**Authorizing Official/Designating Representative**

**NICE SP-RSK-001**

Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

**Specialty Area:**Internal Cybersecurity Auditor

**Knowledges**

[**K0001**](https://performatron.risk-redux.io/nice_knowledges/K0001): Knowledge of computer networking concepts and protocols, and network security methodologies.

[**K0002**](https://performatron.risk-redux.io/nice_knowledges/K0002): Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

[**K0003**](https://performatron.risk-redux.io/nice_knowledges/K0003): Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

[**K0004**](https://performatron.risk-redux.io/nice_knowledges/K0004): Knowledge of cybersecurity and privacy principles.

[**K0005**](https://performatron.risk-redux.io/nice_knowledges/K0005): Knowledge of cyber threats and vulnerabilities.

[**K0006**](https://performatron.risk-redux.io/nice_knowledges/K0006): Knowledge of specific operational impacts of cybersecurity lapses.

[**K0013**](https://performatron.risk-redux.io/nice_knowledges/K0013): Knowledge of cyber defense and vulnerability assessment tools and their capabilities.

[**K0019**](https://performatron.risk-redux.io/nice_knowledges/K0019): Knowledge of cryptography and cryptographic key management concepts

[**K0027**](https://performatron.risk-redux.io/nice_knowledges/K0027): Knowledge of organization's enterprise information security architecture.

[**K0028**](https://performatron.risk-redux.io/nice_knowledges/K0028): Knowledge of organization's evaluation and validation requirements.

[**K0037**](https://performatron.risk-redux.io/nice_knowledges/K0037): Knowledge of Security Assessment and Authorization process.

[**K0038**](https://performatron.risk-redux.io/nice_knowledges/K0038): Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.

[**K0040**](https://performatron.risk-redux.io/nice_knowledges/K0040): Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).

[**K0044**](https://performatron.risk-redux.io/nice_knowledges/K0044): Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

[**K0048**](https://performatron.risk-redux.io/nice_knowledges/K0048): Knowledge of Risk Management Framework (RMF) requirements.

[**K0049**](https://performatron.risk-redux.io/nice_knowledges/K0049): Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).

[**K0054**](https://performatron.risk-redux.io/nice_knowledges/K0054): Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.

[**K0059**](https://performatron.risk-redux.io/nice_knowledges/K0059): Knowledge of new and emerging information technology (IT) and cybersecurity technologies.

[**K0070**](https://performatron.risk-redux.io/nice_knowledges/K0070): Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).

[**K0084**](https://performatron.risk-redux.io/nice_knowledges/K0084): Knowledge of structured analysis principles and methods.

[**K0089**](https://performatron.risk-redux.io/nice_knowledges/K0089): Knowledge of systems diagnostic tools and fault identification techniques.

[**K0101**](https://performatron.risk-redux.io/nice_knowledges/K0101): Knowledge of the organization’s enterprise information technology (IT) goals and objectives.

[**K0126**](https://performatron.risk-redux.io/nice_knowledges/K0126)**:** Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)

[**K0146**](https://performatron.risk-redux.io/nice_knowledges/K0146)**:** Knowledge of the organization's core business/mission processes.

[**K0168**](https://performatron.risk-redux.io/nice_knowledges/K0168)**:** Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.

[**K0169**](https://performatron.risk-redux.io/nice_knowledges/K0169)**:** Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.

[**K0170**](https://performatron.risk-redux.io/nice_knowledges/K0170)**:** Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.

[**K0179**](https://performatron.risk-redux.io/nice_knowledges/K0179)**:** Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).

[**K0199**](https://performatron.risk-redux.io/nice_knowledges/K0199)**:** Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).

[**K0203**](https://performatron.risk-redux.io/nice_knowledges/K0203)**:** Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).

[**K0260**](https://performatron.risk-redux.io/nice_knowledges/K0260)**:** Knowledge of Personally Identifiable Information (PII) data security standards.

[**K0261**](https://performatron.risk-redux.io/nice_knowledges/K0261)**:** Knowledge of Payment Card Industry (PCI) data security standards.

[**K0262**](https://performatron.risk-redux.io/nice_knowledges/K0262)**:** Knowledge of Personal Health Information (PHI) data security standards.

[**K0267**](https://performatron.risk-redux.io/nice_knowledges/K0267)**:** Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.

[**K0295**](https://performatron.risk-redux.io/nice_knowledges/K0295)**:** Knowledge of confidentiality, integrity, and availability principles.

[**K0322**](https://performatron.risk-redux.io/nice_knowledges/K0322)**:** Knowledge of embedded systems.

[**K0342**](https://performatron.risk-redux.io/nice_knowledges/K0342)**:** Knowledge of penetration testing principles, tools, and techniques.

[**K0622**](https://performatron.risk-redux.io/nice_knowledges/K0622)**:** Knowledge of controls related to the use, processing, storage, and transmission of data.

[**K0624**](https://performatron.risk-redux.io/nice_knowledges/K0624)**:** Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

**Skills**

[**S0034**](https://performatron.risk-redux.io/nice_skills/S0034): Skill in discerning the protection needs (i.e., security controls) of information systems and networks.

[**S0367**](https://performatron.risk-redux.io/nice_skills/S0367): Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

**Abilities**

[**A0028**](https://performatron.risk-redux.io/nice_abilities/A0028): Ability to assess and forecast manpower requirements to meet organizational objectives.

[**A0033**](https://performatron.risk-redux.io/nice_abilities/A0033): Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.

[**A0077**](https://performatron.risk-redux.io/nice_abilities/A0077): Ability to coordinate cyber operations with other organization functions or support activities.

[**A0090**](https://performatron.risk-redux.io/nice_abilities/A0090): Ability to identify external partners with common cyber operations interests.

[**A0094**](https://performatron.risk-redux.io/nice_abilities/A0094): Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.

[**A0111**](https://performatron.risk-redux.io/nice_abilities/A0111): Ability to work across departments and business units to implement organization’s privacy principles and programs, and align privacy objectives with security objectives.

[**A0117**](https://performatron.risk-redux.io/nice_abilities/A0117): Ability to relate strategy, business, and technology in the context of organizational dynamics.

[**A0118**](https://performatron.risk-redux.io/nice_abilities/A0118): Ability to understand technology, management, and leadership issues related to organization processes and problem solving.

[**A0119**](https://performatron.risk-redux.io/nice_abilities/A0119): Ability to understand the basic concepts and issues related to cyber and its organizational impact.

[**A0123**](https://performatron.risk-redux.io/nice_abilities/A0123): Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

[**A0170**](https://performatron.risk-redux.io/nice_abilities/A0170): Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

**Tasks**

[**T0145**](https://performatron.risk-redux.io/nice_tasks/T0145): Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).

[**T0221**](https://performatron.risk-redux.io/nice_tasks/T0221): Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.

[**T0371**](https://performatron.risk-redux.io/nice_tasks/T0371): Establish acceptable limits for the software application, network, or system.

[**T0495**](https://performatron.risk-redux.io/nice_tasks/T0495): Manage Accreditation Packages (e.g., ISO/IEC 15026-2).