digital Literacy	Advanced
Global Mindset	Advanced
Sense Making	Advanced
Creative Thinking	Advanced

CYBER RISK MANAGER

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Implement cyber security risk strategy	• Manage the strategic development and improvement of risk frameworks, methodologies and requirements • Recommend strategies to address key risk areas in cyber security • Assess business needs against cyber security concerns and legal and/or regulatory requirements • Anticipate internal and external business challenges and legal or regulatory issues • Provide strategic risk guidance to stakeholders in the implementation and execution of cyber risk strategies across the organisation	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Establish cyber security standards and policies	• Formulate governance procedures for documenting and updating security policy, standards, guidelines and procedures • Plan the implementation of information systems and cyber security policies • Develop the organisation's Cyber Risk Maturity model • Develop policies and frameworks for conducting cyber security risk assessments and compliance audits	• As above
Manage cyber risks and assessments	• Advise the development of techniques and procedures for the conduct of cyber risk assessments • Develop plans for cyber risk assessment activities across the organisation • Coordinate the on-going cyber risk assessment activities across the organisation • Provide strategic and technical recommendations following identification of vulnerabilities in operating systems • Incorporate emerging security and risk management trends, issues, and alerts into risk assessment framework • Develop cyber risk mitigation strategies and policies for the organisation	• As above
Develop cyber risk documentation	• Oversee the development of documentation on methodologies and tools to mitigate cyber risks • Establish guidelines for reporting outcome of cyber risk assessments • Oversee the development of internal threat awareness reports • Present threat awareness reports to technical and non-technical staff	• As above
Mitigate cyber security risks	• Develop programmes and initiatives to strengthen the capability of the organisation to mitigate risks • Oversee the planning and conduct of organisational cyber security exercises • Act as a subject matter expert in cyber security incident and breach investigations and post-breach remediation work • Propose procedures to prevent future incidents and improve cyber security • Monitor the maintenance of the cyber security operations training plans for all security staff • Manage responses to regulatory inquiries, inspections or audits	• As above
Manage people and organization	• Review operational strategies, policies and targets across teams and projects • Develop strategies for resource planning and utilization • Review the utilisation of resources • Oversee the development of learning roadmaps for teams and functions • Establish performance indicators to benchmark effectiveness of learning and development programmes against best practices • Implement succession planning initiatives for key management positions	• As above

CHIEF INFORMATION SECURITY OFFICER

Job Description

The Chief Information Security Officer develops and drives the vision for the information security function. He/She acts as the authority for the development and enforcement of organisation security strategy, standards and policies, and has ultimate responsibility for ensuring the protection of corporate information. He guides the design and continuous improvement of the IT security architecture and Cyber Risk Maturity Model that balances business needs with security risks. He advises the board and top executives on all security matters and sets directions for complying with regulatory inquiries, legal and compliance regulations, inspections and audits.

He is an expert in cyber security compliance standards, protocols and frameworks, as well as the Cyber Security Act 2018. He is keeps abreast of cyber-related applications and hardware technologies and services, and is constantly on the look-out for new technologies that may be leveraged on to enhance work processes, or which may pose as potential threats.

The Chief Information Security Officer is an inspirational and influential leader, who displays sound judgement and decisiveness in ensuring that corporate information is well protected and secured. He is strategic in his approach toward resource management and capability development among his teams.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	5
Budgeting	6
Business Continuity	6
Business Needs Analysis	5
Business Performance Management	6
Business Risk Management	6
Cyber Forensics	6
Cyber and Data Breach Incident Management	6
Cyber Risk Management	6
Disaster Recovery Management	6
Emerging Technology Synthesis	6
IT Standards	6
Learning and Development	6
Manpower Planning	5
Network Security	5
Networking	5
Partnership Management	6
People and Performance Management	5
Security Architecture	5
Security Governance	6
Security Strategy	6
Stakeholder Management	6
Strategy Planning	6
Threat Analysis and Defence	6
Threat Intelligence and Detection	6

Critical Core Skills (Top 5)	Proficiency Level
Leadership	Advanced
Global Mindset	Advanced
Decision Making	Advanced
Transdisciplinary Thinking	Advanced
Sense Making	Advanced

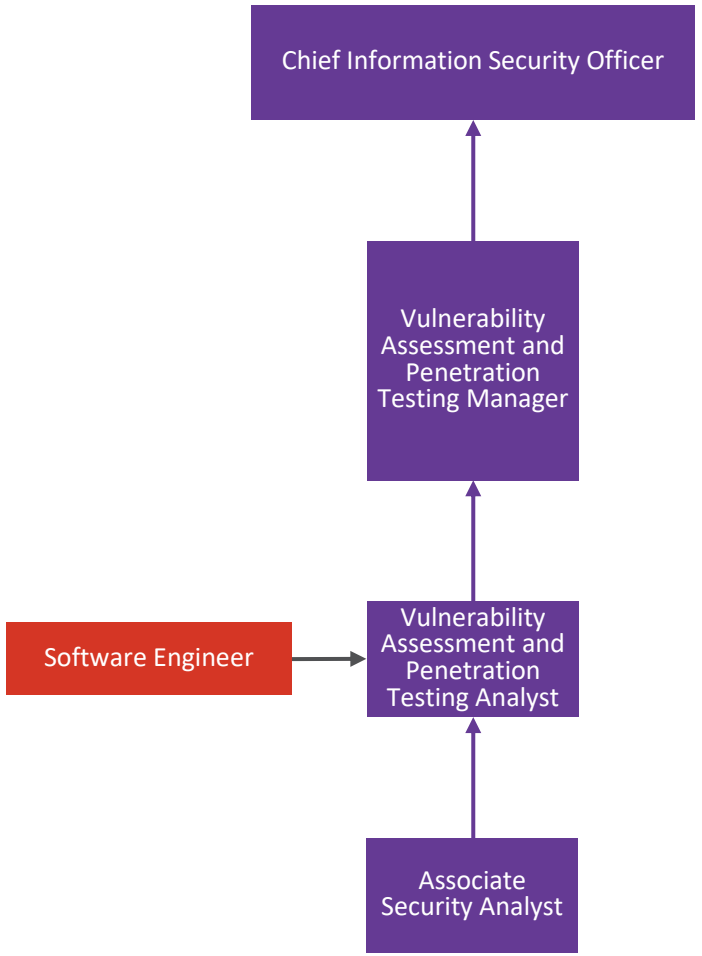
CHIEF INFORMATION SECURITY OFFICER

BACK TO Career Pathway

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

Click on Sub-track names below to view feeder roles and next moves

VULNERABILITY ASSESSMENT AND PENETRATION TESTING



Lateral Movement | Vertical Progression

BACK TO Career Pathway

VULNERABILITY ASSESSMENT AND PENETRATION TESTING ANALYST

Job Description

The Vulnerability Assessment and Penetration Testing Analyst designs and performs tests and check cases to determine if infrastructure components, systems and applications meet confidentiality, integrity, authentication, availability, authorisation and non-repudiation standards. He/She translates requirements into test plan, writes and executes test scripts or codes in line with standards and procedures to determine vulnerability from attacks. He certifies infrastructure components, systems and applications that meet security standards.

The Vulnerability Assessment and Penetration Testing Analyst is well versed with cyber security standards, protocols and frameworks, has a creative and analytical mind, and deploys new and innovative methods to perform penetration tests. He works well in a team and communicates findings and implications effectively to relevant stakeholders.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	3
Cyber Risk Management	4
Emerging Technology Synthesis	4
Learning and Development	4
Network Security	4
Security Assessment and Testing	4
Security Strategy	4
Stakeholder Management	3
Strategy Implementation	3
Strategy Planning	4
Test Planning	4
Threat Analysis and Defence	4

Critical Core Skills (Top 5)	Proficiency Level
Digital Literacy	Advanced
Computational Thinking	Advanced
Sense Making	Advanced
Transdisciplinary Thinking	Intermediate
Problem Solving	Advanced

VULNERABILITY ASSESSMENT AND PENETRATION TESTING ANALYST

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Establish cyber security policies	• Assist in the development of cyber security standards, policies and best practices • Assist in establishing certification based policies for maintaining compliance to cyber security standards • Conduct reviews and assessment of existing security policies, procedures, standards and exceptions	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Oversee vulnerability assessment and penetration testing (VAPT) activities	• Carry out scoping activities to identify systems components which require testing • Define and translate requirements into test plans, scenarios, scripts or procedures • Conduct VAPT, black box and code reviews, and reverse engineering • Perform on-site security assessments of infrastructure components and computer systems • Propose recommendations for continuous improvement of testing processes and methodologies • Identify emerging security and risk management trends, issues, and alerts in VAPT activities	• As above
Manage VAPTs	• Prepare reports on VAPT results based on established guidelines • Provide inputs on security penetration testing in the development of software and applications • Review software designs, source codes and deployment to address cyber security issues • Prepare documentation to facilitate certification of software • Maintain repositories for certification documentation and modifications	• As above

BACK TO Career Pathway

VULNERABILITY ASSESSMENT AND PENETRATION TESTING MANAGER

Job Description

The Vulnerability Assessment and Penetration Testing Manager plans and oversees the delivery of testing and certification services to determine whether infrastructure components, systems and applications meet confidentiality, integrity, authentication, availability, authorisation and non-repudiation standards. He/She reports on testing outcomes and activities. He provides recommendations and manages stakeholder expectations. He ensures compliance with assessment and testing standards, processes and tools. He develops organisational testing capability and supports knowledge management.

He is well versed with cyber security standards, protocols and frameworks, and has sound knowledge of various testing applications and services.

The Vulnerability Assessment and Penetration Testing Manager possesses strong analytical and critical thinking abilities to resolve and advise on highly complex issues, and effectively communicates outcomes to relevant stakeholders. He is adept at managing resources and developing his team.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	4
Budgeting	5
Business Performance Management	5
Cyber Risk Management	5
Emerging Technology Synthesis	5
Learning and Development	5
Manpower Planning	5
Network Security	5
Networking	5
People and Performance Management	5
Security Assessment and Testing	5
Security Education and Awareness	5
Security Governance	5
Security Strategy	5
Stakeholder Management	4
Strategy Implementation	4
Strategy Planning	5
Test Planning	5
Threat Analysis and Defence	5

Critical Core Skills (Top 5)	Proficiency Level
Computational Thinking	Advanced
Digital Literacy	Advanced
Global Mindset	Advanced
Sense Making	Advanced
Creative Thinking	Advanced

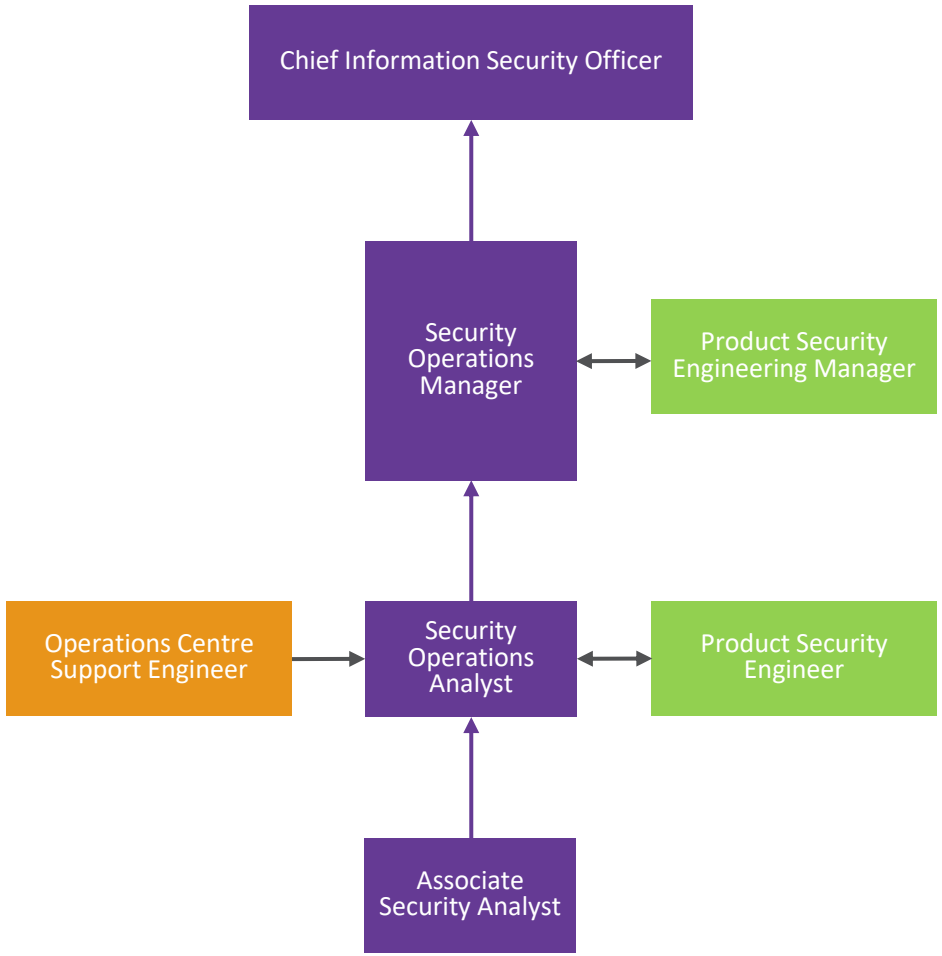
VULNERABILITY ASSESSMENT AND PENETRATION TESTING MANAGER

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Establish cyber security policies	• Develop policies and frameworks to conduct security penetration testing • Establish certification-based policies for maintaining compliance • Formulate governance procedures for documenting and updating security testing policy, standards, guidelines and procedures	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Establish cyber security guidelines and methodologies	• Design service strategies and scope for security testing technologies and solutions • Recommend strategic and operational changes to security testing to address new threats • Drive cyber security awareness within the organisation	• As above
Oversee vulnerability assessment and penetration testing (VAPT) activities	• Establish test metrics to benchmark against requirements and industry best practices • Monitor the conduct of certification tests, audits, inspections and reviews • Provide advice on complex security test data analysis to support security vulnerability assessment processes, including root cause analysis • Act as an escalation point on issues, dependencies, and risks related to security testing • Lead team members to continuously improve testing capabilities • Incorporate emerging security and risk management trends, issues, and alerts in penetration testing activities	• As above
Manage VAPTs	• Develop frameworks and dashboards for the reporting of VAPT results • Communicate the outcome of testing initiatives and results to the stakeholder groups • Recommend strategies and techniques to mitigate identified risks • Provide advice based on security VAPT considerations • Approve documentation to certify penetration testing results • Propose corrections and recommendations to improve and facilitate certification of software	• As above
Manage people and organisation	• Review operational strategies, policies and targets across teams and projects • Develop strategies for resource planning and utilisation • Review the utilisation of resources • Oversee the development of learning roadmaps for teams and functions • Establish performance indicators to benchmark effectiveness of learning and development programs against best practices • Implement succession planning initiatives for key management positions	• As above

Click on Sub-track names below to view feeder roles and next moves

SECURITY OPERATIONS



Lateral Movement | Vertical Progression

BACK TO Career Pathway

SECURITY OPERATIONS ANALYST

Job Description

The Security Operations Analyst performs real-time analysis and trending of security log data from various security devices and systems. He/She maintains data sources feeding the log monitoring system, develops and maintains detection and alerting rules. He responds to user incident reports and evaluates the type and severity of security events. He documents incidents and develops reports. He identifies recurring security issues and risks to develop mitigation plans and recommends process improvements. He interprets and applies security policies and procedures. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays.

He is familiar with cyber security standards, protocols and frameworks, and works in accordance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security monitoring and testing tools and techniques.

The Security Operations Analyst is diligent and takes an analytical approach to perform real-time analyses. He is skilled in synthesising trends and insights, and is confident in putting forth creative mitigation plans and solutions to security incidents.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	3
Business Continuity	4
Cyber and Data Breach Incident Management	3
Cyber Risk Management	4
Disaster Recovery Management	4
Network Security	3
Security Administration	3
Security Programme Management	4
Stakeholder Management	3
Threat Analysis and Defence	4
Threat Intelligence and Detection	3

Critical Core Skills (Top 5)	Proficiency Level
Communication	Intermediate
Creative Thinking	Intermediate
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

SECURITY OPERATIONS ANALYST

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Monitor cyber security systems	• Carries out audits, reviews, security control assessments, and tests of security operations based on established schedules and protocols • Perform real-time analysis and trending of security log data from cyber security systems • Analyse security event data to identify suspicious and malicious activities • Provide inputs to improve security monitoring rules and alerts • Document processes related to cyber security monitoring	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Maintain cyber security operations	• Implement cyber security protocols • Formulate emergency response procedures • Maintain data sources feeding the log monitoring system • Schedule security checks in accordance with reporting schedules • Prepare periodic status reports for presentation to management	• As above
Manage response to cyber security incidents	• Review security incident reports • Analyse the type and severity of cyber security incidents • Assist in establishing procedures for handling detected cyber security incidents • Provide status updates during the lifecycle of a cyber security incident • Prepare final incident report detailing the events of the cyber security incident • Support the maintenance and update of business recovery, contingency plans and procedures	• As above

SECURITY OPERATIONS MANAGER

Job Description

The Security Operations Manager plans and oversees monitoring and maintenance of security operations and provides direction and leadership to internal resources. He/She provides expertise on security technologies and innovative security concepts and works toward enhancing the resilience of security operations. He coordinates ongoing reviews of existing security programs, protocols and planned upgrades. He establishes escalation processes for security incidents and develops contingency plans and disaster recovery procedures. He focuses on policy implementation and control.

He is familiar with cyber security standards, protocols and frameworks, and ensures the organisation's compliance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security monitoring and testing tools and techniques.

The Security Operations Manager is diligent and watchful in monitoring security operations, systems and activities. He is also a confident leader who develops plans and solutions to address security incidents and also one who has a passion for engaging and developing others in his team.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	4
Budgeting	5
Business Continuity	5
Business Performance Management	5
Cyber and Data Breach Incident Management	4
Cyber Risk Management	5
Disaster Recovery Management	5
Emerging Technology Synthesis	5
Learning and Development	4,5
Manpower Planning	4
Network Security	4
Networking	4
People and Performance Management	4
Security Administration	4
Security Education and Awareness	5
Security Strategy	5
Stakeholder Management	4,5
Strategy Implementation	5
Strategy Planning	5
Threat Analysis and Defence	5
Threat Intelligence and Detection	4,5

Critical Core Skills (Top 5)	Proficiency Level
Communication	Advanced
Developing People	Advanced
Problem Solving	Advanced
Resource Management	Advanced
Sense Making	Advanced

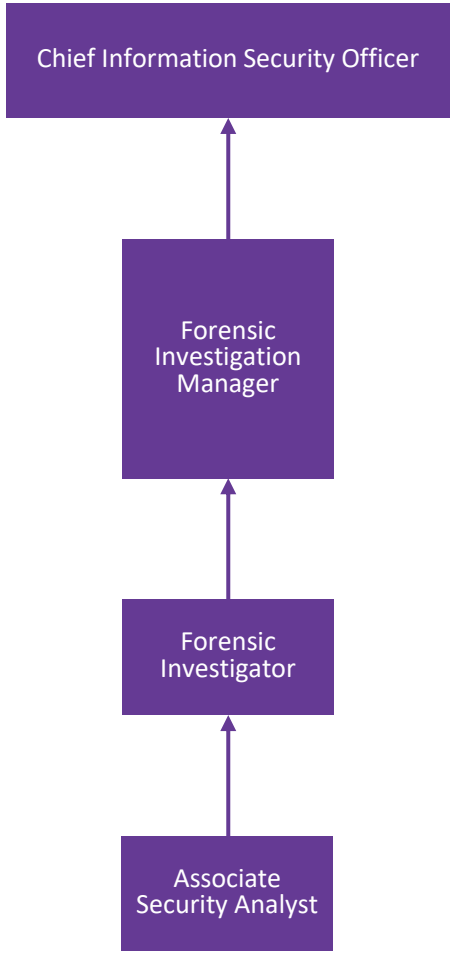
SECURITY OPERATIONS MANAGER

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Implement cyber security strategy	• Develop the organisation's cyber security strategy • Align security operations functions with the organisation's overall business objectives • Advise senior leaders on critical issues that may affect corporate security objectives • Advise the design and implementation of security policy and controls • Provide expertise on security technologies and innovative security concepts • Provide technical and operational oversight for security tool deployment and implementation	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Monitor cyber security systems	• Develop plans for monitoring security systems and responding to cyber security incidents • Oversee the identification and measurement of critical cyber security operations metrics • Develop cyber threat detection and incident alert rules and implement regulations • Monitor levels of service of the cyber security operations • Present periodic cyber security status reports to management	• As above
Maintain cyber security operations	• Oversee planning and coordination of 24 x 7 security operations coverage • Coordinate ongoing reviews of existing security programs, protocols and planned upgrades • Monitor compliance to security policies, regulations, rules and norms • Drive continuous improvement of security operations	• As above
Manage response to cyber security incidents	• Formulate internal guidelines for processing and escalation of cyber security incidents • Review reports on incidents and breaches of cyber security • Oversee prioritisation of alerts and resources for incident responses • Present final incident reports on cyber security incidents to senior management for approval • Recommend systems and procedures for the prevention, detection, containment and correction of cyber security breaches	• As above
Manage people and organisation	• Review operational strategies, policies and targets across teams and projects • Develop strategies for resource planning and utilisation • Review the utilisation of resources • Oversee the development of learning roadmaps for teams and functions • Establish performance indicators to benchmark effectiveness of learning and development programs against best practices • Implement succession planning initiatives for key management positions	• As above

Click on Sub-track names below to view feeder roles and next moves

FORENSICS INVESTIGATION



Lateral Movement | Vertical Progression

BACK TO Career Pathway

FORENSICS INVESTIGATOR

Job Description

The Forensics Investigator is responsible for the investigation processes after a cyber-threat or incident. He/She is responsible to collect and analyse the threat data from the affected systems. He is also responsible for performing the forensics investigation and determining the root cause of cyber-attacks.

He is familiar with different types of threats, cyber security standards, protocols and frameworks, and acts in accordance with the Cyber Security Act 2018. He is knowledgeable of hardware and software applications to analyse threat data from various sources.

The Forensics Investigator is diligent and takes an analytical approach to perform analyses and uncover insights. He is skilled in synthesising trends and insights, and is confident in putting forth creative mitigation plans and solutions to mitigate security incidents.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Cyber Forensics	3
Cyber Risk Management	4
Emerging Technology Synthesis	3
Failure Analysis	3
Network Security	3
Security Administration	3
Security Assessment and Testing	3
Stakeholder Management	3
Threat Analysis and Defence	3
Threat Intelligence and Detection	3

Critical Core Skills (Top 5)	Proficiency Level
Communication	Intermediate
Creative Thinking	Intermediate
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

FORENSICS INVESTIGATOR

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Collate threat data post-cyber attack	• Collect information from affected stakeholders and document the impact of the cyber-attack • Scan IT systems to retrieve information from storage and other electronic devices • Collect and decrypt threat data from affected IT systems • Perform cross analysis of threat data with existing threat database to classify the threat data	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Oversee forensic investigations	• Conduct forensic analysis and investigations to determine the causes of security incidents • Distil key insights and impact from analyses of security incidents • Contain the impact of security incidents • Prepare investigative reports detailing incident findings, analysis and conclusions • Update threat database based on investigation findings • Provide insights and recommendations to affected stakeholders on post investigation findings and cyber-attack mitigation strategies	• As above

BACK TO Career Pathway

FORENSICS INVESTIGATION MANAGER

Job Description

The Forensics Investigation Manager plans and oversees the investigation processes and protocols after a cyber-threat or incident. He/She is responsible to ensure that the data is collected and analysed properly. He is also responsible for developing a forensics investigation strategy and overseeing the forensics investigations to ensure the threat is classified and future actions are recommended to the affected stakeholders.

He is familiar with different types of threats, cyber security standards, protocols and frameworks, and ensures the organisation's compliance with the Cyber Security Act 2018. He is knowledgeable of hardware and software applications to analyse threat data from various sources.

The Forensics Investigation Manager is diligent and watchful in the investigation activities. He is also a confident leader who develops plans and solutions to address security incidents, and has a passion for engaging and developing others in his team.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Budgeting	5
Business Performance Management	5
Cyber Forensics	4,5
Cyber Risk Management	5
Emerging Technology Synthesis	4
Failure Analysis	4
Learning and Development	4,5
Manpower Planning	4
Network Security	4
Networking	4
People and Performance Management	4
Security Administration	4
Security Assessment and Testing	5
Security Governance	5
Security Strategy	5
Stakeholder Management	4,5
Strategy Implementation	5
Strategy Planning	5
Threat Analysis and Defence	4
Threat Intelligence and Detection	4

Critical Core Skills (Top 5)	Proficiency Level
Communication	Advanced
Developing People	Advanced
Problem Solving	Advanced
Resource Management	Advanced
Sense Making	Advanced

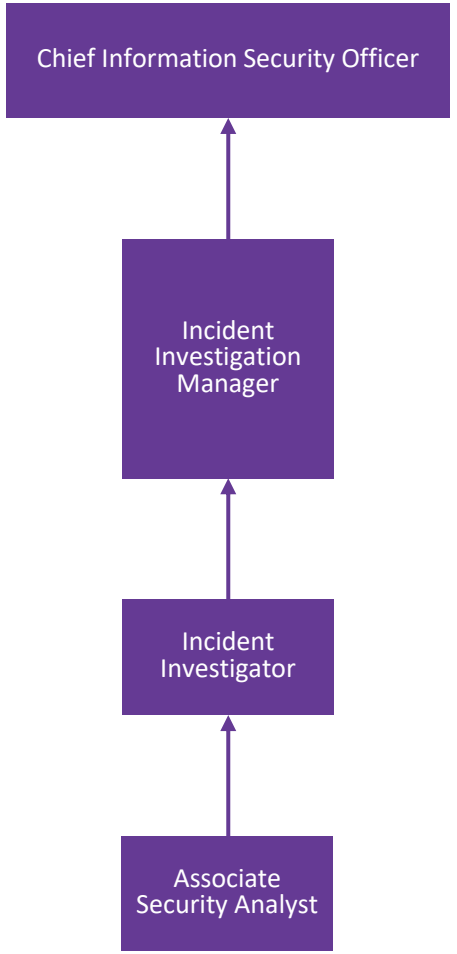
FORENSICS INVESTIGATION MANAGER

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Develop a forensics investigation strategy	• Develop strategy to collect and analyse threat data after an incident • Establish digital forensic investigation policies and standards for the organisation • Develop threat mitigation processes and policies after analysing the root cause of the incident, refreshing them when required • Advise senior management on major information security-related risks and forensics investigations policies and procedures	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Oversee forensic investigations	• Lead forensic investigations and coordinate forensic teams post cyber-attacks to determine the root cause of the incident • Scrutinise forensic incident trends to ensure correct measures are taken during the investigation process • Determine the tactics, techniques and procedures used for cyber attacks • Manage the evidence and causal analysis of cyber threats, incidents and attacks • Present reports and outcomes in investigations or legal proceedings to senior management and key stakeholders	• As above
Manage people and organisation	• Review operational strategies, policies and targets across teams and projects • Develop strategies for resource planning and utilisation • Review the utilisation of resources • Oversee the development of learning roadmaps for teams and functions • Establish performance indicators to benchmark effectiveness of learning and development programs against best practices • Implement succession planning initiatives for key management positions	• As above

Click on Sub-track names below to view feeder roles and next moves

INCIDENT RESPONSE



Lateral Movement | Vertical Progression

BACK TO Career Pathway

INCIDENT INVESTIGATOR

Job Description

The Incident Investigator conducts complex analysis to investigate causes of intrusion, attack, loss or breach occurring in an organisation. He/She identifies and defines cyber threats and root causes. He develops reports that detail incident timeline, evidence, findings, conclusions and recommendations. He is responsible for managing cyber incidents and resolving the incidents in a timely manner. He prepares reports, communicates findings to senior stakeholders, and recommends corrective actions to prevent and mitigate internal control failures. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays.

He is familiar with cyber security standards, protocols and frameworks, and works in compliance with the Cyber Security Act 2018. He is knowledgeable in using various cyber security tools and techniques to resolve incidents.

The Incident Investigator is detail-oriented and adopts a critical and systematic approach in conducting investigations and analyses. He views issues from multiple perspectives and actively communicates his thoughts and engages with other team members.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Cyber Forensics	3
Cyber and Data Breach Incident Management	3
Cyber Risk Management	4
Security Assessment and Testing	3
Stakeholder Management	3
Threat Analysis and Defence	3
Threat Intelligence and Detection	3

Critical Core Skills (Top 5)	Proficiency Level
Communication	Intermediate
Creative Thinking	Intermediate
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

INCIDENT INVESTIGATOR

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Develop and implement cyber incident response strategy	• Develop approaches to combat cyber threats and mitigate risks to information systems assets • Develop guidelines to perform incident response strategies and policies • Implement processes and guidelines to perform incident response protocols, analyse data, and create incident reports • Implement mechanisms to improve cyber security measures and incident response times	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Manage cyber security incidents	• Handle responses to cyber security incidents • Lead the recovery of contained cyber security incidents, following established processes and policies • Utilise appropriate cyber incident management techniques to resolve challenges	• As above
Oversee cyber threat analysis	• Collect, analyse and store cyber threat intelligence information • Analyse past cyber-attacks to draw insights and implications on the organisation • Scrutinise vulnerabilities within systems that may pose cyber security risks • Recommend ways to enhance the resilience and security of IT systems • Propose mitigation techniques and countermeasures to ensure cyber threats are kept at a minimum	• As above

BACK TO Career Pathway

INCIDENT INVESTIGATION MANAGER

Job Description

The Incident Investigation Manager plans and oversees the performance of security response during the event of a cyber-incident or threat. He proposes mitigation techniques and countermeasures as well as develops cyber security solutions to prevent future attacks. He develops and implements cyber incident response strategies. He presents cyber-incident reports to senior leaders. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays.

He is familiar with cyber security standards, protocols and frameworks, and ensures the organisation's compliance to the Cyber Security Act 2018. He is knowledgeable in using various cyber security analysis tools and techniques to resolve incidents.

The Incident Investigation Manager is diligent and watchful in monitoring security operations, systems and activities. He is quick to provide solutions and fix issues when they arise. He is adept at dealing with complexity, and is an articulate and developmental leader in his team.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Budgeting	5
Business Performance Management	5
Cyber and Data Breach Incident Management	4
Cyber Forensics	4,5
Cyber Risk Management	5
Learning and Development	4,5
Manpower Planning	4
Networking	4
People and Performance Management	4
Security Assessment and Testing	4
Security Governance	5
Security Strategy	5
Stakeholder Management	4,5
Strategy Implementation	5
Strategy Planning	5
Threat Analysis and Defence	4
Threat Intelligence and Detection	4

Critical Core Skills (Top 5)	Proficiency Level
Communication	Advanced
Developing People	Advanced
Problem Solving	Advanced
Resource Management	Advanced
Sense Making	Advanced

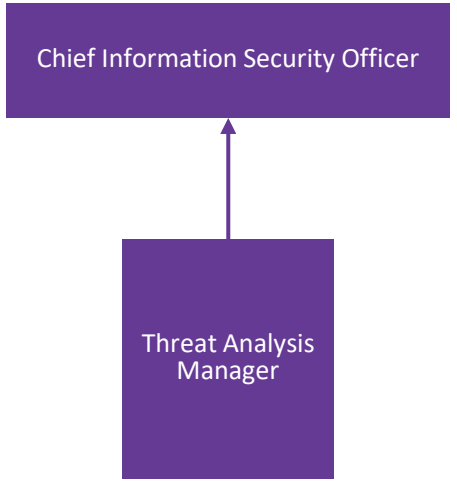
INCIDENT INVESTIGATION MANAGER

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Develop and implement cyber incident response strategy	• Develop contingency and disaster recovery plans tailored specifically for every security incident • Establish incident response policies and standards for the organisation • Develop incident response processes and policies, refreshing them where required • Advise senior management on major information security-related risks and cyber incident response strategies	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Oversee cyber threat analysis	• Oversee the identification of security risks and exposures to internal systems • Optimise cyber security data analytics models to pre-empt and detect suspicious activities • Provide risk analysis and security design advice to internal software and system design teams • Oversee the sharing of cyber threat intelligence with security partners, vendors and law enforcement • Oversee the development of cyber security solutions to prevent future cyber incidents	• As above
Manage people and organisation	• Review operational strategies, policies and targets across teams and projects • Develop strategies for resource planning and utilisation • Review the utilisation of resources • Oversee the development of learning roadmaps for teams and functions • Establish performance indicators to benchmark effectiveness of learning and development programs against best practices • Implement succession planning initiatives for key management positions	• As above

Click on Sub-track names below to view feeder roles and next moves

THREAT ANALYSIS



Lateral Movement | Vertical Progression

BACK TO Career Pathway

THREAT ANALYSIS MANAGER

Job Description

The Threat Analysis Manager plans out strategies to pre-empt potential threats in an organisation's cyber related systems. He/She is responsible for identifying the IT assets that are prone to cyber threats and attacks. He proactively monitors the open web and identifies potential threats and groups or individuals capable of attempting cyber-attacks. He runs tests and analyses different areas of the IT assets to ensure they are safe from cyber-attacks.

He is familiar with cyber security standards, protocols and frameworks. He is knowledgeable in using various cyber security analysis tools and techniques to monitor and identify potential incidents.

The Threat Analysis Manager is alert and vigilant in performing monitoring activities, and is able to analyse and identify potential security-related issues, which may have critical impact on security and operational systems. He communicates clearly in his interactions with others and coordinates effectively with his team to perform security operations.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Audit and Compliance	4
Budgeting	5
Business Performance Management	4,5
Cyber and Data Breach Incident Management	5
Cyber Risk Management	5
Emerging Technology Synthesis	5
IT Standards	5
Learning and Development	5
Manpower Planning	4,5
Network Security	4
Networking	4
People and Performance Management	4
Security Architecture	4
Security Assessment and Testing	5
Security Programme Management	5
Security Strategy	5
Stakeholder Management	5
Strategy Implementation	4
Strategy Planning	5
Threat Analysis and Defence	5
Threat Intelligence and Detection	5

Critical Core Skills (Top 5)	Proficiency Level
Virtual Collaboration	Intermediate
Transdisciplinary Thinking	Advanced
Problem Solving	Advanced
Leadership	Advanced
Global Mindset	Advanced

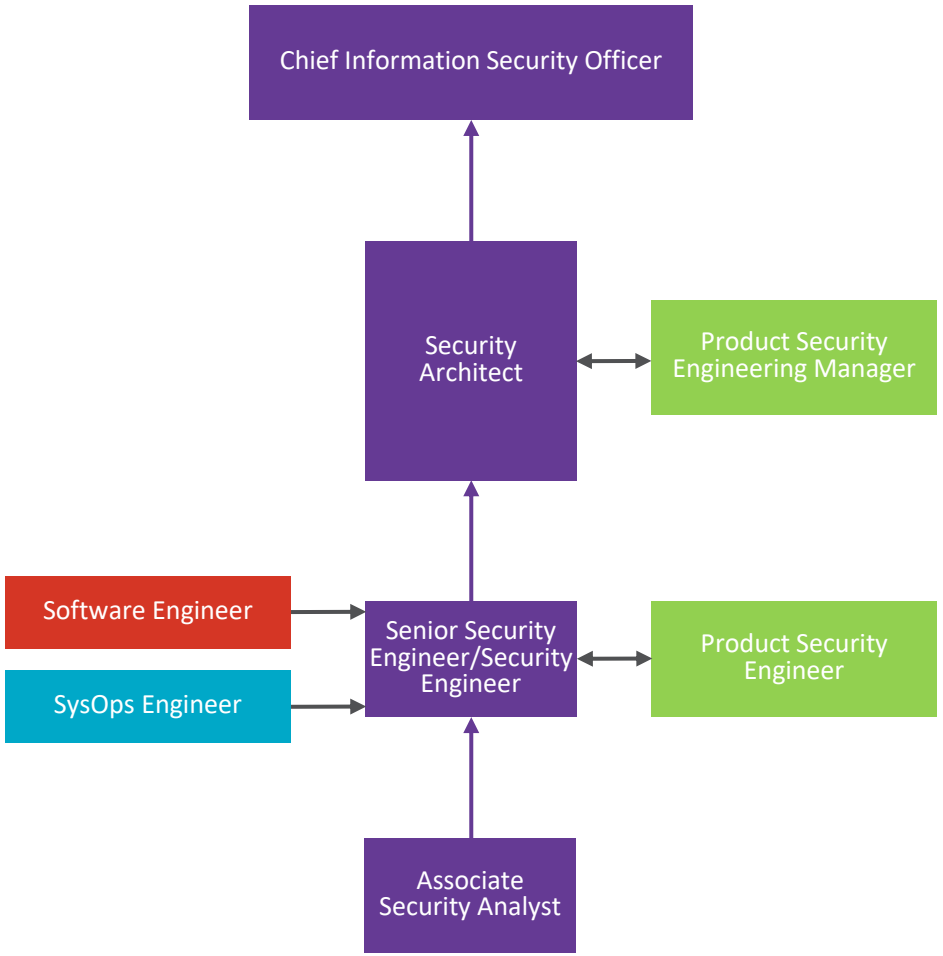
THREAT ANALYSIS MANAGER

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Assess organisational assets for potential cyber threats	• Develop and implement strategies to identify assets prone to cyber threats and attacks • Deconstruct the architecture of the application to uncover potential threats and vulnerabilities in the design, implementation, deployment or configuration of the application and systems • Conduct in-depth analysis of existing threats and identify existing gaps in the current cyber security set-up • Provide advice on the design and implementation of security policy and controls on identified assets • Evaluate and provide feedback to improve intelligence production, intelligence reporting, collection requirements, and operations	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Research and pro-active monitoring of threats and attacks	• Run continuous scans and monitor threats that may exist in the dark web and external web-based applications • Conduct research on new and existing threats that may impact existing IT systems • Identify potential attacker groups or individuals and take preventive measures • Recommend and develop approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists • Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives related to designated cyber operations warning problem sets	• As above
Classifying threats and simulating attacks on systems and applications	• Identify potential threats that may affect applications and systems using the knowledge of the application and system vulnerabilities • Run test attacks and simulations on the systems to identify the possibilities of threats and extent of damage it could cause • Prioritise and rate identified threats based on its severity • Provide timely notice of imminent or hostile intentions or activities which may impact organisation objectives, resources, or capabilities • Use existing database of threats and attack histories to pre-empt and classify potential new threats	• As above
Implement and document threat mitigation strategies and protocols	• Document new threats based on a core set of attributes to develop threat mitigation protocols • Provide guidance on threat mitigation strategies and potential threats and cyber-attacks to ensure current cyber security standards and set-up are updated • Analyse intelligence and support designated exercises, planning activities, and time sensitive operations • Provide evaluation and feedback to improve intelligence production, reporting, collection requirements, and operations.	• As above
Manage people and organisation	• Manage the budget expenditure and allocation across teams and projects • Monitor and track the achievement of the team's achievements and key performance indicators • Propose new operational plans, including targeted budgets, work allocations and staff forecasts • Acquire, allocate and optimise the use of and allocation of resources • Develop learning roadmaps to support the professional development of the team • Manage the performance and development process, including providing coaching and development opportunities to maximise the potential of each individual	• As above

Click on Sub-track names below to view feeder roles and next moves

SECURITY DESIGN AND ENGINEERING



Lateral Movement | Vertical Progression

BACK TO Career Pathway

SENIOR SECURITY ENGINEER/ SECURITY ENGINEER

Job Description

The Senior Security Engineer/Security Engineer designs, develops and implements secure system architectures. He/She embeds security principles into the design of system architectures to mitigate the risks posed by new technologies and business practices. He designs artefacts, spanning design, development and implementation, into enterprise systems that describe security principles and how they relate to the overall enterprise system architecture. He performs routine activities related to the periodic review and audit activities of infrastructure security systems and maintains documentation of security standards and procedures.

He is well versed with cyber security standards, protocols and frameworks, and works in compliance with the Cyber Security Act 2018. He is knowledgeable of various application and hardware technologies and services.

The Senior Security Engineer/Security Engineer is structured and systematic in his approach to designing and implementing secure system architectures. He is articulate and works well with his team and other stakeholders.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Business Needs Analysis	3
Cyber and Data Breach Incident Management	3
Cyber Risk Management	4
Emerging Technology Synthesis	3
Infrastructure Design	3
Network Security	4
Security Administration	3
Security Architecture	3
Security Governance	4
Security Programme Management	3
Strategy Implementation	4
Strategy Planning	4

Critical Core Skills (Top 5)	Proficiency Level
Communication	Intermediate
Computational Thinking	Intermediate
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

SENIOR SECURITY ENGINEER/SECURITY ENGINEER

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Develop architecture requirements and maintain oversight	• Design security controls and systems in alignment with security guidelines • Assist in the testing and evaluation of new security technologies and controls • Recommend security products, services and procedures to enhance system architecture designs • Document the design, operation, use, and expected outputs of new systems • Conduct research on modern security software architectures and network architecture design best practices	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Implement security systems	• Implement new enterprise security architecture, technologies and enhancements • Identify techniques to scale up and automate security infrastructure and processes • Resolve issues that arise in implementation of new security systems • Monitor security systems for strengths and weaknesses and propose improvements to address weaknesses	• As above
Manage security systems	• Oversee the maintenance of security systems, platforms and associated software • Develop and implement custom disaster recovery drills and simulation tests on existing systems • Assist in the resolution of identified problems and incidents	• As above

BACK TO Career Pathway

SECURITY ARCHITECT

Job Description

The Security Architect leads unique and highly complex projects involving design, development and implementation of secure system architectures. He/She plans and monitors the design of artefacts into enterprise systems that describe security principles and how they relate to the overall enterprise system architecture. He is involved in the development and application of new solutions in infrastructure security. He recommends and leads the adoption of new technological advances and best practices in infrastructure security systems to mitigate security risks. He identifies and resolves unique and complex issues, which may have organisation-wide and long-term impact.

He is an expert in cyber security standards, protocols and frameworks, and ensures the organisation's compliance to the Cyber Security Act 2018. He is knowledgeable of various application and hardware technologies and services.

The Security Architect has a creative and critical mind, and enjoys identifying linkages and interconnections among various parts of a system or architecture. He is a technical expert who should also be people-oriented, consultative, developmental and actively engaging stakeholders to design optimal secure system architectures. He also mentors and provides technical leadership to the junior staff.

Critical Work Functions and Key Tasks View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Business Needs Analysis	4
Cyber Risk Management	5
Emerging Technology Synthesis	4
Infrastructure Design	4
Network Security	5
Security Administration	4
Security Architecture	4,5
Solution Architecture	5
Security Governance	5
Security Programme Management	4,5
Security Strategy	5
Stakeholder Management	5
Strategy Implementation	5
Strategy Planning	5

Critical Core Skills (Top 5)	Proficiency Level
Communication	Advanced
Creative Thinking	Advanced
Developing People	Advanced
Problem Solving	Advanced
Sense Making	Advanced

SECURITY ARCHITECT

BACK TO Career Pathway

Critical Work Functions	Key Tasks	Performance Expectations
Formulate the organisation's security architecture strategy, governance, roadmap, standards, policies and procedures	• Lead and coordinate the domain technical and business discussions • Participate in ecosystem strategy development, environment analysis and opportunity identification • Analyse, design and develop roadmaps and implementation plans based on a current versus future state • Design standard configurations and patterns • Lead and facilitate the business architecture governance process based on the enterprise architecture governance structure • Manage exceptions to architectural standards at a security level • Review and approve recommendations to security architectural standards	In accordance with: • Cyber Security Act 2018, Cyber Security Agency of Singapore
Develop architecture requirements and maintain oversight	• Analyse and develop security architectural requirements • Align architectural requirements with IT strategy • Assess near-term needs to establish business priorities • Ensure compatibility with existing solutions, infrastructure, services and strategic requirements • Coordinate architecture implementation and modification activities • Assist in post-implementation and continuous improvement efforts to enhance performance and provide increased functionality • Ensure conceptual completeness of the technical solution	• As above
Manage quality and continuous improvement of architecture	• Analyse the current architecture to identify weaknesses and develop opportunities for improvement • Identify and propose variances to the architecture to accommodate project needs • Perform ongoing architecture quality review activities	• As above
Research emerging technologies	• Consult with clients and IT teams on security architecture solutions • Analyse cost versus benefits, risks, impact and technology priorities • Provide recommendations on emerging technology to senior management • Develop a communication plan for security architecture • Lead the research and evaluation of emerging technology, industry and market trends to assist in project development • Identify organisational requirements for resources	• As above
Translate security architecture into security solutions	• Oversee the development and maintenance of the organisation's security strategy • Oversee the translation of the security architecture to solutions • Ensure adequate security solutions are in place throughout all IT systems and platforms • Define the alignment of security governance with enterprise architecture governance • Act as a security expert in application development, database design and network efforts • Ensure compliance with enterprise and IT security policies and industry regulations • Contribute to the alignment of security governance with enterprise architecture governance • Evaluate secure solutions based on approved security architectures • Explores new security technologies and architectures	• As above