Information Systems Security Manager - Cybersecurity Operations

NICE Framework Reference	Oversee & Govern, OV-MGT-001, Information Systems Security Manager,	
Functional Description	Plans, organizes, directs, controls and evaluates the activities of the cybersecurity operations centre within an organization. Employed throughout the public and private sectors.	
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in catastrophic failure of organizational IT and data systems and associated implications to the organizational functions which rely on those systems.	
Development pathway	Typically follows 5 to 10 years in related roles in IT operations or cybersecurity operations or similar employment. This role supports increasing management level responsibilities based on a solid technical foundation in cybersecurity operations or a related work role (e.g. vulnerability assessment & management, digital forensics, cybersecurity analysis).	
Other titles	▪ Cybersecurity Operations Manager (CSOC) ▪ Security Operations (SOC) Manager ▪ Cybersecurity Manager ▪ Information Systems Security Manager (Cybersecurity Operations)	
Related NOCs	0213 Computer and information systems managers	
Tasks	▪ Lead and manage SOC personnel including hiring, training, staff development, performance management and conducting annual performance reviews ▪ Maintain currency in cybersecurity threat landscape and security technologies ▪ Develop and implement an integrated SOC program that meets legislative and organizational requirements ▪ Develop and publish SOC governance mechanisms (policies, procedures and guidance) ▪ Develop and implement a measurement and quality assurance program ▪ Monitor and report on SOC program effectiveness to senior management ▪ Monitor and manage relationships with security services and technologies providers ▪ Provide strategic assessments on threat landscape, SOC technology trends, and emerging security technologies ▪ Seek and interpret threat intelligence based on organizational risks ▪ Manage cybersecurity events and incidents within the SOC ▪ Provide reports, briefings and risk-based recommendations on routine and non-routine cybersecurity events and incidents including responding to organizational crises (e.g. business systems shut-downs) ▪ Lead and facilitate lessons learned, post-mortem and best practices activities on cybersecurity events and incidents ▪ Develop and oversee implementation of action plans in support of continuous improvement of cybersecurity posture	
Required qualifications	Education	Bachelor's degree in computer science or related discipline or College diploma in IT field.
	Training	Cybersecurity operations training with industry-level certification in related field (e.g. network security, incident handling, threat detection and mitigation, digital forensics).

<table>
<tr><td rowspan="2"></td><td></td><td>Security operations team management training or equivalent development and experience.
Training on organization relevant tools and technology that support cybersecurity operations</td></tr>
<tr><td>Work experience</td><td>Significant (5-10 years) experience in IT domain with 3-5 years' experience in cybersecurity operations or related domain.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Incident management processes and procedures
▪ Defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms
▪ Security event and incident management systems and/or incident reporting systems and networks,
▪ Authentication software and systems,
▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used
▪ Security services provided if applicable</td></tr>
<tr><td>Competencies</td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an activity manager as well as the Information Systems Security Manager within the NICE framework. Specifically, this work requires:

Basic level of application of the following KSAs:
☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls

Advanced level of application of the following KSAs
☐ Organizational threats and vulnerabilities including:
o Cybersecurity threat landscape and adapting SOC processes to meet the evolving threat
o Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist
☐ Defensive systems management including:
o Firewalls, anti-virus, intrusion detection and protection systems
o Required manual and automated settings
o Monitoring, testing and maintenance requirements
☐ Developing, implementing, and managing:
o Incident management processes and policies
o Incident management responsibilities
o Incident monitoring and reporting practices in accordance with legislative requirements and organizational policies
o Post-incident analyses and reports
o Organizational lessons learned in support of continuous improvement
☐ Supplier management (if IT or security services are outsourced):
o Roles and responsibilities of security controls of supplied services
o Roles and responsibilities of supplier in incident management and reporting
o Incident monitoring, assessment and reporting requirements during the lifecycle of the contract
o Organizational responsibilities in response to a compromise/breach on the part of the supplier
o Managing supplier communications and relations during a crisis
☐ Advising on security requirements, policies, plans and activities
☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)</td></tr>
</table>

	☐ Maintaining broader security situational awareness ☐ Self-awareness regarding knowledge, skills and abilities required to respond to business, threat and technical changes ☐ Continuous learning to support currency in knowledge of emerging threats, technological innovations in security, and the changing cybersecurity landscape.
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. Understanding quantum threat capabilities and knowledge and skills related to implementing a quantum safe strategy will be required.