Secure Software Assessor

NICE Framework Reference	Security Provision, SP Dev-001, Secure Software Assessor	
Functional Description	Given references, organizational security documentation, cybersecurity guidance and required tools and resources, analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.	
Consequence of error or risk	Error, neglect, outdated information could result in vulnerabilities in software and web-based tools can place organizational systems and services at risk.	
Development pathway	Typically follows formal education and 5-10 years' experience in the software development field. This role often requires advanced training, education or experience related to secure software and vulnerability assessment activities for software / application security.	
Other titles	▪ Secure software developer/programmer ▪ Software testing and evaluation specialists ▪ Vulnerability analyst / assessor	
Related NOCs	2171 Information systems analysts and consultants 2173 Software engineers/designers 2174 Computer programmers and interactive media developers	
Tasks	▪ Define/validate business needs for security & security requirements ▪ Review and analyze security IT architectures & design documents, as well as related systems, protocols, services, controls, appliances, applications, encryption and crypto algorithms relative to security requirements and industry standards ▪ Research, analyze and implement secure application development processes and techniques; ▪ Analyze the security data and provide advisories and reports ▪ Develop and conduct software system or application testing and validation procedures, programming, and secure coding, and report on functionality and resiliency; ▪ Develop and review system use cases ▪ Conduct vulnerability scans and reviews on software systems or applications, and examine controls and measures required to protect software systems or applications; ▪ Prepare reports on software systems, development and applications, patches or releases that would leave systems vulnerable; ▪ Develop countermeasures against potential exploitations of vulnerabilities in systems; ▪ Perform risk analysis whenever an application or system undergoes a change; and ▪ Prepare technical reports such as IT security solutions option analysis and implementation plans ▪ Provide Independent Verification and Validation (IV&V) on software projects ▪ Advise on software security policies, plans and practices ▪ Review, develop and deliver training materials	
Required qualifications	Education	Relevant computer science degree or diploma related to programming, software design or software development

	Training	Valid industry level certification in related secure software development and software security testing
	Work experience	Moderate experience (3-5 years) in software development followed by moderate experience (3-5 years) in secure software development activities.
Tools & Technology	▪ Software development tools, processes and protocols ▪ Threat and risk assessment tools and methodologies ▪ Protective and defensive systems including firewalls, anti-virus software and systems, intrusion detection and protection systems, scanners and alarms ▪ Open source software and application security information (e.g. OWASP) ▪ Security event and incident management systems and/or incident reporting systems and networks ▪ Software security testing and evaluation tools and techniques ▪ Authentication software and systems, ▪ Vulnerability management processes and vulnerability assessment systems including penetration testing if used ▪ Common vulnerability data bases ▪ Software development social collaboration sites (e.g. GITHUB) ▪ Security services provided if applicable	
Competencies	Basic application of the following KSAs: ☐ Security architecture concepts and enterprise information security architecture model ☐ Security assessment and authorization processes ☐ Software procurement processes and supply chain integrity assessments ☐ IT security systems testing and evaluations tools, procedures and practices Advanced application of the following KSAs: ☐ Software engineering models, processes and principles ☐ Software development lifecycle and software project management ☐ Secure coding/software development operations processes, procedures, practices, tools and techniques ☐ Business needs for security including compliance requirements ☐ Data security characteristics and requirements ☐ Security controls for software development ☐ Software development standards ☐ Secure software standards ☐ Secure software testing and evaluation methodologies and processes ☐ Vulnerability assessment and penetration testing methodologies and applications ☐ Developing and testing threat models ☐ Vulnerability scanning, assessment and analysis ☐ Penetration testing activities and techniques ☐ Investigating and analyzing software vulnerabilities and breaches ☐ Establishing and managing a secure software/ web application testing environment ☐ Advising on security requirements, policies, plans and activities ☐ Drafting and providing briefings and reports to different audience levels (users, managers, executives)	
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services to be provided, software systems and applications used and how they are integrated into the organizational networks.	

	▪ If practiced within the organization, there will be a requirement to fully understand the implications of ‘bring your own device’ (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization and mitigations implemented to the level of acceptable risk. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools that may support software development, testing and integration will be used as well as the potential security implications. If automated security tools in software development and assessment, responsibilities for testing, integration and monitoring requirements will need to be defined and those responsible for these activities will need to be advised / trained on the resulting process and procedural changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant assessments of the robustness of software / applications security and potential mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ 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 for increased understanding of organizational risks posed within the dynamic threat environment. ▪ 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 as it applies to the software/application environment.