Chief Information Security Officer (CISO)

NICE Framework Reference	Oversee and Govern, OV-EXL-001, Executive Cyber Leadership
Functional Description	An executive level role with accountability and responsibility for digital/information security activities of the organization. This includes planning, overseeing and managing strategy development and implementation, cybersecurity operations, as well as budget and resources that ensure protection of the enterprise information assets throughout the supply chain. Employed throughout the public and private sectors.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business. Lack of a full appreciation of the business needs for security will jeopardize the security posture of the organization in the face of evolving threats.
Development pathway	This is often considered the pinnacle of a cybersecurity career within a given organization. A CISO often has extensive experience (10+ years) in IT or systems, preferably with cybersecurity management experience. As an executive level position, the pathway also includes competency development including training, education and experience outside of the technical field.
Other titles	▪ Chief Security Officer ▪ Departmental Security Officer ▪ Information Security Director Note: depending on the size of the organization and the reliance on information technology, this occupational role may be subsumed within the responsibilities of the Chief Information Officer, Chief Technology Officer, Chief Resiliency Officer or similar role.
Related NOCs	0012 - Senior government managers and officials 0013 - Senior managers - financial, communications and other business services
Tasks	▪ Collaborate with key stakeholders to plan and establish an effective cybersecurity risk management program. ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement strategic plans that are aligned to the organizational objectives and security requirements ▪ Direct and approve the design of cybersecurity systems ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support cybersecurity objectives ▪ Advise other senior management on cybersecurity programs, policies, processes, systems, and elements ▪ Ensure development and implementation of security controls to support organizational objectives ▪ Review, approve, oversee monitoring of cybersecurity policies and controls ▪ Ensure incident response, disaster recovery and business continuity plans are in place and tested

<table>
<tr><td></td><td colspan="2">▪ Draft terms of reference, oversee and review cybersecurity investigations
▪ Maintain a current understanding the IT threat landscape for the business context;
▪ Schedule and oversee security assessments and audits
▪ Oversee and manage vendor relations related to acquired IT security products and services
▪ Provide training and mentoring to security team members
▪ Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.</td></tr>
<tr><td rowspan="3"><b>Required qualifications</b></td><td>Education</td><td>Bachelor’s degree in computer science or related discipline or equivalent training and experience.</td></tr>
<tr><td>Training</td><td>Role-based training to support senior level management of security preferred.</td></tr>
<tr><td>Work experience</td><td>Significant (5-10 years) experience in IT domain with 3-5 years’ experience in cybersecurity management roles.</td></tr>
<tr><td><b>Tools &amp; Technology</b></td><td colspan="2">▪ Strategic and business plans
▪ Threat and risk assessments
▪ Vulnerability management processes and vulnerability assessments
▪ Incident management processes and procedures
▪ Security event and incident management systems and/or incident reporting systems and networks,
▪ Cybersecurity risk management processes & policies
▪ Privacy and security legislation
▪ Organizational security infrastructure and reporting systems</td></tr>
<tr><td><b>Competencies</b></td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework.

Basic application of the following KSAs:
☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel)
☐ Preventative technical, operational and management controls available and organizational responsibilities for those controls
☐ Sector/context relevant threats, business needs and technical infrastructure
☐ Project management and security requirements throughout the project lifecycle
☐ Supply chain vulnerabilities and integrity

Advanced application of the following KSAs:
☐ Organizational threats and vulnerabilities including:
☐ Cybersecurity threat landscape
☐ Vulnerability management requirements and the range of potential mitigations available when a vulnerability management protocol does not exist
☐ Organizational security infrastructure including protective and defensive systems
☐ Developing, implementing and allocating resources, personnel and technology to address organizational security objectives.
☐ Identifying requirements and developing cybersecurity and cybersecurity risk management policies and procedures.</td></tr>
</table>

	□ Supplier management (if IT or security services are outsourced) □ Organizational communications, public communications and communicating during a crisis. □ Cybersecurity program management, measures and monitoring
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 cybersecurity responsibilities relative to organizational cybersecurity risks. As the primary security advisor to senior management, this discussion will be led by the CISO, therefore a full appreciation of the business risks is required. ▪ If practiced within the organization, there will be a requirement to fully understand the security implications of 'bring your own devices' (BYOD) and managing the associated risks. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the organizational security infrastructure and the implications to personnel, resources, procedures, and policies. This will need to be integrated into a security strategy and action plan for the organization. ▪ Increased use of automated tools by threat actors poses challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. ▪ 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 be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. Actions will also need to consider the organizational constraints and alternatives. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require advanced knowledge and skills related to implementing a quantum safe strategy and supporting processes within the organization.