|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – SECURITY OPERATIONS MANAGER** | | | | | |
| **Sector** | Infocomm Technology | | | | |
| **Track** | Cyber Security | | | | |
| **Sub-track** | Security Operations | | | | |
| **Occupation** | ICT Security Specialist | | | | |
| **Job Role** | **Security Operations Manager** | | | | |
| **Job Role 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, Key Tasks and Performance Expectations** | **Critical Work Functions** | **Key Tasks** | | | **Performance Expectations** |
| **Implement cyber security strategy** | Develop the organisation’s cyber security strategy | | | In accordance with:     * Cyber Security Act 2018, Cyber Security Agency of Singapore |
| 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 | | |
| **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 | | |
| **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 | | |
| **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 | | |
| **Manage people and organisation** | Review operational strategies, policies and targets across teams and projects | | |
| Develop strategies for resource planning and utilisation | | |
| Review the utilisation of resources | | |
| Oversee the development of learning roadmaps for teams and functions | | |
| Establish performance indicators to benchmark effectiveness of learning and development programmes against best practices | | |
| Implement succession planning initiatives for key management positions | | |
| **Skills and Competencies** | **Technical Skills and Competencies** | | | **Generic Skills and Competencies** | |
| Audit and Compliance | | Level 4 | Communication | Advanced |
| Budgeting | | Level 5 | Developing People | Advanced |
| Business Continuity | | Level 5 | Problem Solving | Advanced |
| Business Performance Management | | Level 5 | Resource Management | Advanced |
| Cyber and Data Breach Incident Management | | Level 4 | Sense Making | Advanced |
| Cyber Risk Management | | Level 5 |  | |
| Disaster Recovery Management | | Level 5 |
| Emerging Technology Synthesis | | Level 5 |
| Learning and Development | | Level 4, Level 5 |
| Manpower Planning | | Level 4 |
| Network Security | | Level 4 |
| Networking | | Level 4 |
| People and Performance Management | | Level 4 |
| Security Administration | | Level 4 |
| Security Education and Awareness | | Level 5 |
| Security Strategy | | Level 5 |
| Stakeholder Management | | Level 4, Level 5 |
| Strategy Implementation | | Level 4 |
| Strategy Planning | | Level 5 |
| Threat Analysis and Defence | | Level 5 |
| Threat Intelligence and Detection | | Level 4, Level 5 |
| **Programme Listing** | For a list of Training Programmes available for the ICT sector, please visit: www.skillsfuture.sg/skills-framework/ict | | | | |
|  |  | |  |  |  |
| The information contained in this document serves as a guide. | | | | | |