Supply Chain Security Analyst

NICE Framework Reference	None.
Functional Description	Has the primary responsibility to collect and analyze data to identify cybersecurity flaws and vulnerabilities in an organization's supply chain operations, and to provide advice and guidance to help reduce these supply chain risks.
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in organizational decisions that can have a significant impact on the business.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	Typically drawn from cybersecurity analysis roles (e.g. Cybersecurity operations analyst, vulnerability analyst, etc.) this role can nonetheless be assumed by a broad cross-section of professionals who can assess and provide insights on the potential supply chain threats. This includes those who may specialize in human factors aspects of supply chain (e.g. close access, insider threat).
Other titles	Cybersecurity analyst Supply chain integrity analyst
Related NOCs	2171 Information systems analysts and consultants 2174 Computer programmers and interactive media developers
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement plans that are aligned to the organizational objectives and security requirements ▪ Collect and analyze supply chain relevant information to identify and mitigate flaws and vulnerabilities, including component integrity, in an organization's computer networks or systems ▪ Analyze system hardware and software configurations ▪ Recommend hardware, software, and countermeasures to install or update based on cyber threats and security vulnerabilities ▪ Coordinate with colleagues to implement changes and new systems ▪ Track and report on cyber threats and security vulnerabilities that impact supply chain performance ▪ Define, develop, implement, and maintain cybersecurity plans, policies and procedures ▪ Ensure compliance with cybersecurity policies, regulations, and procedures of the organization ▪ Ensure compliance with security requirements of organization networks and systems ▪ Develop and maintain risk assessments and related reports on vendors, products and services ▪ Define and maintain tool sets and procedures that support supply chain integrity ▪ Prepare technical reports

	▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to cybersecurity and supply chain integrity	
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	In addition to formal training in cybersecurity analysis, specialized training and skills in vulnerability analysis and supply chain threats required.
	Work experience	Individuals employed in this role can have diverse levels of cybersecurity expertise. Requested experience will depend on the organizational need and complexity of systems to be analyzed.
Tools & Technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessment tools and applications ▪ Incident management processes and procedures ▪ Organizational security infrastructure and reporting systems Security event and incident management systems and/or incident reporting systems and networks, ▪ Cybersecurity risk management processes & policies across the supply chain ▪ Third party and service level agreements and contracts	
Competencies	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 ☐ Procurement processes and security requirements Advanced application of the following KSAs: ☐ Organizational security infrastructure including protective and defensive systems across the supply chain ☐ Cybersecurity threat landscape and threat intelligence sources for supply chain threats ☐ Legal and compliance requirements as they extend to organizational third-party arrangements ☐ Vulnerability analysis and tools ☐ Advanced security information and data security analysis and techniques ☐ Functional and technical design of networks and system, and cybersecurity solutions ☐ Risk management processes, responsibilities and authorities within the organization and across the supply chain ☐ Third party risk management and liability	

	□ System life cycle management principles, including software security and usability □ Current national supply chain processes
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. ▪ 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. ▪ 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. ▪ 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. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization.