Carnegie Mellon University
Software Engineering Institute

# Software Engineering Institute (SEI) Adversarial Emulation Testing (AET) Assessor Requirements and Evaluation v1.0

Anne Connell
Gavin Jurecko

March 2021

**CERT Division**


http://www.sei.cmu.edu

# Table of Contents

# Revision History

| Date | Description |
|---|---|
| 3/2/2021 | Adversarial Emulation Testing Assessment Team Requirements and Evaluation |

# 1 Introduction

The Carnegie Mellon University Software Engineering Institute (SEI) is dedicated to fostering a culture of continuous improvement. It sets clear goals and encourages the use of information to assess the degree to which goals are being met.

The SEI Adversarial Emulation Testing (AET) program:

- provides an informed and critical view of the role and value of an assessment;
- articulates how policy is made in the areas of technology, both within the United States and elsewhere; and
- recommends how to approach the capabilities of the technologies that policies are trying to govern.

Many organizations are conducting similar cybersecurity assessments, but their methods and rigor vary. Organizations conducting these assessments may or may not have mature operational guidance, or their assessors might have varying competency and skills. The vulnerability and risk data discovered through adversarial emulation testing may be ingested at an organizational level with the authority to create or update organizational policies. As such, an assessor must have a strong foundation of skills required in penetration testing to lead or participate in an adversarial emulation testing assessment.

## 1.1 Document Purpose

The purpose of this document is to identify the roles in the SEI Adversarial Emulation Testing (AET) Assessment team and to identify the skills and prerequisites needed to complete the qualification process for the assessors to fulfill these roles.

## 1.2 Scope

The scope of this document is to define the assessment team, which includes the roles, requirements for the roles, qualification, and assessor tracking mechanisms for SEI-AET assessors. This ensures that the process and procedures of an SEI-AET engagement are consistently followed, and provides for the standardization of categorizing findings and reporting.

# 2 Assessment Team Roles & Responsibilities

The work of the SEI-AET Assessment Team includes complex duties that combine technical skills and communication skills. There are three assessment team roles: Program Lead (PL), Technical Lead (TL), and Operators (OP). The Operator role is also referred to as the Assessor. In this document we use "Operator." Collectively, these Assessment Team roles are responsible for conducting all tasks that occur during an SEI-AET Assessment, from conducting the Technical Exchange Meeting (TEM) through producing the final SEI-AET Assessment report.

## 2.1 SEI-AET Program Lead (PL)

The role and responsibilities of the SEI-AET Program Lead are to manage the SEI-AET schedule and to ensure that the assessment team member resources are properly vetted, effectively assigned, engaged, and utilized to support stakeholder needs.

## 2.2 SEI-AET Assessment Lead (AL)

The role and responsibilities of the SEI-AET Assessment Lead are to interact as the primary point of contact with the respective stakeholder. The SEI-AET Assessment Lead ensures that services are selected, agreements are signed and gathered, communication plans for stakeholder are disseminated, notifications are sent to third party organizations, and team member support is scheduled. The SEI-AET Assessment Lead confirms that the stakeholder organization's lab manager is made aware of the engagement requirements, and that daily status and final reports are delivered to the stakeholder.

The SEI-AET Assessment Lead:

- participates with the Program Lead in the planning phase of the SEI-AET Assessment activities
- examines (check, inspect, review, observe, study, or analyze) one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence
- leads the Technical Exchange Meeting (TEM) which consists of interviews with individual or group SMEs to facilitate understanding, achieve clarification, or lead to the location of evidence
- communicates and shares information gained during the TEM with the entire assessment team
- participates in the post-execution outbrief to the organization POC and SMEs, to present preliminary observations as a result of the TEM
- drafts the majority of the SEI-AET Assessment reports

## 2.3 SEI-AET Technical Lead (TL)

The role and responsibilities of the SEI-AET Technical Lead (TL) is responsible for leading and facilitating the Technical Exchange Meeting (TEM) that occurs during an SEI-AET Assessment. The TL is responsible for drafting the majority of the SEI-AET Assessment reports. The TL also supports other meetings throughout the assessment and shares information gained during the TEM with the entire Assessment Team.

The SEI-AET Technical Lead:

- works directly with the AL and organization POC to successfully plan and execute the assessment, as well as notify and manage the assessment services
- participates in assessment activities and leads the adversarial emulation testing to ensure the Operator(s) are able to operate efficiently
- leads the scoping section of the Technical Exchange Meeting (TEM) which consists of interviews with individual or group SMEs to complete the Rules of Engagement (ROE) activities, achieve clarification, or lead to the location of evidence
- will apply technical and professional skillsets to lead the Technical Exchange Meeting (TEM)
- communicates and shares information gained during the TEM with the entire assessment team
- participates in the post-execution outbrief to the organization POC and SMEs, to present preliminary observations as a result of the TEM
- identify potential improvements to the target organization security posture that are related to organizational social media system(s) use and interconnections, as well as identifying strengths and weaknesses in incident management capabilities that are applicable to protecting and sustaining the SEI-AET
- drafts the majority of the critical findings of the SEI-AET Assessment reports

The TL is responsible for translating the outcomes of the SEI-AET assessment testing into risks that are understandable to the technical and management-level stakeholders. The TL ensures SEI-AET team members are assigned specific tasks and follow the assessment operational procedures, processes, tools, and activities.

## 2.4 SEI-AET Assessment Team Operators (OP)

The role and responsibilities of SEI-AET Team Operators are to support the Team Lead in any capacity necessary to deliver SEI-AET services and to address stakeholder needs in the context of SEI-AET services.

# 3 Requirements

For an organization to employ the SEI-AET assessment process, the organization must be first made aware of and be educated about the qualification requirements of the SEI-AET team.

Organization may use existing workforce frameworks to help them meet their mission, goals, and objectives such as:

- National Initiative for Cybersecurity Careers & Studies (NICCS) National Initiative for Cybersecurity Education (NICE) blueprint to identify the knowledge, skills, and abilities needed to perform SEI-AET assessment tasks.
- U.S. Department of Defense (DoD) Cyber Workforce Framework (DCWF) to categorize the full spectrum of cyber workforce roles. This framework is defined in DoD 8140, which replaced DoD 8570, an expanded and updated version of DoD8570, and draws on the National Initiative for Cybersecurity Education (NICE) and the DoD Joint Cyberspace Training and Certification Standards (JCT & CS).

For organizations that apply these frameworks, the corresponding mappings are listed in the description of each assessment role. Appendix B contains a complete listing of the NICE Work Roles, Competencies, and Knowledge, Skills and Abilities, as well as the DCWF workforce framework that DoD cybersecurity uses to categorize the full spectrum of cyber workforce roles.

## 3.1 Program Lead

The SEI-AET Program Lead ensures that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions. The Program Lead's primary duties are leading the assessment program implementation and management, communication with organization points of contact, interviews with subject matter experts, and advancing assessment program strategy. The PL will participate with the Assessment Lead and the Technical Lead in the planning phase of the SEI-AET Assessment activities.

### 3.1.1 Role requirements

The PL directs the Assessment Lead, Technical Lead, and Operator on all engagements of the SEI-AET Assessment activities. The PL role requirements are:

- experience in public speaking, giving executive briefings, and communicating with stakeholders
- extensive experience in leading interviews with technical subject matter experts
- experience in leading teams and managing assessments or projects
- an understanding of penetration testing
- knowledge of cybersecurity and privacy principles and organizational requirements
- knowledge of new and emerging information technology and cybersecurity technologies
- skill to apply cybersecurity and privacy principles to organizational requirements
- ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture

- ability to communicate effectively when writing

### 3.1.2 Role qualifications

The PL role qualifications are:

- experience in conducting audits or reviews of technical systems
- experience in performing impact/risk assessments
- knowledge of new and emerging information technology and cybersecurity technologies
- experience in developing insights about the context of an organization's threat environment.
- knowledge of risk/threat assessment processes (e.g., NIST SP 800-30 Rev. 1, NIST SP 800-53A Rev. 4)
- knowledge of the of the Risk Management Framework Assessment Methodology (NIST SP 800-37 Rev. 2, NIST SP 800-53 Rev. 5)
- It is recommended that the candidate for this role holds one or more nationally recognized information security-related certifications, for example:
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information Security Manager (CISM)
  - Certified Information Security Auditor (CISA)
  - Program Lead, Cybersecurity (Applications Security/RMF)

### 3.1.3 Role mappings

- NICE IT Program Manager, Cybersecurity Policy Vulnerability Analyst
- DCFW IT Program Auditor, IT Program Manager, Auditor, Cyber Operations Planner, Partner Integration Planner

## 3.2 Assessment Lead

The SEI-AET Assessment Lead is responsible for the coordination and leadership of the SEI-AET assessment. The AL is responsible for the overall assessment execution and success. As the lead, this role is responsible for ensuring that all assessment deliverables are completed according to quality standards and to the planned scheduled.

The AL is the primary assessment team point of contact (POC) and main interface for the organization being assessed. As the main assessment POC, the AL works directly with the organization POC to successfully plan and execute the assessment. The AL participates in assessment activities, including the Technical Exchange Meetings (TEM) and penetration testing when possible, to ensure the Technical Lead and Operator are able to operate efficiently.

The AL is responsible for translating the outcomes of the assessment into risks that are understandable to the technical and management-level stakeholders. The AL ensures that SEI-AET team members are familiar with and follow the assessment operational procedures, processes, tools, and activities.

### 3.2.1 Role Requirements

The Assessment Lead directs the Technical Lead and Operator in all phases of the SEI-AET Assessment activities. The AL role requirements are:

- experience in public speaking, giving executive briefings, and communicating with stakeholders
- extensive experience in leading interviews with technical subject matter experts
- experience in leading teams and managing assessments or projects
- experience in penetration testing
- knowledge of cybersecurity and privacy principles and organizational requirements
- knowledge of new and emerging information technology and cybersecurity technologies
- skill to apply cybersecurity and privacy principles to organizational requirements
- ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture
- ability to communicate effectively when writing

### 3.2.2 Role qualifications

The AL role qualifications are:

- skill in conducting audits or reviews of technical systems
- skill in performing impact/risk assessments
- knowledge of new and emerging information technology and cybersecurity technologies
- skill to develop insights about the context of an organization's threat environment.
- knowledge of risk/threat assessment processes (e.g., NIST SP 800-30 Rev. 1, NIST SP 800-53A Rev. 4)
- knowledge of the of the Risk Management Framework Assessment Methodology (NIST SP 800-37 Rev. 2, NIST SP 800-53 Rev. 5)

- It is recommended that the candidate for this role holds one or more nationally recognized information security-related certifications, for example:
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information Security Manager (CISM)
  - Certified Information Security Auditor (CISA)

### 3.2.3 Role mappings

- NICE IT Program Manager, Cybersecurity Policy Vulnerability Analyst, Information Assurance Workforce Improvement Program, Vulnerability Assessment Analyst
- DCFW IT Program Auditor, IT Program Manager, , Cyber Operations Planner, Vulnerability Assessment and Management, COMSEC Manager, Information Systems Security Manager

## 3.3 Technical Lead

The SEI-AET Assessment team role for a Technical Lead is responsible for leading and facilitating the Technical Exchange Meeting that occurs during an SEI-AET Assessment. The TL is responsible for drafting the majority of the SEI-AET Assessment reports. The TL also supports other meetings throughout the assessment, and shares information gained during the TEM with the entire Assessment Team.

The SEI-AET Technical Lead will apply technical and professional skillsets to lead the TEM, to help the assessment team to gain an understanding of the cybersecurity state of the organization, identify risks, and provide recommendations. These include the identification of potential improvements to the target organization security posture that are related to system design and interconnections, as well as identification of strengths and weaknesses in incident management capabilities that are applicable to protecting and sustaining the SEI-AET.

The TL works directly with the AL and organization POC to successfully plan and execute the assessment, notify, and manage the assessment services. The TL participates in assessment activities and leads the adversarial emulation testing to ensure that the Operator(s) are able to work efficiently.

The TL is responsible for translating the outcomes of the assessment services into risks that are understandable to the technical and management-level stakeholders. The TL ensures that SEI-AET team members are assigned specific tasks and follow the assessment operational procedures, processes, tools, and activities.

### 3.3.1 Role requirements

The Technical Lead directs the Operators in all phases of the SEI-AET Assessment activities. The TL role requirements are:

- experience and familiarity with the assessment methods defined in NIST SP 800-30 Rev. 1 and NIST SP 800-53A Rev. 5 (interview, examine, and test).
- experience and familiarity with risk/threat assessment processes (e.g., NIST SP 800-30 Rev. 1, NIST SP 800-53A Rev. 5).
- experience and familiarity with the Risk Management Framework Assessment Methodology (NIST SP 800-37 Rev. 2, NIST SP 800-53 Rev. 5).

- skill in performing impact/risk assessments.
- experience and familiarity with new and emerging penetration testing technologies.
- skill to develop insights about the context of an organization's threat environment.
- experience in drafting written reports
- extensive experience in reviewing and examining data and information that supports cybersecurity assessments

### 3.3.2 Role qualifications

The TL role qualifications are:

- ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture
- ability to communicate effectively when writing
- knowledge of cybersecurity and privacy principles and organizational requirements
- experience using new and emerging information technology and cybersecurity technologies
- skill to apply cybersecurity and privacy principles to organizational requirements
- It is recommended that the candidate for this role holds one or more nationally recognized information system auditing certifications, for example:
  - Certified Information Systems Auditor (CISA)
  - Certified in Risk and Information Systems Control (CRISC)
  - Certified Information Systems Security Professional (CISSP)
  - CISSP Information Systems Security Architecture Professional (CISSP-ISSAP)
  - CompTIA PenTest+
  - Offensive Security Certified Professional (OSCP)
  - Offensive Security Certified Expert (OSCE)
  - SANS GIAC Defensible Security Architecture (GDSA)
  - SANS GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
  - SANS GIAC Penetration Tester (GPEN)

### 3.3.3 Role mappings

- NICE Security Control Assessor, Cybersecurity Policy Vulnerability Analyst , Vulnerability Assessment Analyst
- DCFW IT Program Auditor, IT Program Manager, Cyber Operations Planner, Vulnerability Assessment and Management, Auditor

## 3.4 Operator

The SEI-AET Assessment team Operator Role leads the penetration test part of the assessment. They are responsible for developing the testing results appendix of the report. They may also contribute to other portions of the assessment report. As needed, the OP supports the Technical Exchange Meeting or other meetings.

### 3.4.1 Role Requirements

The Operator executes the SEI-AET Assessment activities assigned by the TL. The OP role requirements are:

- experience and familiarity with the assessment methods defined in NIST SP 800-30 Rev. 1 and NIST SP 800-53A Rev. 4 (interview, examine, and test)
- experience in drafting written reports
- extensive experience in reviewing and examining data and information that supports cybersecurity assessments
- experience in pen testing fundamentals
- experience in Kali Linux and its toolsets, including Metasploit
- experience in pen testing tools including scanners like Nessus and Nmap
- a minimum of three years of the following experience:
  - performing authorized pen testing on enterprise networks;
  - gaining access to targeted networks;
  - applying expertise to enable new exploitation and maintaining access;
  - obeying appropriate laws and regulations;
  - providing infrastructure analysis;
  - performing analysis of physical and logical digital technologies;
  - conducting in-depth target and technical analysis;
  - creating exploitation strategies for identified vulnerabilities;
  - monitoring target networks; and
  - profiling network users or system administrators and their activities

### 3.4.2 Role qualifications

The OP role qualifications are:

- one or more nationally recognized information system auditing certifications, for example
  - Certified Information Systems Security Professional (CISSP)
  - CompTIA PenTest+
  - Offensive Security Certified Professional (OSCP)
  - Offensive Security Certified Expert (OSCE)
  - SANS GIAC Defensible Security Architecture (GDSA)
  - SANS GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
  - SANS GIAC Penetration Tester (GPEN)

### 3.4.3 Role mappings

- NICE Security Control Assessor, Cybersecurity Policy Vulnerability Analyst , Vulnerability Assessment Analyst
- DCFW IT Program Auditor, IT Program Manager, Cyber Operations Planner, Vulnerability Assessment and Management, Auditor

## 3.5 Assessment Team Scope

The SEI-AET assessment candidate requirements exist to ensure that the Stakeholder Organization trusts the SEI-AET team's assessment of the organization's network, data, and facilities. The SEI-AET assessment team has the following responsibilities:

- Perform scoped assessments on internal- and external-facing systems.
- Perform threat emulation activities and network scanning to identify vulnerabilities to achieve the SEI-AET's program mission and act as a source for innovation within the cybersecurity industry.
- Assist the Stakeholder Organization as an SEI-AET program contact throughout the engagement.
- Report all critical findings immediately to the Stakeholder Organization's primary point of contact (POC) and maintain consistent contact with the Stakeholder Organization throughout the engagement.
- Work collaboratively with internal and external stakeholders (cybersecurity consultants, project managers, service managers, development teams, technical subject-matter experts, vendors) to deliver high quality assessments.
- Work with the Stakeholder Organization to ensure that identifying gaps, reporting findings, and performing tasks remain within the scope of the engagement.

The SEI-AET team will be limited to the scope identified in the Rules of Engagement (ROE) with the Stakeholder Organization, even if the test team identifies access to other networks. The scope can only change with approval of the Stakeholder Organization POC and a signed revision of the ROE to validate the request.

The work of the SEI-AET Assessment Technical Lead includes complex duties combining technical skills and communication skills.

# 4 Evaluation

Individuals must have the prerequisite knowledge necessary to successfully fulfill their role as part of an assessment. To evaluate this assumption all assessors, referred to as assessor candidates until their qualifications are confirmed, will take a Candidate Technical Evaluation (CTE). The assessor candidate will qualify for the role of AL, TL, or OP based on defined experience and skills. This common baseline can assist in educating stakeholders interested in establishing an internal SEI-AET team.

## 4.1 Assessor Evaluation

The methodology and standards defined by the SEI-AET program are meant for use either as a guideline for organizations looking to stand up a new assessment capability or to help organizations mature their existing capabilities and meet SEI-AET operational standards.

The SEI-AET program is designed to verify that:

- SEI-AET Assessors have the minimum skills required to perform an assessment
- the participant understands the importance of policies and procedures that support and foster a mature and responsible team culture
- the participant has a clear understanding of the expectations, guidelines, and methodologies of the SEI-AET program
- the participant understands SEI-AET reporting and documentation standards

The SEI-AET program helps standardize the way impact-based assessments are conducted throughout networks. In addition, qualified SEI-AET assessors team requirements are such that each member of the SEI-AET Assessment team already possesses skills necessary to complete the assessment process. The Assessment team consists of an Assessment Lead, a Technical Lead, and an Operator. Individuals must have the prerequisite knowledge necessary to successfully fulfill their role as part of an assessment. To evaluate this assumption all candidate assessors will take a Candidate Technical Evaluation (CTE). The candidate will qualify for the role of AL, TL or OP based on defined experience and skills and successful completion of the CTE.

The CTE ensures that all assessors have the fundamental skillset to both understand the SEI-AET processes and provide a quality assessment. The Operator must demonstrate penetration testing technical skills, such as enumeration, exploitation, privilege escalation, and pivoting within a network. Like other assessment courses, completion of the CTE is a requirement for the all candidate assessors prior to observing or conducting an SEI-AET assessment.

The candidate assessor completes the evaluation individually. Results are reported to the candidate assessor and to the SEI-AET Program Lead. The CTE is not an official certification, but a process developed to be used to demonstrate a candidate assessors knowledge.

## 4.2 Assessor Technical Evaluation Process

Before an assessor participates on an SEI-AET assessment, they must verify their ability to perform an assessment role. For a Technical Lead or Operator to participate on an assessment engagement they

must first substantiate their qualifications by submitting to the SEI-AET Candidate Technical Evaluation. During the evaluation, the candidate connects to the test network using the instructions provided by the SEI-AET Evaluation Team. The assessment candidate is required to scan, enumerate, and compromise as many systems as possible within the testing environment. For each compromised system, the assessment candidate must demonstrate proof-of-compromise, e.g., modifying `local.txt` or `proof.txt` on the compromised user's desktop. By the completion of the SEI-AET CTE, candidate assessors must demonstrate pen testing, and write a report that identifies technical requirement gaps.

Assessment candidates learn their results—and whether they have passed the preliminary skill evaluation—after they submit their quiz responses manually, and score each individual system using the buttons on the dashboard.

# Appendix A: Abbreviations and Acronyms

**AET**
Adversarial Emulation Testing

**C2**
Command and Control

**CDE**
Cardholder Data Environment

**HIPAA**
Health Insurance Portability and Accountability Act of 1996

**HVA**
High Value Asset

**IP**
Internet Protocol

**NIST**
National Institute of Standards and Technology

**OSSA**
Operating System Security Assessment

**PCI DSS**
Payment Card Industry Data Security Standard

**PII**
Personally Identifiable Information

**POC**
Point of Contact

**ROE**
Rules of Engagement

**SOCTPOC**
Technical Point of Contact

**TTP**
Tactics, Techniques, and Procedures

**WAP**
Wireless Access Point

# Appendix B: Qualification Requirements Framework

## NICE Framework

The SEI-AET program is based on the recognition that, in order to best meet its mission, goals, and objectives, it should consider the National Initiative for Cybersecurity Careers & Studies (NICCS) National Initiative for Cybersecurity Education (NICE) blueprint to identify the knowledge, skills, and abilities (KSAs) needed to perform SEI-AET assessment tasks.

The NICE Framework is a methodology to categorize, organize, and describe cybersecurity work into Work Roles, Tasks, and Knowledge. It provides a common language to speak about cyber roles and jobs, and can be referenced by those who wish to define professional requirements in cybersecurity.

NICE Work Roles, Competencies, and KSAs

| | | | **NICE Work Role** | | | |
|---|---|---|---|---|---|---|
| Competency | KSA or Task ID | KSA / Task Description | IT Program Auditor (OV-PMA-005) | Vulnerability Assessment Analyst (PR-VAM-001) | Security Architect (SP-ARC-002) | Security Control Assessor (SP-RSK-002) |
| | **Knowledge** | | | | | |
| Infrastructure Design | K0001 | Knowledge of computer networking concepts and protocols, and network security methodologies. | X | X | X | X |
| Risk Management | K0002 | Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). | X | X | X | X |
| Legal, Government, and Jurisprudence | K0003 | Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. | X | X | X | X |
| Information Systems/Network Security | K0004 | Knowledge of cybersecurity and privacy principles. | x | X | X | X |
| Vulnerabilities Assessment | K0005 | Knowledge of cyber threats and vulnerabilities. | X | X | X | X |
| Vulnerabilities Assessment | K0006 | Knowledge of specific operational impacts of cybersecurity lapses. | X | X | X | X |
| Data Analysis | K0043 | Knowledge of industry-standard and organizationally accepted analysis principles and methods. | X | | X | |
| Information Assurance | K0044 | Knowledge of cybersecurity and privacy principles and organizational requirements. | | X | X | |
| Enterprise Architecture | K0047 | Knowledge of information technology (IT) architectural concepts and frameworks. | X | | | |
| Risk Management | K0048 | Knowledge of Risk Management Framework (RMF) requirements. | X | | | X |

| NICE Work Roles, Competencies, and KSAs | | | | | | |
|---|---|---|---|---|---|---|
| | | | **NICE Work Role** | | | |
| Competency | KSA or Task ID | KSA / Task Description | IT Program Auditor (OV-PMA-005) | Vulnerability Assessment Analyst (PR-VAM-001) | Security Architect (SP-ARC-002) | Security Control Assessor (SP-RSK-002) |
| Technology Awareness | K0059 | Knowledge of new and emerging information technology (IT) and cybersecurity technologies. | | | X | X |
| Risk Management | K0165 | Knowledge of risk threat assessment. | X | | | |
| | **Skill** | | | | | |
| Information Technology Assessment | S0085 | Skill in conducting audits or reviews of technical systems. | X | | | |
| Risk Management | S0171 | Skill in performing impact/risk assessments. | | X | | X |
| Threat Analysis | S0364 | Skill to develop insights about the context of an organization's threat environment. | | X | | |
| Information Assurance | S0367 | Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | | X | X | X |
| | **Ability** | | | | | |
| Vulnerabilities Assessment | A0001 | Ability to identify systemic security issues based on the analysis of vulnerability and configuration data. | | X | | X |
| Enterprise Architecture | A0008 | Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture. | | | X | |
| Vulnerabilities Assessment | A0015 | Ability to conduct vulnerability scans and recognize vulnerabilities in security systems. | | | X | |
| Risk Management | A0120 | Ability to share meaningful insights about the context of an organization's threat environment that improve its risk management posture. | | X | | |
| | **Task** | | | | | |
| | T0188 | Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. | | X | | |

Additionally, the Department of Defense (DoD) Directive 8570 was issued in 2005 to identify, tag, track and manage the information assurance, or cybersecurity, workforce. It also established a manual that includes an enterprise-wide baseline IT certification requirement to validate the knowledge, skills, and abilities of people working in cybersecurity roles.

# Error! Reference source not found.**KSAs Mapping to SEI-AET Roles**

| **Common Set of KSAs from NICE for all SEI-AET roles** | |
|---|---|
| K0001 | Knowledge of computer networking concepts and protocols, and network security methodologies. |
| K0002 | Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). |
| K0003 | Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. |
| K0004 | Knowledge of cybersecurity and privacy principles. |
| K0005 | Knowledge of cyber threats and vulnerabilities. |
| K0006 | Knowledge of specific operational impacts of cybersecurity lapses. |
| K0007 | Knowledge of authentication, authorization, and access control methods. |
| K0013 | Knowledge of cyber defense and vulnerability assessment tools and their capabilities. |
| K0043 | Knowledge of industry-standard and organizationally accepted analysis principles and methods. |
| K0047 | Knowledge of information technology (IT) architectural concepts and frameworks. |
| K0048 | Knowledge of Risk Management Framework (RMF) requirements. |
| K0154 | Knowledge of supply chain risk management standards, processes, and practices. |
| K0162 | Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). |
| K0165 | Knowledge of risk/threat assessment. |
| K0267 | Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures. |
| S0147 | Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). |
| A0013 | Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means. |
| A0106 | Ability to think critically. |