|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SKILLS FRAMEWORK FOR INFOCOMM TECHNOLOGY SKILLS MAP – VULNERABILITY ASSESSMENT AND PENETRATION TESTING MANAGER** | | | | | |
| **Sector** | Infocomm Technology | | | | |
| **Track** | Cyber Security | | | | |
| **Sub-track** | Vulnerability Assessment and Penetration Testing | | | | |
| **Occupation** | ICT Security Specialist | | | | |
| **Job Role** | **Vulnerability Assessment and Penetration Testing Manager** | | | | |
| **Job Role 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, Key Tasks and Performance Expectations** | **Critical Work Functions** | **Key Tasks** | | | **Performance Expectations** |
| **Establish cyber security policies** | Develop policies and frameworks to conduct security penetration testing | | | In accordance with:     * Cyber Security Act 2018 by the Cyber Security Agency of Singapore |
| Establish certification-based policies for maintaining compliance | | |
| Formulate governance procedures for documenting and updating security testing policy, standards, guidelines and procedures | | |
| **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 | | |
| **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 | | |
| **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 | | |
| **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 | Computational Thinking | Advanced | |
| Budgeting | Level 5 | Digital Literacy | Advanced | |
| Business Performance Management | Level 5 | Global Mindset | Advanced | |
| Cyber Risk Management | Level 5 | Sense Making | Advanced | |
| Emerging Technology Synthesis | Level 5 | Creative Thinking | Advanced | |
| Learning and Development | Level 5 |  | | |
| Manpower Planning | Level 5 |
| Network Security | Level 5 |
| Networking | Level 5 |
| People and Performance Management | Level 5 |
| Security Assessment and Testing | Level 5 |
| Security Education and Awareness | Level 5 |
| Security Governance | Level 5 |
| Security Strategy | Level 5 |
| Stakeholder Management | Level 4 |
| Strategy Implementation | Level 4 |
| Strategy Planning | Level 5 |
| Test Planning | Level 5 |
| Threat Analysis and Defence | 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. | | | | | |