Security Testing and Evaluation Specialist

NICE Framework Reference	Securely Provision, Security Testing and Evaluation, SP-TST-001	
Functional Description	Plans, prepares, and executes tests of security devices, operating systems, software and hardware to evaluate results against defined specifications, policies, and requirements, and documents results and makes recommendations that can improve information confidentiality, integrity, and availability.	
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in IT systems, software or services being integrated and deployed with vulnerabilities that increase threat exposure and organizational risk. Resulting compromises could have a significant impact on the business.	
Development pathway	Typically follows formal education and 5-10 years' experience in IT security. This role often requires specialized training, education or experience related to systems testing and measurement.	
Other titles	Systems security assessor	
Related NOCs	2171 Information systems analysts and consultants 2147 Computer engineers (except software engineers and designers)	
Tasks	▪ Tests, evaluates, and verifies systems under development; systems exchanging electronic information with other systems; related operating system software and hardware; and security controls and devices used within an organization to determine level of compliance with defined specifications, policies, and requirements ▪ Analyze test results of operating systems, software, and hardware and make recommendations based on finding ▪ Develop test plans to address specifications, policies, and requirements ▪ Validate specifications, policies and requirements for testability ▪ Create verifiable evidence of security measure ▪ Prepare assessments that document the test results and any security vulnerabilities present ▪ Deploy, validate, and verify network infrastructure device operation ▪ Develop, deliver, and oversee training material and educational efforts ▪ Provide training and mentoring to security team members	
Required qualifications	Education	Bachelor's degree in computer science or related discipline or equivalent training and experience.
	Training	Training in system security measurement, assessment and testing.
	Work experience	Significant (5-10 years) experience in IT domain with 3-5 years' experience in systems security role supporting security assessments and IT audits preferred. Experience working in secured testing environments.
Tools & Technology	▪ 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, ▪ System architecture ▪ Cybersecurity risk management processes & policies ▪ Privacy and security legislation ▪ Organizational security infrastructure and reporting systems ▪ System testing and evaluation policies tools, techniques, procedures and protocols ▪ Legislation and compliance requirements
Competencies	Basic application of the following KSAs: ☐ Security procurement processes and supply chain integrity assessments ☐ Systems engineering process Advanced application of the following KSAs: ☐ Security assessment and authorization processes ☐ IT systems testing and evaluation strategies ☐ IT systems testing and evaluation infrastructure and resources ☐ IT security systems testing and evaluations tools, procedures and practices ☐ Technical knowledge of networks, computer components, power supply technology, system protocols, cybersecurity-enabled software ☐ Network security architecture and models ☐ Conducting independent validation and verification security testing ☐ Systems testing and evaluation methods and techniques ☐ Test design, scenario development, and readiness review ☐ Systems integration testing ☐ Security assessment and authorization processes ☐ Security architecture concepts and enterprise information security architecture model ☐ Identifying test and evaluation policies and requirements ☐ Collect, analyze, verify and validate test data and translate data and test results into conclusion ☐ Designing and document test and evaluation strategies ☐ Writing technical and test and evaluation reports.
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 systems, how those systems are integrated and how they can be tested and evaluated. ▪ 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 to organizational systems. ▪ 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 testing and evaluation practices. ▪ Increased use of automated tools by threat actors pose challenges that will require continuous assessment of testing and evaluation practices and required tools. ▪ 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 and any implications on security testing and evaluation. ▪ 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 relevant to testing and evaluating encryption and degree of quantum resistance.