CAREER PATHWAY VULNERABILITY ASSESSMENT ANALYST (541)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 541-VULNERABILITY ASSESSMENT ANALYST

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 541-Vulnerability Assessment Analyst.

Table 1. 541-Vulnerability Assessment Analyst Work Role Overview

NICE Work Role Definition	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
OPM Occupational Series	Personnel performing the 541-Vulnerability Assessment Analyst work role are most commonly aligned to the following Occupational Series: - 2210-Information Technology – 59% - 0080-Security Administration – 15% - 0855-Electronics Engineering – 6% - 1550-Computer Science – 5% - 1801-General Inspection, Investigation, Enforcement, and Compliance Series – 5%
Work Role Pairings	Personnel performing the 541-Vulnerability Assessment Analyst work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 521-Cyber Defense Infrastructure Spt. Spec – 14% - 511-Cyber Defense Analyst – 9% - 531-Cyber Defense Incident Responder – 9% - 461-Systems Security Analyst – 8% - 641-Systems Requirements Planner – 7%
Functional Titles	Personnel performing the 541-Vulnerability Assessment Analyst work role may unofficially or alternatively be called: - Blue Team Technician - Computer Network Defense (CND) Auditor - Ethical Hacker - Information Security Engineer - Network Security Engineer - Penetration Tester - Red Team Technician - Reverse Engineer - Risk Assessor - Risk Assessment Engineer

	- Risk/Vulnerability Specialist / Manager - System / Application Security Tester
Distribution of GS-Levels	Personnel performing the 541-Vulnerability Assessment Analyst work role are most commonly found within the following grades on the General Schedule*. - ☐ GS-4 – redacted** - ☐ GS-7 – redacted** - ☐ GS-8 – redacted** - ☒ GS-9 – 4% - ☒ GS-11 – 11% - ☒ GS-12 – 21% - ☒ GS-13 – 32% - ☒ GS-14 – 13% - ☐ GS-15 – redacted** *19% of all 541s are in non-GS pay plans and excluded from this section **Percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 541-Vulnerability Assessment Analyst work role: - 441-Network Operations Specialist - 451-System Administrator - 461-Systems Security Analyst - 511-Cyber Defense Analyst - 521-Cyber Defense Infrastructure Support Specialist - 531-Cyber Defense Incident Responder - 612-Security Control Assessor - 671-System Testing and Evaluation Specialist
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 541-Vulnerability Assessment Analyst work role. 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: - 612-Security Control Assessor - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 541-Vulnerability Assessment 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* - *751-Cyber Workforce Developer and Manager*

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

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 541-Vulnerability Assessment Analyst work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 541-Vulnerability Assessment Analyst Core Tasks

Task ID	Task	Core or Additional
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	Core
T0138	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.	Core
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	Core
T0188	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Core
T0549	Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).	Core
T0028	Conduct and/or support authorized penetration testing on enterprise network assets.	Additional
T0252	Conduct required reviews as appropriate within environment.	Additional
T0550	Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).	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 541-Vulnerability Assessment Analyst work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 541-Vulnerability Assessment Analyst Core Knowledge, Skills, and Abilities

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity and privacy 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 laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	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
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
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design	Core
K0009	Knowledge of application vulnerabilities.	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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment	Core
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment	Core
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment	Core
S0051	Skill in the use of penetration testing tools and techniques.	Vulnerabilities Assessment	Core
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).	Vulnerabilities Assessment	Core

KSA ID	Description	Competency	Importance to Work Role
S0137	Skill in conducting application vulnerability assessments.	Vulnerabilities Assessment	Core
K0021	Knowledge of data backup and recovery.	Business Continuity	Additional
K0210	Knowledge of data backup and restoration concepts.	Business Continuity	Additional
S0120	Skill in reviewing logs to identify evidence of past intrusions.	Computer Forensics	Additional
K0068	Knowledge of programming language structures and logic.	Computer Languages	Additional
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages	Additional
A0044	Ability to apply programming language structures (e.g., source code review) and logic.	Computer Languages	Additional
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense	Additional
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption	Additional
K0308	Knowledge of cryptology.	Encryption	Additional
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management	Additional
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance	Additional
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Additional
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security	Additional
K0265	Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.	Infrastructure Design	Additional
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Additional
S0171	Skill in performing impact/risk assessments.	Risk Management	Additional
A0120	Ability to share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.	Risk Management	Additional

KSA ID	Description	Competency	Importance to Work Role
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration	Additional
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration	Additional
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation	Additional
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis	Additional
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis	Additional
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis	Additional
K0344	Knowledge of an organization's threat environment.	Threat Analysis	Additional
S0044	Skill in mimicking threat behaviors.	Threat Analysis	Additional
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	Threat Analysis	Additional
S0364	Skill to develop insights about the context of an organization's threat environment	Threat Analysis	Additional
K0206	Knowledge of ethical hacking principles and techniques.	Vulnerabilities Assessment	Additional
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 541-Vulnerability Assessment 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. 541-Vulnerability Assessment Analyst Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Core or Additional
Information Systems/ Network Security	C024	This area contains KSAs that relate to computer languages and their applications to enable a system to perform specific functions.	• Knowledge of cybersecurity and privacy principles. • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). • Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Core
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 network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. • Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability. • Knowledge of computer networking concepts and protocols, and network security methodologies. • Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Core
Threat Analysis	C055	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks.	• Knowledge of an organization's threat environment. • Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.). • Skill in mimicking threat behaviors. • Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). • Skill to develop insights about the context of an organization's threat environment • Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). • Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Core
Vulnerabilities Assessment	C057	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or	• Ability to identify systemic security issues based on the analysis of vulnerability and configuration data. • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Core or Additional
		recommending appropriate mitigation countermeasures.	• Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) • Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.). • Knowledge of application vulnerabilities. • 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). • Knowledge of cyber threats and vulnerabilities. • Skill in conducting application vulnerability assessments. • Knowledge of ethical hacking principles and techniques. • Skill in the use of penetration testing tools and techniques. • Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). • Knowledge of penetration testing principles, tools, and techniques. • Knowledge of specific operational impacts of cybersecurity lapses.	
Computer Languages	C066	This area contains KSAs that relate to computer languages and their applications to enable a system to perform specific functions.	• Ability to apply programming language structures (e.g., source code review) and logic. • Knowledge of programming language structures and logic. • Knowledge of interpreted and compiled computer languages.	Additional
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.	• Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). • Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Additional
Risk Management	C044	This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.	• Ability to share meaningful insights about the context of an organization's threat environment that improve its risk management posture. • Skill in performing impact/risk assessments. • Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 541-Vulnerability Assessment Analyst Suggested Qualifications / Capability Indicators

For indicators of capability for the 541-Vulnerability Assessment Analyst 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 541-Vulnerability Assessment Analyst.

2 APPENDIX: 541-VULNERABILITY ASSESSMENT ANALYST 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.

2.2 541-Vulnerability Assessment Analyst Task Analysis and KSA Mapping

Table 8. T0010 Task Analysis

Proficiency	Task Statement	Importance
As Written	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	Core
Entry	*Become familiar with organization's cyber defense policies, configurations, and regulations and assist with gathering compliance data.*	
Intermediate	*Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.*	
Advanced	*Plan and oversee the implementation of the organization's cyber defense policies, configurations, and its compliance with regulations and organizational directives; highlight and archive decencies for non-compliance remediation.*	

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

KSA ID	Description	Competency
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	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
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
S0171	Skill in performing impact/risk assessments.	Risk Management
A0120	Ability to share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis

KSA ID	Description	Competency
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	Threat Analysis
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0344	Knowledge of an organization's threat environment.	Threat Analysis
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	Threat Analysis
S0364	Skill to develop insights about the context of an organization's threat environment	Threat Analysis
K0009	Knowledge of application vulnerabilities.	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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0206	Knowledge of ethical hacking principles and techniques.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0051	Skill in the use of penetration testing tools and techniques.	Vulnerabilities Assessment
S0137	Skill in conducting application vulnerability assessments.	Vulnerabilities Assessment
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment

Table 10. T0138 Task Analysis

Proficiency	Task Statement	Importance
As Written	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.	Core
Entry	*Apply basic knowledge and assist in the maintenance of deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support compliance of organizational security policies and cyber programs.*	
Intermediate	*Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.*	
Advanced	*Recommend, create, and/or manage deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) ensuring that the deployed toolkit is sufficient to meet the requirements of the organization's audit policies to support cyber defense audit missions.*	

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

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	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
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0265	Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
S0171	Skill in performing impact/risk assessments.	Risk Management
A0120	Ability to share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis

KSA ID	Description	Competency
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
S0044	Skill in mimicking threat behaviors.	Threat Analysis
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	Threat Analysis
S0364	Skill to develop insights about the context of an organization's threat environment	Threat Analysis
K0009	Knowledge of application vulnerabilities.	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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0206	Knowledge of ethical hacking principles and techniques.	Vulnerabilities Assessment
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0051	Skill in the use of penetration testing tools and techniques.	Vulnerabilities Assessment
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).	Vulnerabilities Assessment
S0137	Skill in conducting application vulnerability assessments.	Vulnerabilities Assessment
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment

Table 12. T0142 Task Analysis

Proficiency	Task Statement	Importance
As Written	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	Core
Entry	*Acquire knowledge of basic applicable cyber defense policies and compliance documents related to cyber defense auditing.*	
Intermediate	*Maintain knowledge of and assist with the maintenance and review of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.*	
Advanced	*Develop and advise stakeholders of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.*	

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

KSA ID	Description	Competency
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
A0120	Ability to share meaningful insights about the context of an organization's threat environment that improve its risk management posture.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0344	Knowledge of an organization's threat environment.	Threat Analysis
S0044	Skill in mimicking threat behaviors.	Threat Analysis
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	Threat Analysis
S0364	Skill to develop insights about the context of an organization's threat environment	Threat Analysis
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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0051	Skill in the use of penetration testing tools and techniques.	Vulnerabilities Assessment
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).	Vulnerabilities Assessment
S0137	Skill in conducting application vulnerability assessments.	Vulnerabilities Assessment
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment

Table 14. T0188 Task Analysis

Proficiency	Task Statement	Importance
As Written	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Core
Entry	*Assist with preparing audit reports that identify technical and procedural findings, and provide input on recommended remediation strategies/solutions.*	
Intermediate	*Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.*	
Advanced	*Review audit reports that identify technical and procedural findings, and approve recommended remediation strategies/solutions.*	

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

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	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
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0265	Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
S0171	Skill in performing impact/risk assessments.	Risk Management
A0120	Ability to share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0344	Knowledge of an organization’s threat environment.	Threat Analysis
S0044	Skill in mimicking threat behaviors.	Threat Analysis
S0364	Skill to develop insights about the context of an organization’s threat environment	Threat Analysis

KSA ID	Description	Competency
K0009	Knowledge of application vulnerabilities.	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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0206	Knowledge of ethical hacking principles and techniques.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0051	Skill in the use of penetration testing tools and techniques.	Vulnerabilities Assessment
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).	Vulnerabilities Assessment
S0137	Skill in conducting application vulnerability assessments.	Vulnerabilities Assessment
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment

Table 16. T0549 Task Analysis

Proficiency	Task Statement	Importance
As Written	Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).	Core
Entry	*Assist with routine technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).*	
Intermediate	*Under supervision, perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications)*	
Advanced	*Plan, perform, and/or oversee complex or novel technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).*	

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

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0009	Knowledge of application vulnerabilities.	Vulnerabilities Assessment
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
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
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	Threat Analysis
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	Threat Analysis
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0206	Knowledge of ethical hacking principles and techniques.	Vulnerabilities Assessment

KSA ID	Description	Competency
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	System Administration
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	Vulnerabilities Assessment
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0344	Knowledge of an organization's threat environment.	Threat Analysis
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	Computer Network Defense
S0044	Skill in mimicking threat behaviors.	Threat Analysis
S0051	Skill in the use of penetration testing tools and techniques.	Vulnerabilities Assessment
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).	Threat Analysis
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).	Vulnerabilities Assessment
S0137	Skill in conducting application vulnerability assessments.	Vulnerabilities Assessment
S0171	Skill in performing impact/risk assessments.	Risk Management
S0364	Skill to develop insights about the context of an organization's threat environment	Threat Analysis
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment
A0120	Ability to share meaningful insights about the context of an organization's threat environment that improve its risk management posture.	Risk Management
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance