

Information System Security Officer (ISSO)

NICE Framework Reference	None.
Functional Description	This is an adhoc management role within cybersecurity that is primarily engaged in oversight and reporting of information system security within a department, branch, or organization. This role is primarily responsible for local planning and management of the security of system(s) over which they have been given authority. This role may report indirectly or directly to the CISO or another authority (e.g. Corporate Security Officer or Chief Information Officer or their delegate).
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in decisions or actions that could compromise the security of the system over which the ISSO has authority. Depending on the system, this could have a significant impact on the business. A 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 commonly a part-time role assigned or assumed by an individual with some technical experience but is not normally a 'cybersecurity professional'. In small and medium organizations this role may also be an IT manager or senior manager with some technical or security experience.
Other titles	<ul style="list-style-type: none"> ▪ Chief Security Officer ▪ Departmental Security Officer ▪ Information Security Director <p>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.</p>
Related NOCs	0213 – Communication and Information Systems Managers
Tasks	<ul style="list-style-type: none"> ▪ 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 ▪ Draft terms of reference, oversee and review cybersecurity investigations

	<ul style="list-style-type: none"> ▪ 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 ▪ Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. 	
Required qualifications	Education	Post-secondary education in a cyber or IT related field (e.g.; Computer engineering, Computer Science, Information Technology, Business Technology Management – Digital Security or equivalent)
	Training	As required to support the role for example cybersecurity team management, incident management and cybersecurity planning would be an asset.
	Work experience	3-5 years' experience in IT domain with some management experience.
Tools & Technology	<ul style="list-style-type: none"> ▪ 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 	
Competencies	<p>Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework.</p> <p>Basic application of the following KSAs:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) <input type="checkbox"/> Preventative technical, operational and management controls available and organizational responsibilities for those controls <input type="checkbox"/> Sector/context relevant threats, business needs and technical infrastructure <input type="checkbox"/> Project management and security requirements throughout the project lifecycle <input type="checkbox"/> Supply chain vulnerabilities and integrity <p>Advanced application of the following KSAs:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Organizational threats and vulnerabilities including: <ul style="list-style-type: none"> ○ 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 <input type="checkbox"/> Cybersecurity team management <input type="checkbox"/> Developing, implementing and allocating resources, personnel and technology to address organizational security objectives. 	

	<ul style="list-style-type: none"> <input type="checkbox"/> Identifying requirements and developing cybersecurity and cybersecurity risk management policies and procedures. <input type="checkbox"/> Supplier management (if IT or security services are outsourced) <input type="checkbox"/> Organizational communications, public communications and communicating during a crisis. <input type="checkbox"/> Cybersecurity program management, measures and monitoring
<p>Future Trends Affecting Key Competencies</p>	<ul style="list-style-type: none"> ▪ 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 a senior security advisor to management, this role will need 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.