Security Architect

NICE Framework Reference	Securely Provision, SP-ARC 002, Security Architect
Functional Description	Designs, develops and oversees the implementation of network and computer security structures for an organization, ensuring security requirements are adequately addressed in all aspects of the infrastructure, and the system supports an organization's processes
Consequence of error or risk	Error, neglect, outdated information or poor judgment could result in flawed designs or architectures that could fail or experience exploitable vulnerabilities which could place IT systems upon which the organization relies in jeopardy. 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	Primarily following education and a career pathway from an existing enterprise architect role, this is an emerging specialist role primarily employed in large tech-enabled organizations, shared services or systems or security providers.
Other titles	Enterprise security architect
Related NOCs	2147 Computer engineers (except software engineers and designers) 2171 Information systems analysts and consultants
Tasks	▪ Collaborate with key stakeholders to establish an effective cybersecurity risk management program ▪ Ensure compliance with the changing laws and applicable regulations ▪ Define and review an organization's technology and information systems, and ensure security requirements ▪ Recognize appropriate disaster recovery plans and business continuity functions, including any failover or backup requirements for system restoration ▪ Plan, research, and develop robust security architectures for systems and networks ▪ Research current and emerging technologies to understand capabilities of required networks or systems ▪ Prepare cost estimates and identify integration issues ▪ Conduct vulnerability testing, risk analyses and security assessments ▪ Research and develop a system security context, and define security assurance requirements based on industry standards and cybersecurity policies and practices ▪ Ensure the acquired or developed systems and architectures are consistent with an organization's cybersecurity policies and practices ▪ Perform security reviews and identify gaps or determine the capability of security architectures and designs (e.g., firewall, virtual private networks, routers, servers, etc.), and develop a security risk management plan ▪ Prepare technical reports that document the architecture development process

<table>
<tr><td></td><td colspan="2">▪ Document and address an organization's information security, cybersecurity architecture, and systems security engineering requirements throughout a system life cycle
▪ Advise on security requirements and risk management process activities
▪ Support incident management and post-analysis advising on recovery operations
▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>Post-secondary education in IT infrastructure and architecture (e.g.; computer engineering, IT systems architecture)</td></tr>
<tr><td>Training</td><td>Specialized training in security architecture concepts, principles, and practices. Training to support security tools needed to support role.</td></tr>
<tr><td>Work experience</td><td>Previous training and experience in IT security infrastructure, requirements analysis or program management is preferred – 5-10 years of relevant IT experience for advanced-level.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">▪ Strategic and business plans
▪ Threat and risk assessments
▪ Systems architectures
▪ IT mapping tools and applications
▪ 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</td></tr>
<tr><td>Competencies</td><td colspan="2">Underpinning this occupation are those competencies demonstrated for an executive level which include those identified within the NICE framework.

Advanced application of the following KSAs:
☐ Business needs for security
☐ Legal, policy and compliance requirements
☐ 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
☐ Cryptography and cryptographic key management concepts;
☐ Virtual Private Network devices and encryption;
☐ Engineering concepts and practices as applied to systems security and systems architecture
☐ Security architecture concepts and enterprise architecture reference models;
☐ Security assessment and authorization processes
☐ Authentication, authorization, and access control methods
☐ System testing and evaluation methodologies and processes</td></tr>
</table>

	☐ Application security system concepts and functions ☐ System life cycle management principles, including software security and usability ☐ Industry standards and organizationally accepted analysis principles and methods ☐ Configuring and using software-based computer protection tools ☐ Designing hardware and software solutions ☐ Cybersecurity program management, measures and monitoring ☐ Incident management and system recovery planning and operations
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require deep knowledge at the intersection between organizational and service providers architectures to determine and manage 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 how security controls are integrated into the organizational infrastructure. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the overall security architecture and 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 that will need to be integrated into the security architecture. ▪ 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 to support an integrated security architecture. ▪ 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 and integrating it across the architecture.