Information Security (IS) Auditor

NICE Framework Reference	None. Associated with OV-PMA-005 IT Program Auditor	
Functional Description	A specialized auditor role, an information security auditor is responsible for evaluating and reporting on the security and effectiveness of IT systems and related controls in support of organizational information / data security, IT systems and their components. The audit conducted is often reported to a senior manager with recommendations for changes or improvements.	
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in an incomplete or inaccurate audit that does not identify critical system or process issues and fails to address organizational security requirements and increasing the potential risks of a compromise or security system failure.	
Development pathway	Employment in this role is often preceded by formal education with a degree or diploma in an IT field as well as experience in an organizational cybersecurity role. There is also a requirement for specialized training and education in information system and information security audit practices.	
Other titles	Cybersecurity auditor Security control assessor IT security auditor	
Related NOCs	2171 - Information systems analysts and consultants 2147 – Computer Engineers	
Tasks	▪ Collaborate with key stakeholders to establish an effective information security audit strategy which defines both internal and external audit requirements ▪ Liaise with external auditors as required to support organizational requirements ▪ Ensure compliance with the changing laws and applicable regulations ▪ Develop and implement detailed internal audit plans that are aligned to the organizational objectives and security requirements ▪ Identify, acquire and oversee management of financial, technical and personnel resources required to support IS audit activities ▪ Develop and deploy policy testing on IS systems ▪ Review security assessment and authorization activities ▪ Advise other senior management on cybersecurity programs, policies, processes, systems, and elements ▪ Review and interpret cybersecurity / information security policies and controls ▪ Maintain a current understanding the IT threat landscape for the business context ▪ Schedule and conduct internal IS audits ▪ Analyze and interpret and external IS audit results ▪ Report results and provide recommendations to leadership and system owner(s).	
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	Specialized training in IT or information system audit and security audit.
	Work experience	Experience (3-5 years) in cybersecurity with preference in systems analytics (e.g. cybersecurity operations analyst, vulnerability analyst, IT systems security analyst)
Tools & Technology	▪ Strategic and business plans ▪ Threat and risk assessments ▪ Vulnerability management processes and vulnerability assessments ▪ Incident management processes and procedures ▪ Cybersecurity risk management processes & policies ▪ Compliance requirements including privacy and security legislation ▪ Organizational security infrastructure and reporting systems ▪ IS audit tools and systems ▪ Vulnerability assessments ▪ Penetration testing results ▪ IT systems performance measures	
Competencies	Basic application of the following KSAs: ☐ Project and program management ☐ IT audit policies, practices and procedures Advanced application of the following KSAs: ☐ Legal, policy and compliance requirements ☐ Business objectives and how IT/data/systems enable the business ☐ Information security audit polices, practices and procedures ☐ Integrated/organizational security concepts, principles and practice (software, system, data, physical and personnel) ☐ External audit resources, competencies and capabilities ☐ Sector/context relevant threats, business needs and technical infrastructure ☐ Organizational security responsibilities, accountabilities and performance measures ☐ Cybersecurity program management, measures and monitoring ☐ Organizational cybersecurity controls and responsible agents ☐ Organizational threats and vulnerabilities including: o Cybersecurity threat landscape o Vulnerability assessments and application of mitigations o Organizational security infrastructure including protective and defensive systems ☐ Security throughout the system / software development lifecycle ☐ Supply chain security ☐ System integration, testing and deployment ☐ Supplier management (if IT or security services are outsourced) and supply arrangements	
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or ‘cloud-based’ services will require knowledge of responsibilities of the services provider and linkages with organizational systems. ▪ 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 are integrated into the organizational security infrastructure, the implications to security controls and how they will be measured and assessed against security goals. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Therefore, audits of defensive tools and systems will evolve. ▪ 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 how those tools operate, how their performance can be measured and what audit activities may be necessary. ▪ 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.