CAREER PATHWAY SECURITY CONTROL ASSESSOR (612)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 612-SECURITY CONTROL ASSESSOR

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 612-Security Control Assessor.

Table 1. 612- Security Control Assessor Work Role Overview

NICE Role Description	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).
OPM Occupational Series	Personnel performing the 612-Security Control Assessor work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 72% - 0080-Security Administration – 8% - 0343-Management and Program Analysis – 8% - 1550-Computer Science – 4% - 0854-Computer Engineering – 3%
Work Role Pairings	Personnel performing the 612-Security Control Assessor work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 541-Vulnerability Assessment Analyst – 20% - 722-Information Systems Security Manager – 11% - 622-Secure Software Assessor – 10% - 671-System Testing and Evaluation – 9% - 461-Systems Security Analyst – 8%
Functional Titles	Personnel performing the 612-Security Control Assessor work role may unofficially or alternatively be called: - Information Assurance (IA) Compliance Analyst - Information Assurance (IA) Auditor - Certifying Agent/Authority - System Certifier - Controls Validator - IT Auditor - Assessor

Distribution of GS-Levels	Personnel performing the 612-Security Control Assessor work role are most commonly found within the following grades on the General Schedule. - ☐ GS-5 – redacted** - ☐ GS-6 – redacted** - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☐ GS-10 – redacted** - ☒ GS-11 – 5% - ☒ GS-12 – 15% - ☒ GS-13 – 35% - ☒ GS-14 – 16% - ☒ GS-15 – 4% *23% of all 612s are in non-GS pay plans and excluded from this section **Percentages below 3% are redacted.
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 612-Security Control Assessor work role: - 461-Systems Security Analyst - 541-Vulnerability Assessment Analyst - 622-Secure Software Assessor - 671-System Testing and Evaluation Specialist - 722-Information Systems Security Manager
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 612-Security Control Assessor. This is not an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles: - 461-Systems Security Analyst - 541-Vulnerability Assessment Analyst - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 211-Law Enforcement Counterintelligence Forensics Analyst work role, individuals may prepare themselves to transition into one or more of the following cross-functional work roles: - *711-Cyber Instructional Curriculum Developer* - *712-Cyber Instructor* - *732-Privacy Compliance Manager / Officer* - *751-Cyber Workforce Developer and Manager*

	- *752-Cyber Policy and Strategy Planner* - *802-IT Project Manager* - *803-Product Support Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 612-Security Control Assessor work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 612- Security Control Assessor Core Tasks

Task ID	Task	Core or Additional
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Core
T0079	Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.	Core
T0083	Draft statements of preliminary or residual security risks for system operation.	Core
T0141	Maintain information systems assurance and accreditation materials.	Core
T0150	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.	Core
T0309	Assess the effectiveness of security controls.	Core
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Core
T0178	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Core
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Core
T0184	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Core
T0244	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Core
T0145	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Additional
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Additional
T0251	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	Additional
T0371	Establish acceptable limits for the software application, network, or system.	Additional
T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Additional
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Additional

Task ID	Task	Core or Additional
T0243	Verify and update security documentation reflecting the application/system security design features.	Additional
T0255	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Additional
T0264	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Additional
T0265	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Additional
T0268	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Additional
T0272	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Additional
T0275	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Additional
T0277	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Additional

1.3 CORE KNOWLEDGE, SKILLS, AND ABILITIES

The table below provides a ranking of KSAs that represent the Core, or baseline, expectations for performance in the 612-Security Control Assessor work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 612- Security Control Assessor Core Knowledge, Skills, and Abilities

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity principles.	Information Systems/Network Security	Foundational to all work roles.
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to all work roles.
K0003	Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	Legal, Government, and Jurisprudence	Foundational to all work roles.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to all work roles.
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to all work roles.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to all work roles.
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.	Information Assurance	Core
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance	Core
K0037	Knowledge of the Security Assessment and Authorization process.	Information Assurance	Core
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security	Core
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Core
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security	Core

KSA ID	Description	Competency	Importance to Work Role
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment	Core
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	Legal, Government, and Jurisprudence	Core
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management	Core
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation	Core
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	Vulnerabilities Assessment	Core
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Vulnerabilities Assessment	Core
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment	Core
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).	Vulnerabilities Assessment	Core
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection	Additional
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection	Additional
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Additional
K0019	Knowledge of cryptography and cryptographic key management concepts.	Encryption	Additional
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zackman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture	Additional
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture	Additional
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance	Additional
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance	Additional
S0006	Skill in applying confidentiality, integrity, and availability principles.	Information Assurance	Additional
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Additional

KSA ID	Description	Competency	Importance to Work Role
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	Information Technology Assessment	Additional
K0322	Knowledge of embedded systems.	Infrastructure Design	Additional
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design	Additional
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed.	Legal, Government, and Jurisprudence	Additional
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness	Additional
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	Risk Management	Additional
K0084	Knowledge of structured analysis principles and methods.	Risk Management	Additional
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation	Additional
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness	Additional
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 511-Cyber Defense Analyst work role, and their associated importance. Listed competencies are collections of three or more similar Knowledge, Skills, or Abilities aligned to the Work Role. *These competencies originate from the NICE Framework Competency Pivot Tool.*

Table 4. 612- Security Control Assessor Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Risk Management	C044	This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.	• Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). [*K0002] • Knowledge of Risk Management Framework (RMF) requirements. [K0048] • Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures. [K0169] • Knowledge of structured analysis principles and methods. [K0084]	Core
Information Assurance	C022	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	• 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. [K0054] • Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [K0044] • Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data. [K0038] • Knowledge of the Security Assessment and Authorization process. [K0037] • Knowledge of organization's enterprise information security architecture system. [K0027] • Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). [K0203] • Skill in applying confidentiality, integrity, and availability principles. [S0006]	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Information Systems/Network Security	C024	This area contains KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.	• Knowledge of cybersecurity principles. [*K0004] • Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). [K0049] • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). [K0179] • Skill in discerning the protection needs (i.e., security controls) of information systems and networks. [S0034]	Core
Vulnerabilities Assessment	C057	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Knowledge of cyber threats and vulnerabilities. [*K0005] • Knowledge of specific operational impacts of cybersecurity lapses. [*K0006] • Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities. [K0013] • Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins. [K0040] • Knowledge of penetration testing principles, tools, and techniques. [K0342] • 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). [K0070] • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. [S0001]	Core
Data Privacy and Protection	C014	This area contains KSAs that relate to the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them	• Knowledge of Payment Card Industry (PCI) data security standards. [K0261] • Knowledge of Personal Health Information (PHI) data security standards. [K0262] • Knowledge of Personally Identifiable Information (PII) data security standards. [K0260]	Additional
Enterprise Architecture	C018	This area contains KSAs that relate to the	• Knowledge of security architecture concepts and enterprise architecture reference models (e.g.,	Additional

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
		principles, concepts, and methods of enterprise architecture to align information technology (IT) strategy, plans, and systems with the mission, goals, structure, and processes of the organization.	Zackman, Federal Enterprise Architecture [FEA]). [K0199] • Knowledge of the organization's enterprise information technology (IT) goals and objectives. [K0101]	
Infrastructure Design	C026	This area contains KSAs that relate to the architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.	• Knowledge of computer networking concepts and protocols, and network security methodologies. [*K0001] • Knowledge of embedded systems. [K0322] • Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability. [K0170]	Additional
Legal, Governance, and Jurisprudence	C030	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.	• Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity. [*K0003] • Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure. [K0267] • Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy 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 relevant to work performed. [K0168]	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 612-Security Control Assessor Suggested Qualifications / Capability Indicators

For indicators of capability for the 612-Security Control Assessor work role, please see Draft NISTR 8193 - National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators.

Section to be populated with updated DoD-8140 Qualification Matrix for 612-Security Control Assessor.

2 APPENDIX: 612-SECURITY CONTROL ASSESSOR TASK ANALYSIS AND KSA MAPPING

2.1 KEY TO READING THE TASK ANALYSIS AND KSA MAPPING

Table 6. Key to Reading the Task Analysis and KSA Mapping

Proficiency	Task Statement	Importance
As Written	Task as written within the NICE Cybersecurity Workforce Framework (NICE Framework).	Overall Importance to Work Role
Entry	*Example behavioral indicator / task permutation for performing this task at an Entry skills proficiency level.*	
Intermediate	*Example behavioral indicator / task permutation for performing this task at an Intermediate skills proficiency level.*	
Advanced	*Example behavioral indicator / task permutation for performing this task at an Advanced skills proficiency level.*	

Table 7. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
ID of K, S, or A	Knowledge, Skill or Ability needed to perform the task as written within the NICE Framework	Competency mapped to the individual K, S, or A.

2.2 612-Security Control Assessor Task Analysis and KSA Mapping

Table 8. T0072 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Core
Entry	*Demonstrate knowledge of methods to monitor and measure risk, compliance, and assurance efforts.*	
Intermediate	*[Assist with] developing methods to monitor and measure risk, compliance, and assurance efforts.*	
Advanced	*Develop, review and/or approve methods to monitor and measure risk, compliance, and assurance efforts.*	

Table 9. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
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.	Information Assurance
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.	Information Assurance
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0037	Knowledge of the Security Assessment and Authorization process.	Information Assurance
S0006	Skill in applying confidentiality, integrity, and availability principles.	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	Risk Management
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Vulnerabilities Assessment

KSA ID	Description	Competency
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).	Vulnerabilities Assessment

Table 10. T0079 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.	Core
Entry	*Assist in the development of specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.*	
Intermediate	*Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.*	
Advanced	*Review, validate, and/or approve that specifications ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.*	

Table 11. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0019	Knowledge of cryptography and cryptographic key management concepts.	Encryption
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0322	Knowledge of embedded systems.	Infrastructure Design

Table 12. T0083 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Draft statements of preliminary or residual security risks for system operation.	Core
Entry	*Provide input to draft statements of preliminary or residual security risks for system operation.*	
Intermediate	*Draft statements of preliminary or residual security risks for system operation.*	
Advanced	*Review and approve statements of preliminary or residual security risks for system operation.*	

Table 13. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Vulnerabilities Assessment
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).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment

Table 14. T0141 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Maintain information systems assurance and accreditation materials.	Core
Entry	*Maintain a subset of information systems assurance and accreditation materials.*	
Intermediate	*Maintain specific information systems assurance and accreditation materials.*	
Advanced	*Maintain an enterprise-wide portfolio of information systems assurance and accreditation materials.*	

Table 15. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0037	Knowledge of the Security Assessment and Authorization process.	Information Assurance
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management

Table 16. T0150 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.	Core
Entry	*Assist with monitoring and evaluating a system's compliance with information technology (IT) security, resilience, and dependability requirements.*	
Intermediate	*Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.*	
Advanced	*Review and approve the evaluation of a system's compliance with information technology (IT) security, resilience, and dependability requirements.*	

Table 17. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0019	Knowledge of cryptography and cryptographic key management concepts.	Encryption
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.	Information Assurance
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	Vulnerabilities Assessment
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
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).	Vulnerabilities Assessment

KSA ID	Description	Competency
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment

Table 18. T0309 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assess the effectiveness of security controls.	Core
Entry	*Assist in assessing the effectiveness of security controls.*	
Intermediate	*Assess the effectiveness of security controls.*	
Advanced	*Provide guidance/interpretation in assessing the effectiveness of security controls in complex conditions.*	

Table 19. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
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.	Information Assurance
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	Vulnerabilities Assessment
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
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).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment

Table 20. T0177/T0178 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	T0177: Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. T0178: Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Core
Entry	*Assist with performing security reviews*	
Intermediate	*Perform security reviews and identify gaps in security architecture resulting in recommendations.*	
Advanced	*Validate and approve recommendations for inclusion in the risk mitigation strategy and/or develop a risk management plan.*	

Table 21. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
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).	Vulnerabilities Assessment

Table 22. T0181 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Core
Entry	*Assist with performing a risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	
Intermediate	*Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	
Advanced	*Review and approve results from risk analysis and recommend corrective actions to address vulnerabilities whenever an application or system undergoes a major change.*	

Table 23. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0019	Knowledge of cryptography and cryptographic key management concepts.	Encryption
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	Risk Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
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).	Vulnerabilities Assessment

Table 24. T0184 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Core
Entry	*Track security authorization reviews and assurance case development for initial installation of systems and networks.*	
Intermediate	*Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.*	
Advanced	*Review and approve results from security authorization reviews and recommend corrective actions to address gaps in security for initial installation of systems and networks.*	

Table 25. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
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.	Information Assurance
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0037	Knowledge of the Security Assessment and Authorization process.	Information Assurance
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
S0006	Skill in applying confidentiality, integrity, and availability principles.	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	Information Technology Assessment
K0322	Knowledge of embedded systems.	Infrastructure Design

KSA ID	Description	Competency
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation

Table 26. T0244 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Core
Entry	*Assist with verifying application software/network/system security postures are implemented as stated and document deviations.*	
Intermediate	*Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.*	
Advanced	*Review and approve recommended required actions to correct those deviations.*	

Table 27. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0019	Knowledge of cryptography and cryptographic key management concepts.	Encryption
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.	Information Assurance
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	Vulnerabilities Assessment
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

KSA ID	Description	Competency
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).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment