CYBER RESILIENCE ASSESSMENT EVALUATION AND STANDARDIZATION (AES)

PROGRAM OVERVIEW

CYBER RESILIENCE

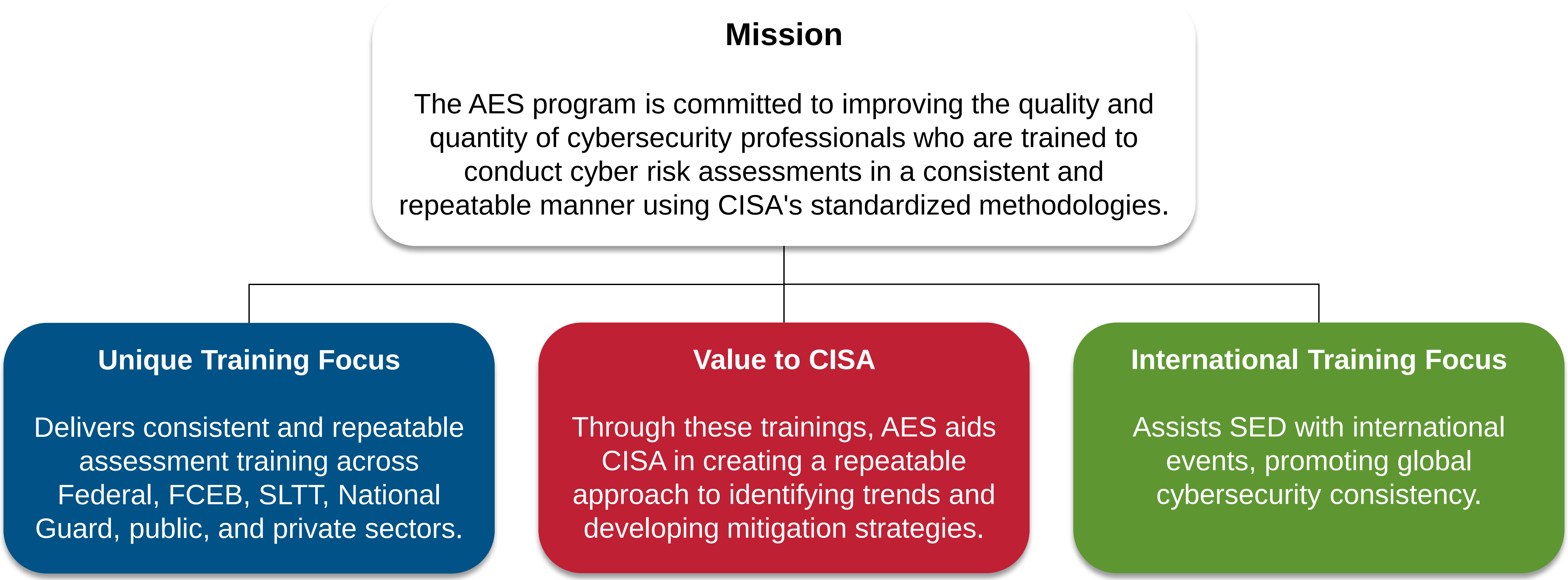
Cyber Resilience Branch
February 7, 2025

Table of Contents:

1. AES Program
2. AES Training Process
3. AES CPG 2.0 Overview
4. AES SSG Overview
5. AES CRR EDM Overview
6. AES CSET Overview
7. AES HVA 3.0 Overview
8. AES RVA Overview
9. AES VADR Overview
10. AES Course Development

AES Program

AES Mission



Mission

The AES program is committed to improving the quality and quantity of cybersecurity professionals who are trained to conduct cyber risk assessments in a consistent and repeatable manner using CISA's standardized methodologies.

Unique Training Focus

Delivers consistent and repeatable assessment training across Federal, FCEB, SLTT, National Guard, public, and private sectors.

Value to CISA

Through these trainings, AES aids CISA in creating a repeatable approach to identifying trends and developing mitigation strategies.

International Training Focus

Assists SED with international events, promoting global cybersecurity consistency.

6 U.S.C. 652(c)(11) AES supports education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security.

Key Stakeholders & Students

Authorized under the **Cybersecurity and Infrastructure Security Agency Act of 2018**, AES provides training to Federal and non-Federal entities to bolster cybersecurity resilience.

Support for IOD/CSAs

AES is the sole resource supporting IOD/CSAs and their stakeholders.

1

Support for Non-Tier 1 HVA

AES is the only supporting resource for the non-Tier 1 HVA communities in meeting their required three-year OMB mandate.

2

Training for Federal Entities

AES is the only assessment training resource for Federal Civilian Executive Branch (FCEB), Federal Department and Agencies (D/A), National Guard, State, Local, Tribal, & Territorial Governments (SLTT), and Critical Infrastructure (CI).

3

Partnering with Public & Private

AES is authorized to train all domestic groups, including contractors and vendors.

4

Key Stakeholders

- EA
- OR
- OCC
- CPG
- OCIO
- JCDC
- OCPO
- Insights
- ASE/RVA
- HVA PMO
- GSA/HAC SIN
- National Guard
- SED International

AES Training Courses

Cyber Performance Goals (CPGs) 2.0

Est. Completion Time: 3 hours

Evaluate whether a minimum baseline of cybersecurity technologies and practices are implemented in Information Technology (IT) and Operational Technology (OT) environments in small- and medium-sized organizations.

Cyber Resilience Review (CRR)

Est. Completion Time: 4-5 days

Conduct an interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices.

External Dependency Management (EDM)

Est. Completion Time: 4-5 days

Conduct an interview-based assessment to evaluate an organization's management of external dependencies.

High Value Asset (HVA) 3.0

Est. Completion Time: 4-5 days

Assess the HVA security architecture to identify technical concerns that could expose the organization to risk.

Risk & Vulnerability Assessment (RVA)

Est. Completion Time: 4-5 days

Collect data through on-site assessments, then combine with national threat and vulnerability information to provide an organization with actionable remediation recommendations prioritized by risk.

Validated Architecture Design Review (VADR)

Est. Completion Time: 4-5 days

Review architecture and design, system configuration, and log files, then analyze network traffic to develop a detailed and sophisticated representation and analysis of the communications, flows, and relationships between devices & identify anomalous and potentially suspicious communication flows.

All AES courses will now be delivered virtually via CISA Learning and must be completed within a 45-day window

For additional information about these assessments, visit
https://www.cisa.gov/resources-tools/programs/assessment-evaluation-and-standardization-program

AES Additional Trainings

ReadySetCyber Guide

Est. Completion Time: Self-Paced

ReadySetCyber simplifies cyber risk management for organizations of all sizes by offering a streamlined, user-friendly guide. It provides practical guidance, baseline assessments, and access to regional CISA cybersecurity advisors, empowering users to assess their cybersecurity posture, implement effective mitigation strategies, and enhance digital security.

Sector-Specific Goals

Est. Completion Time: TBD

Evaluate whether additional, sector-specific cybersecurity technologies and practices beyond the Cross-Sector CPGs are implemented in information technology (IT) and operational technology (OT) environments in organizations aligned to the specific Critical Infrastructure (CI) sectors.

.

Cybersecurity Evaluation Tool (CSET)

Est. Completion Time: 2 hours

CISA's Cyber Security Evaluation Tool (CSET) is a robust platform for assessing and improving cybersecurity posture. This course provides practical guidance on using CSET, covering interface navigation, assessment question sets, and alignment with cybersecurity standards. Participants will gain hands-on experience to enhance resilience and compliance through effective use of CSET's features.

All AES courses will now be delivered virtually via CISA Learning and must be completed within a 45-day window

For additional information about these assessments, visit
https://www.cisa.gov/resources-tools/programs/assessment-evaluation-and-standardization-program

AES Assessment Roles

Assessment Lead (AL)

- Serves as primary assessment team POC
- Leads the assessment team
- Manages the overall assessment execution
- Debriefs and delivers the assessment report
- Role in CPG, SSG, CRR, EDM, HVA, and VADR assessments

Technical Lead (TL)

- Responsible for overall assessment execution
- Leads the Technical Exchange Meeting (TEM)
- Writes majority of the assessment report
- Supports meetings throughout the assessment
- Role in HVA assessments

Operator (OP)

- Leads the Penetration Test
- Responsible for the testing results appendix of the assessment report; contributes to other portions
- Supports meetings throughout the assessment
- Must pass an additional pre-course exam (OST) for acceptance into the course
- Role in RVA assessments

Sector-Specific Subject Matter Expert (S-SME)

- Requires a minimum of 5 years’ OT experience in security operational technology of a specific sector
- Includes oil and gas, electric, water, chemical, manufacturing industries in an operations environment.
- Role in VADR assessments

Prerequisites for All Assessor Roles

The minimum skills for an applicant

- Knowledge of cybersecurity, privacy principles, and their respective organizational requirements including control systems, networks, risk management, incident management, situational awareness, information assurance, and access control

- Ability to express technical and non-technical information, both verbal and written to leadership and staff to ensure proper IT operations

- Experience and skill presenting complex technical issues to a wide audience with varying levels of technical experience

- Experience using a variety of frameworks (i.e., NIST CSF/RMF, COBIT, NIST 800 Series, ISO/IEC27001, CERT Resilience Management Model (RMM)) to assist organizations in evaluating their security programs

Recommended Certifications for All Assessor Roles

AES does not require, but recommends that applicants hold one or more nationally recognized information systems or cybersecurity certifications, particularly for **intermediate** & **advanced courses** (CRR, EDM, HVA, RVA, & VADR)

- GIAC Certified Penetration Tester (GPEN)
- Offensive Security Certified Expert (OSCE)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- GIAC Defensible Security Architecture (GDSA)
- Offensive Security Certified Professional (OSCP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Systems Security Professional (CISSP)
- CISSP Information Systems Security Architecture Professional (CISSP-ISSAP)

Prerequisites for AES HVA/RVA Operator Role

Minimum Applicant Skills	• Knowledge of pen testing fundamentals • Knowledge of Kali Linux and its toolsets, including Metasploit • Knowledge of pen testing tools including scanners like Nessus and Nmap
Minimum 3 yrs 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 • Profiling network users or system administrators and their activities

AES TRAINING PROCESS

AES Training Process Steps

Prerequisites

Step 01 AES Overview

Step 02 Course Registration

Step 03 Candidate Evaluation

Step 3A Operator Skills Test

Courses

Step 04 eLearning Courses

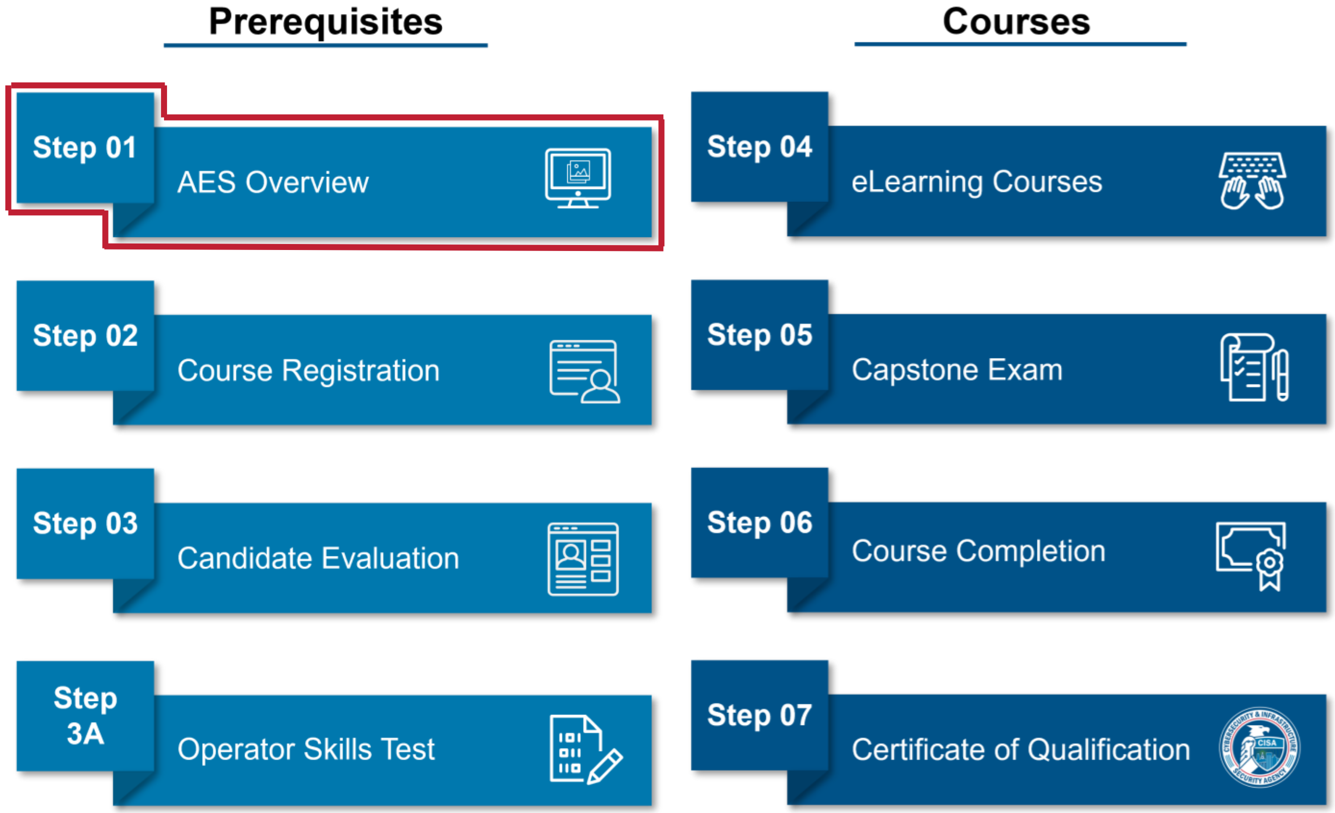
Step 05 Capstone Exam

Step 06 Course Completion

Step 07 Certificate of Qualification

Step 1: AES Overview

- Watch the following video overview of the AES process, roles, & requirements for successful course completion



Prerequisites

- Step 01 AES Overview
- Step 02 Course Registration
- Step 03 Candidate Evaluation
- Step 3A Operator Skills Test

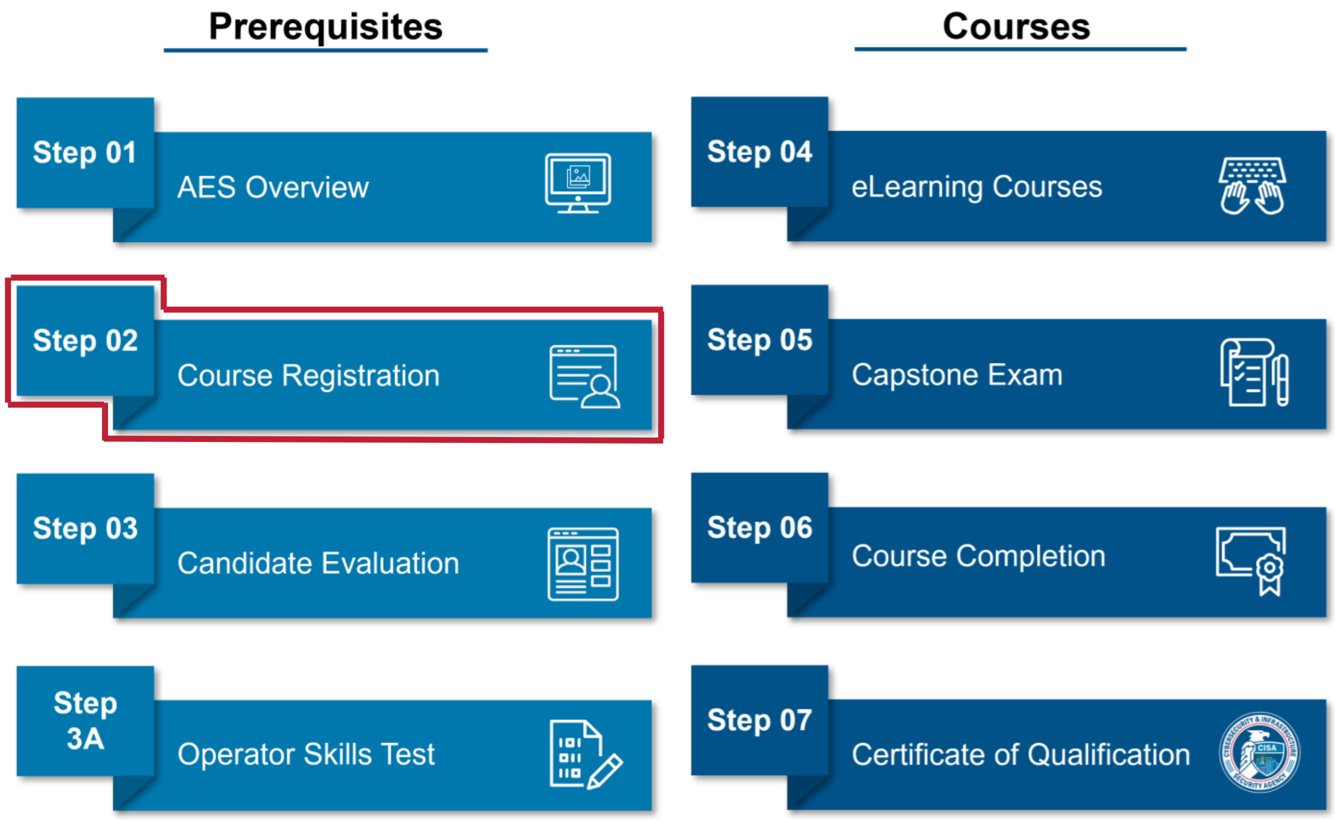
Courses

- Step 04 eLearning Courses
- Step 05 Capstone Exam
- Step 06 Course Completion
- Step 07 Certificate of Qualification

Step 2: Course Registration

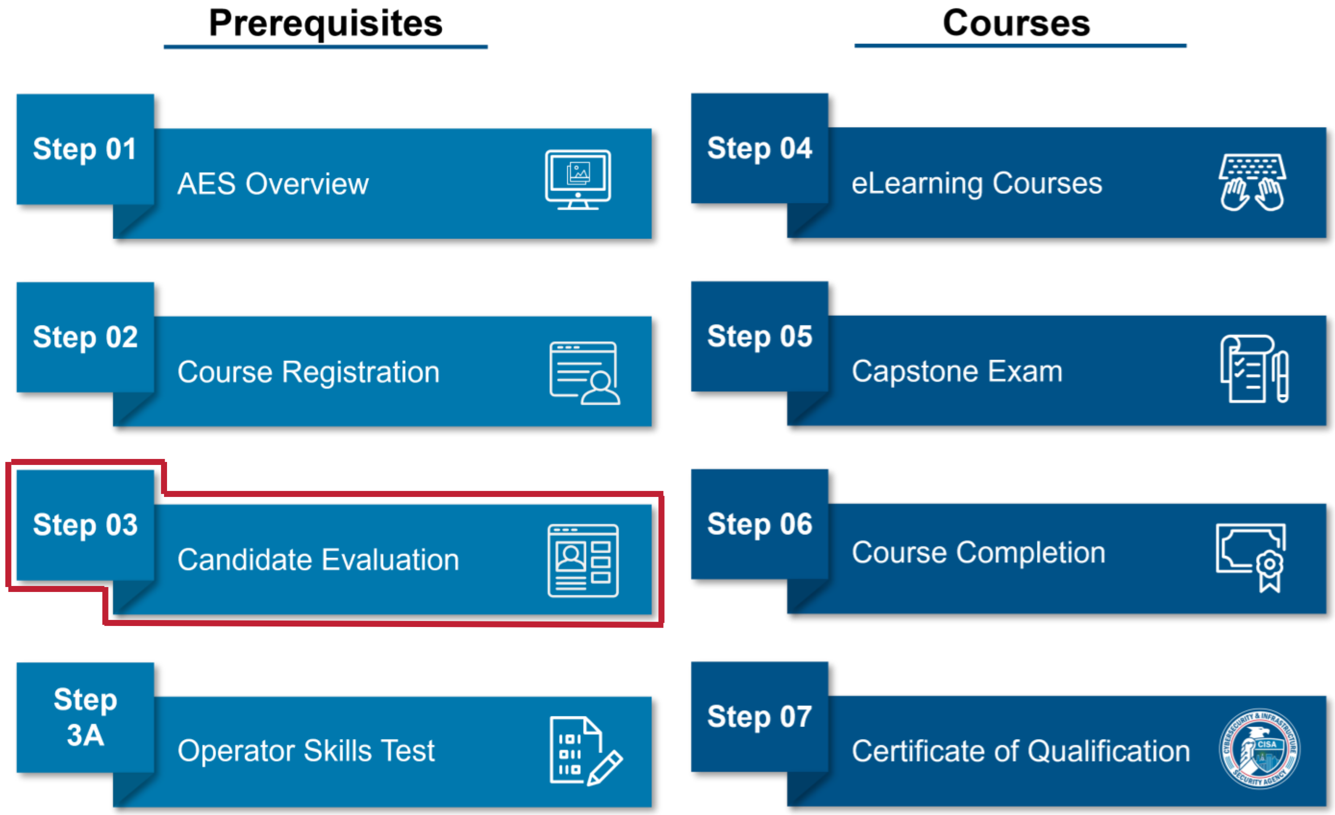
Participants

- Self-register in the CISA Learning portal
- Have access to AES prerequisites and course materials
- Enter and update all profile details, including immediate supervisor or department POC, associated or affiliated Highly Adaptive Cybersecurity Services (HACS) vendor, and critical infrastructure sector



Step 3: Prerequisite Candidate Evaluation

- Confirmation that all applicants have a baseline cybersecurity knowledge to be successful in the course
- Candidates must read and acknowledge AES Rules of Behavior to proceed to the CE exam
- After passing the CE Exam, students will be required to complete the Cyber Performance Goals (CPG) 2.0 course
- Individual administration, online, machine-scored questions
- Passing score of 70% or above required to take the course. Limited to three attempts



Prerequisites

Step 01 AES Overview

Step 02 Course Registration

Step 03 Candidate Evaluation

Step 3A Operator Skills Test

Courses

Step 04 eLearning Courses

Step 05 Capstone Exam

Step 06 Course Completion

Step 07 Certificate of Qualification

CYBERSECURITY
PERFORMANCE
GOALS

AES CPG 2.0 OVERVIEW

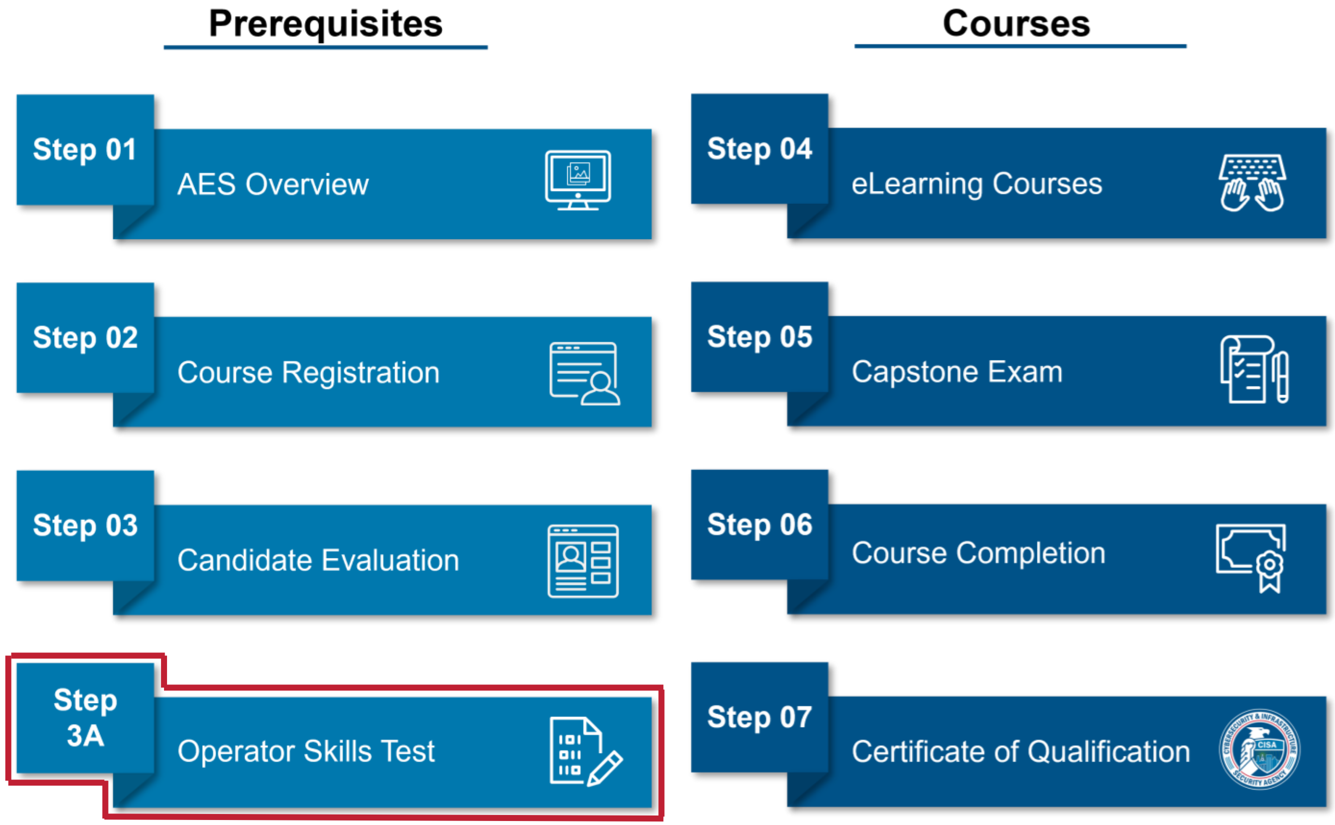
CPG 2.0 Assessment Overview

- **Purpose:** Evaluate whether a minimum baseline of cybersecurity technologies and practices are implemented in information technology (IT) and operational technology (OT) environments in small- and medium-sized organizations
- The Cross-sector Cybersecurity Performance Goals (CPG) training course is designed to empower students to facilitate a CPG assessment using the Cyber Security Evaluation Tool (CSET). Students will use CSET to track responses, conduct posture analysis, and generate a report
- The CPGs are a prioritized subset of information technology (IT) and operational technology (OT) cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques
- The goals were informed by existing cybersecurity frameworks and guidance, as well as by real-world threats and adversary tactics, techniques, and procedures (TTPs) CISA and its government and industry partners observed

For additional information, visit
https://www.cisa.gov/resources-tools/training/cybersecurity-performance-goals-cpg-assessment-training

Step 3A: Operator Skills Test – HVA & RVA

- A lab and quiz designed to assess penetration testing skills. This is an additional prerequisite evaluation that is mandatory for all assessors intending to serve as RVA/HVA operators.
- Additional prerequisite evaluation required for all assessors who will be RVA operators
- Individual, timed evaluation
  - Limited to three attempts in a 24-hour period



Prerequisites

Step 01 AES Overview

Step 02 Course Registration

Step 03 Candidate Evaluation

Step 3A Operator Skills Test

Courses

Step 04 eLearning Courses

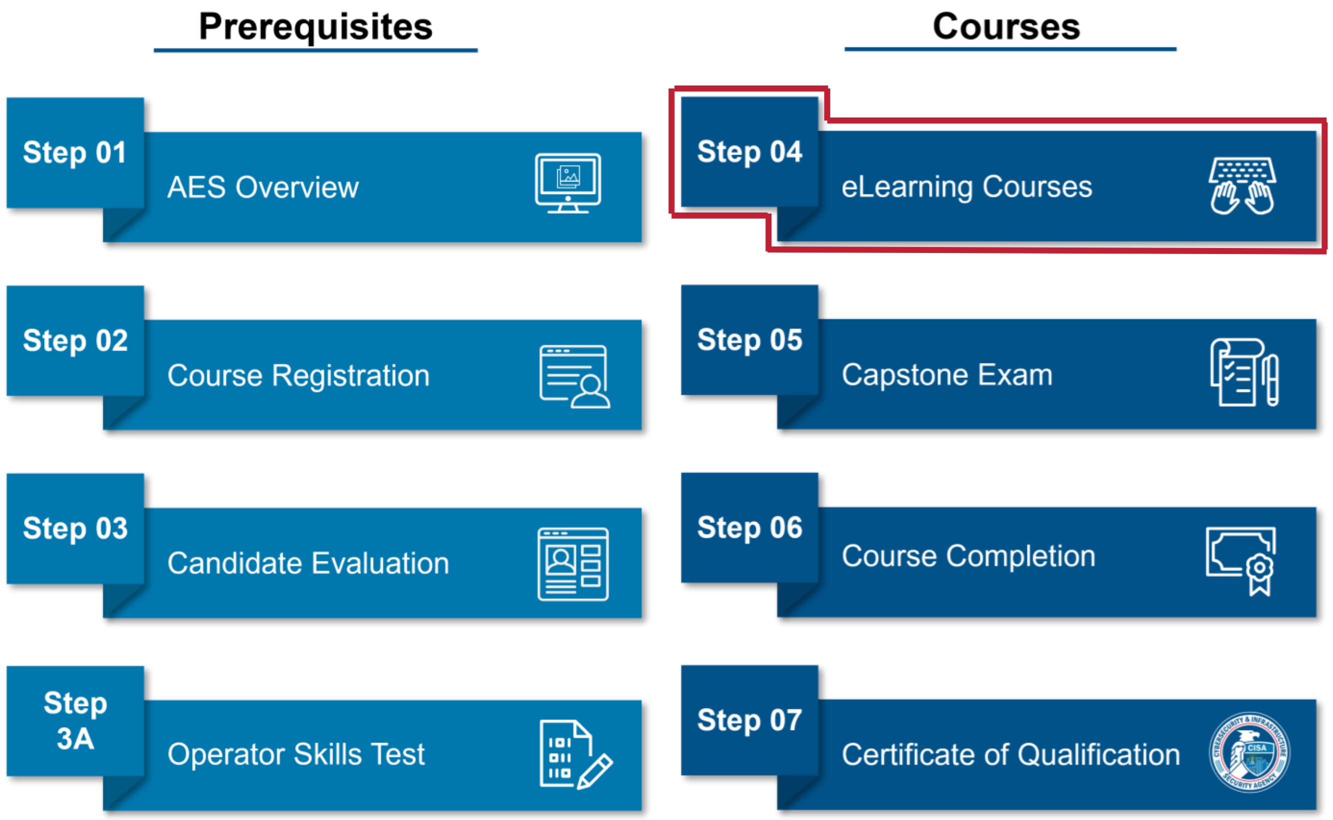
Step 05 Capstone Exam

Step 06 Course Completion

Step 07 Certificate of Qualification

Step 4: eLearning Courses

- Courses are estimated to take 4-5 days to complete
- Exercises allow students to practice assessment activities
- eLearning Courses delivered through CISA Learning
- Class attendance is monitored



Prerequisites

Step 01 AES Overview

Step 02 Course Registration

Step 03 Candidate Evaluation

Step 3A Operator Skills Test

Courses

Step 04 eLearning Courses

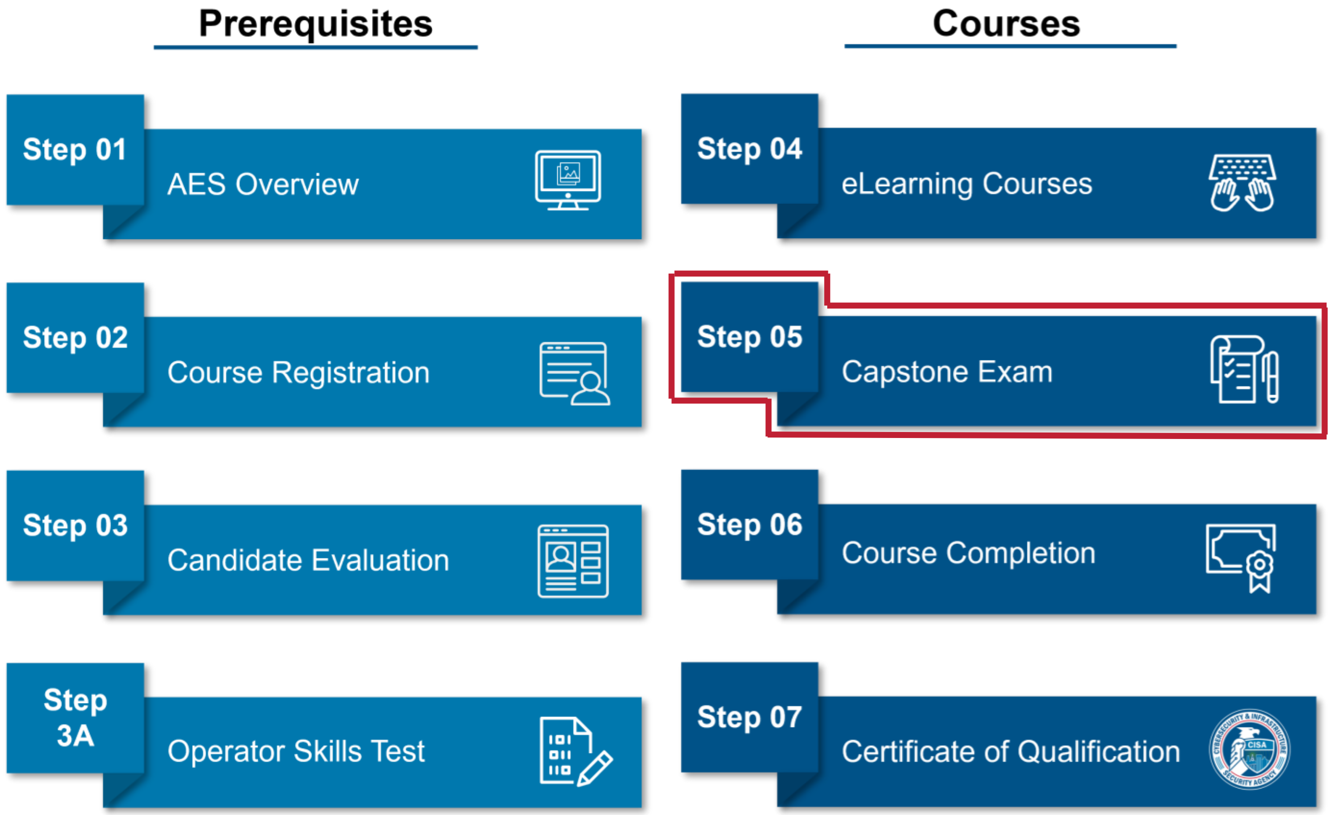
Step 05 Capstone Exam

Step 06 Course Completion

Step 07 Certificate of Qualification

Step 5: Capstone Exam

- Comprehensive exam that covers all phases of the assessment, administered at the end of the course
- Format may vary depending on the assessment
- All candidates will take a machine-scorable exam
- Candidates may be required to work through scenarios, collaborate in teams, or lead presentations as part of demonstrating assessment skills
- Passing score: 70%



Prerequisites

Step 01 AES Overview

Step 02 Course Registration

Step 03 Candidate Evaluation

Step 3A Operator Skills Test

Courses

Step 04 eLearning Courses

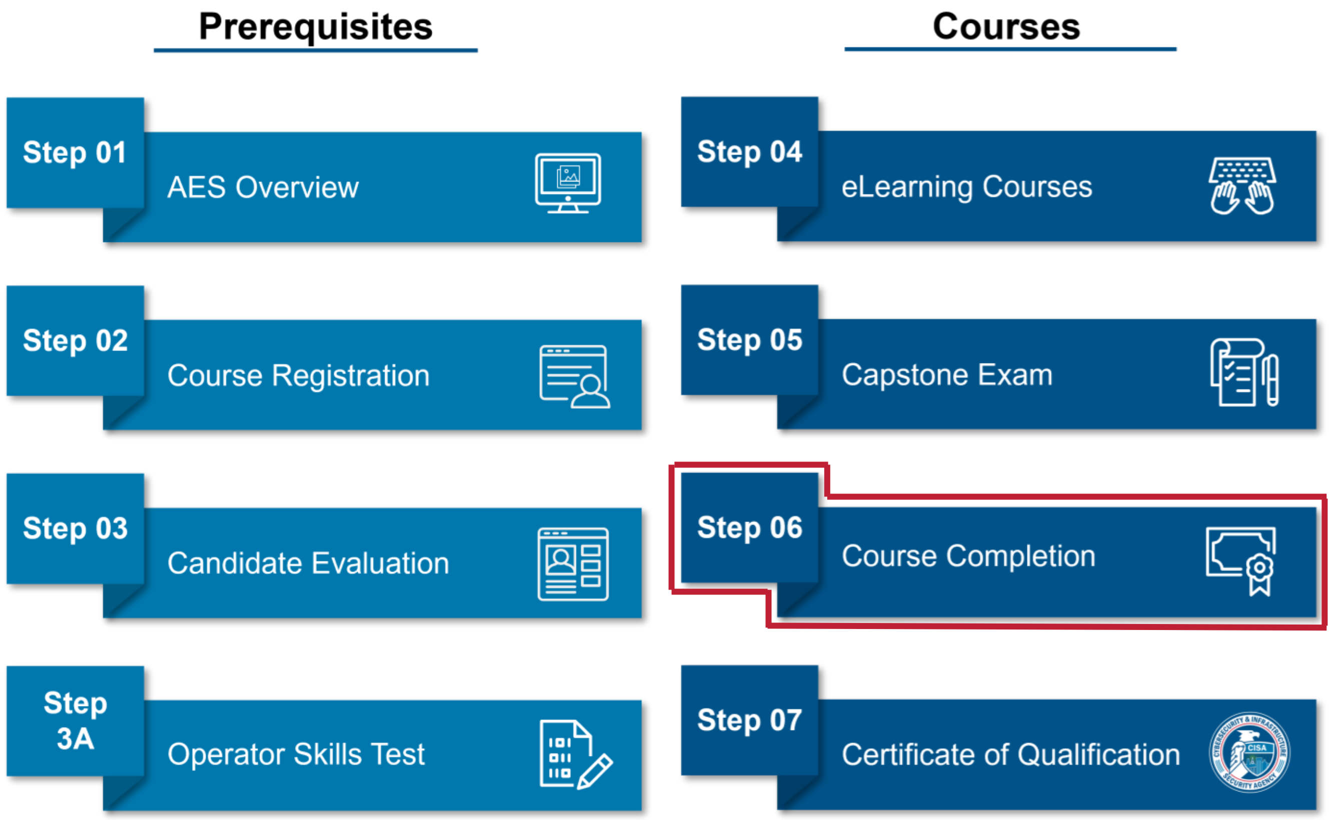
Step 05 Capstone Exam

Step 06 Course Completion

Step 07 Certificate of Qualification

Step 6: Course Completion

- After completing the course and the Capstone Exam and participant survey, students will be informed of their completion and receive a Certificate of Qualification



Prerequisites

Step 01 AES Overview

Step 02 Course Registration

Step 03 Candidate Evaluation

Step 3A Operator Skills Test

Courses

Step 04 eLearning Courses

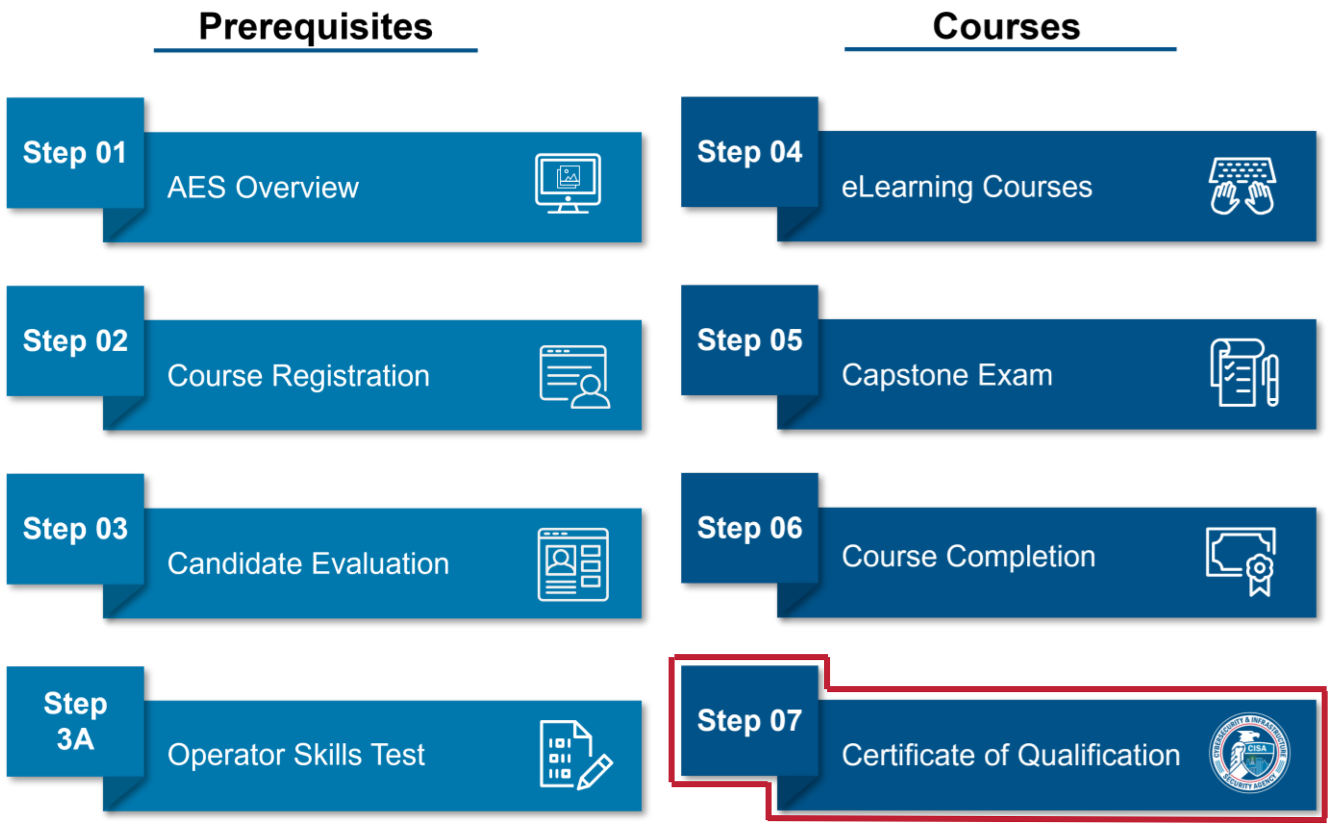
Step 05 Capstone Exam

Step 06 Course Completion

Step 07 Certificate of Qualification

Step 7: Certificate of Qualification

- After successful completion of the course and the Capstone Exam, a student receives a Certificate of Qualification
- Without a Certificate of Qualification, a student is **not** qualified to perform assessments
- Please retain a copy of the certificate as proof of your qualification status



Prerequisites

Step 01 AES Overview

Step 02 Course Registration

Step 03 Candidate Evaluation

Step 3A Operator Skills Test

Courses

Step 04 eLearning Courses

Step 05 Capstone Exam

Step 06 Course Completion

Step 07 Certificate of Qualification

AES SSG OVERVIEW

SSG Assessment Overview (Coming Soon)

- **Purpose:** Evaluate whether additional, sector-specific cybersecurity technologies and practices beyond the Cross-Sector CPGs are implemented in information technology (IT) and operational technology (OT) environments in organizations aligned to the specific Critical Infrastructure (CI) sectors
- The Sector Specific Goals (SSG) training course is designed to empower students to facilitate an SSG assessment using the Cyber Security Evaluation Tool (CSET). Students will use CSET to track responses, conduct posture analysis, and generate a report
- The Sector Specific Goals are additional voluntary practices with high-impact security actions, beyond the Cross-Sector CPGs, that outline sector-specific measures businesses and critical infrastructure owners can take to protect themselves against cyber threats. As of today, CISA has developed and released SSGs for the Energy Distribution, Chemical, and IT sectors, and U.S. Treasury is expected to release the Financial sector SSG’s in the next several weeks
- SSGs were developed based on CISA’s operational data, research on the current threat landscape, and in collaboration with Sector Risk Management Agencies (SRMAs) and sector stakeholders

AES SSG Assessment Role

Assessment Lead (AL)

- Serves as primary assessment team POC
- Leads the assessment team
- Manages the overall assessment execution
- Debriefs and delivers the assessment report

Technical Lead (TL)

- Responsible for overall assessment execution
- Leads the Technical Exchange Meeting (TEM)
- Writes the majority of the assessment report
- Supports meetings throughout the assessment

Operator (OP)

- Leads the Penetration Test
- Responsible for the testing results appendix of the assessment report; contributes to other portions
- Supports meetings throughout the assessment
- Must pass an additional pre-course exam (OST) for acceptance into the course

Sector-Specific Subject Matter Expert (S-SME)

- Requires a minimum of 5 years' OT experience in security operational technology of a specific sector
- Includes oil and gas, electric, water, chemical, manufacturing industries in an operations environment.

AES CRR EDM OVERVIEW

CRR Assessment Overview

- **Purpose:** Conduct an interview-based assessment to evaluate an organization’s operational resilience and cybersecurity practices
- Part of a U.S. Department of Homeland Security (DHS) initiative intended to help the nation’s critical infrastructure providers understand their operational resilience and ability to manage cyber risk
- Assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others
- Designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices
- Consists of 299 questions, typically delivered in a six-hour workshop
- All CRR questions have three possible responses: “Yes,” “No,” and “Incomplete

EDM Assessment Overview

- **Purpose:** Conduct an interview-based assessment to evaluate an organization’s management of external dependencies
- Part of a U.S. Department of Homeland Security (DHS) initiative intended to help the nation’s critical infrastructure providers evaluate the external dependency management (supply chain) cybersecurity practices of critical infrastructure
- Assesses enterprise programs and practices across three domains, including relationship formation, relationship management and governance, and service protection and sustainment
- Consists of 105 questions, typically delivered in a three-hour workshop
- Has three possible responses for each EDM question: “Yes,” “No,” and “Incomplete”
- Has a format similar to CRR

AES CRR EDM Assessment Role

Assessment Lead (AL)

- Serves as primary assessment team POC
- Leads the assessment team
- Manages the overall assessment execution
- Debriefs and delivers the assessment report

Technical Lead (TL)

- Responsible for overall assessment execution
- Leads the Technical Exchange Meeting (TEM)
- Writes the majority of the assessment report
- Supports meetings throughout the assessment

Operator (OP)

- Leads the Penetration Test
- Responsible for the testing results appendix of the assessment report; contributes to other portions
- Supports meetings throughout the assessment
- Must pass an additional pre-course exam (OST) for acceptance into the course

Sector-Specific Subject Matter Expert (S-SME)

- Requires a minimum of 5 years’ OT experience in security operational technology of a specific sector
- Includes oil and gas, electric, water, chemical, manufacturing industries in an operations environment.

AES CRR EDM Combined Training Course Agenda

- AES CRR EDM training course
  - Background, resilience management, critical service, CRR and EDM methodology
  - Assessment process and assessment domains
  - Assessment domains
  - Final report preparation and debrief
  - Conclusion and Capstone exam
- Audience
  - Primary Stakeholders (.gov and .mil)
    - Cyber Security Advisors (CSAs)
    - Departments and Agencies
  - Indirect Stakeholders (primary stakeholder sponsorship required)
    - Contractors

For additional information, visit https://www.cisa.gov/resources-tools/training/cyber-resilience-review-crr-external-dependency-management-edm-training

AES CSET OVERVIEW

CSET Training Overview

- **Purpose:** This course provides practical guidance on using CSET, covering interface navigation, assessment question sets, and alignment with cybersecurity standards
- Participants will gain hands-on experience to enhance resilience and compliance through effective use of CSET's features
- CISA's Cyber Security Evaluation Tool (CSET) is a robust platform for assessing and improving cybersecurity posture. CSET is used to perform CPG Assessments

AES HVA 3.0 OVERVIEW

HVA 3.0 Assessment Overview

- **Purpose:** Assess the HVA security architecture to identify technical concerns that could expose the organization to risk
- Part of a U.S. Cybersecurity and Infrastructure Security Agency (CISA) initiative intended to help government departments and agencies understand their operational resilience and ability to manage cyber risk
- Assess an HVA's security environment and organizational processes through interviews, artifact examination, and technical testing
- Designed to understand the HVA security architecture to understand its resilience as well as provide recommendations for improvement
- Most activities typically occur over a consecutive three-day period. Elapsed time may be five or six weeks, depending on report review turnaround. The Key deliverable is the HVA Assessment Final Report
- Either an HVA individual or team conducts each assessment. Individual HVA assessors are trained or qualified for a particular role

AES HVA 3.0 Assessment Roles

Assessment Lead (AL)

- Serves as primary assessment team POC
- Leads the assessment team
- Manages the overall assessment execution
- Debriefs and delivers the assessment report

Technical Lead (TL)

- Responsible for overall assessment execution
- Leads the Technical Exchange Meeting (TEM)
- Writes majority of the assessment report
- Supports meetings throughout the assessment

Operator (OP)

- Leads the Penetration Test
- Responsible for the testing results appendix of the assessment report; contributes to other portions
- Supports meetings throughout the assessment

Sector-Specific Subject Matter Expert (S-SME)

- Requires a minimum of 5 years' OT experience in security operational technology of a specific sector
- Includes oil and gas, electric, water, chemical, manufacturing industries in an operations environment.

HVA Operator Role

The HVA Operator will participate in the RVA course to include an HVA module as part of their comprehensive training. The operator has the following responsibilities:

- Assists in scoping and planning of penetration test
- Gains awareness of the condensed HVA penetration test methodology as compared to that of the RVA
- Informs higher level report sections (e.g. ExecSum, Statements of Risk)
- Identifies and reports on observed HVA system strengths
- Applies penetration test findings and expertise to overall HVA assessment outcome

Operator (OP)

- Leads the Penetration Test
- Responsible for the testing results appendix of the assessment report; contributes to other portions
- Supports meetings throughout the assessment

AES HVA 3.0 Training Course Agenda

- AES HVA training course
  - Background, HVA roles, methodology (planning)
  - Methodology (execution), Discussion Topics
  - Methodology (execution), (post-execution)
  - Methodology (post-execution)
  - Capstone
- Audience
  - Primary Stakeholders (.gov and .mil)
    - Departments and Agencies
    - National Guard
  - Indirect Stakeholders (primary stakeholder sponsorship required)
    - Contractors

For additional information, visit
https://www.cisa.gov/resources-tools/training/high-value-assets-assessment-hva-training

AES RVA OVERVIEW

RVA Assessment Overview

- **Purpose:** Collect data through on-site assessments, then combine with national threat and vulnerability information to provide an organization with actionable remediation recommendations prioritized by risk
- Part of a U.S. Cybersecurity and Infrastructure Security Agency (CISA) initiative intended to lead the National effort to understand and manage cyber and physical risk to our critical infrastructure
- Assesses organizations' alignment with information security laws, regulations, policies, and standards by conducting collaborative and independent operational testing and assessments
- Provides customer organizations with an understanding of their operational cybersecurity risk and posture, and provides DHS with vital situational awareness
- Delivers the RVA Assessment Final Report

AES RVA Assessment Role

Assessment Lead (AL)

- Serves as primary assessment team POC
- Leads the assessment team
- Manages the overall assessment execution
- Debriefs and delivers the assessment report

Technical Lead (TL)

- Responsible for overall assessment execution
- Leads the Technical Exchange Meeting (TEM)
- Writes the majority of the assessment report
- Supports meetings throughout the assessment

Operator (OP)

- Leads the Penetration Test
- Responsible for the testing results appendix of the assessment report; contributes to other portions
- Supports meetings throughout the assessment
- Must pass an additional pre-course exam (OST) for acceptance into the course

Sector-Specific Subject Matter Expert (S-SME)

- Requires a minimum of 5 years' OT experience in security operational technology of a specific sector
- Includes oil and gas, electric, water, chemical, manufacturing industries in an operations environment.

AES RVA Training Course Agenda

- AES RVA training course
  - Background, RVA roles, methodology (planning, execution)
  - Methodology (post-assessment)
  - Team capstone exercise introduction
  - Team capstone exercise
  - Capstone out-brief presentation and final report
- Audience
  - Primary Stakeholders (.gov and .mil)
    - Departments and Agencies
    - National Guard
  - Indirect Stakeholders (primary stakeholder sponsorship required)
    - Contractors

For additional information, visit
https://www.cisa.gov/resources-tools/training/risk-and-vulnerability-assessment-rva-training

AES VADR OVERVIEW

VADR Assessment Overview

- **Purpose:** The VADR is an expert-based Operational Technology (OT) engagement that relies on Subject Matter Experts (SME) and utilizes federal and industry standards, guidelines, and best practices to perform the analysis. The VADR assessment team examines network architecture and design, reviews system configuration and log files, and analyzes network traffic
- There are three main components to an onsite VADR engagement:
  - **Design Architecture Review**: VADR assessors validate the system’s process, components, boundaries, and communication paths
  - **Network Architecture Verification and Validation:** VADR assessors review PCAP data with Asset-Owners to validate network diagrams and to identify anomalies or abnormal traffic
  - **Cybersecurity Spot Check:** VADR assessors identify gaps between implementation and best practices in various cybersecurity topics
- VADR assessors use best practices, including the Purdue model, NIST 800-53, and the CISA Recommended Secure Architecture
- The VADR is not intended to be a comprehensive audit; instead, VADR assessors identify the most significant weaknesses and make mitigation recommendations to improve an organization’s overall cybersecurity posture

AES VADR Assessment Roles

Assessment Lead (AL)

- Serves as primary assessment team POC
- Leads the assessment team
- Manages the overall assessment execution
- Debriefs and delivers the assessment report

Technical Lead (TL)

- Responsible for overall assessment execution
- Leads the Technical Exchange Meeting (TEM)
- Writes the majority of the assessment report
- Supports meetings throughout the assessment

Operator (OP)

- Leads the Penetration Test
- Responsible for the testing results appendix of the assessment report; contributes to other portions
- Supports meetings throughout the assessment
- Must pass an additional pre-course exam (OST) for acceptance into the course

Sector-Specific Subject Matter Expert (S-SME)

- Requires a minimum of 5 years’ OT experience in security operational technology of a specific sector
- Includes oil and gas, electric, water, chemical, manufacturing industries in an operations environment.

AES VADR Training Course Agenda

- AES VADR training course
  - Pre-execution activities (scoping, intake, OSINT)
  - Network analysis and execution activities (validation of captures, interviewing techniques and subjects)
  - Execution activities and post-execution (cont. interviews, out-briefing, reporting)
  - Test and capstone
  - Hotwash and feedback
- Primary
  - Assessors with IT and OT experience, Control Systems Subject Matter Experts (Both defined as having five or more years' experience)
- Secondary
  - Contractors and others looking to establish an assessment program for Operational Technology systems

For additional information, visit
https://www.cisa.gov/resources-tools/training/validated-architecture-design-review-vadr-training

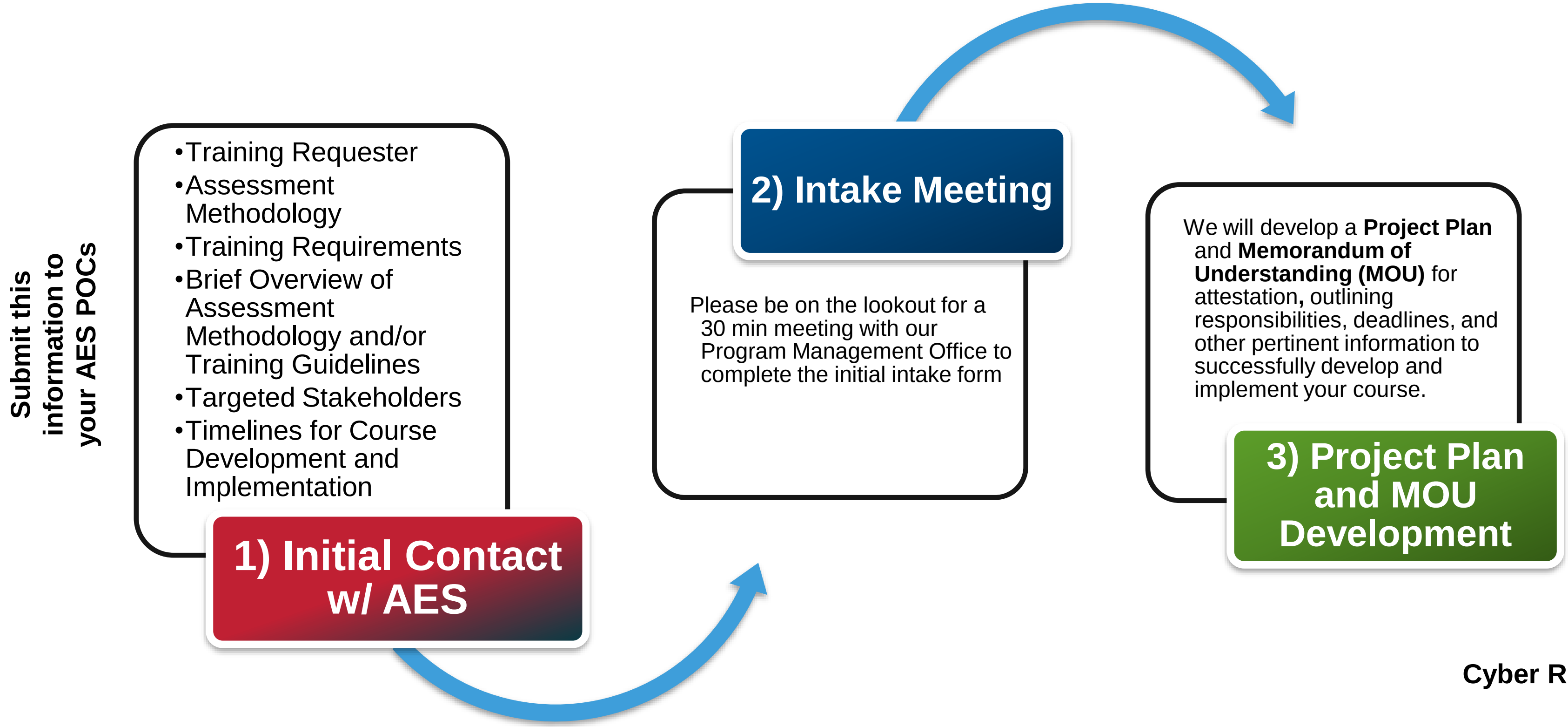
AES COURSE DEVELOPMENT

How AES Develops Courses

We strongly urge our Internal colleagues to employ AES to develop courses to support the scaling of your assessment methodologies and training needs.

The following outlines the process to kickstart course creation. Please note course development can take anywhere from 3 to 11 work weeks, depending on the complexity of the assessment methodology and instructional design.

Note: Your AES federal POCs are Tara Brewer and Victoria Newman.



Submit this information to your AES POCs

- Training Requester
- Assessment Methodology
- Training Requirements
- Brief Overview of Assessment Methodology and/or Training Guidelines
- Targeted Stakeholders
- Timelines for Course Development and Implementation

1) Initial Contact w/ AES

2) Intake Meeting

Please be on the lookout for a 30 min meeting with our Program Management Office to complete the initial intake form

We will develop a **Project Plan** and **Memorandum of Understanding (MOU)** for attestation**,** outlining responsibilities, deadlines, and other pertinent information to successfully develop and implement your course.

3) Project Plan and MOU Development

Why utilize AES's course creation services?

Improved Course Adoption and Enrollment

Courses developed through our professional services see significantly higher adoption and enrollment rates. Since the inception of the program, AES has qualified **1405 students across all its courses.**

Expertise & Customization

Benefit from the extensive knowledge and experience of our subject matter experts. Access a wealth of resources and tools designed to develop high-quality, comprehensive courses. Courses are tailored to meet the specific needs of your assessment methodology, training needs, and targeted stakeholder communities.

Support

Ongoing support and maintenance to ensure your course remains current and effective.

For more information, please contact the AES mailbox

Email: AEStraining@mail.cisa.dhs.gov

Visit: https://www.cisa.gov/aes

Acronyms – 1

Acronym	Meaning
AES	Assessment Evaluation and Standardization
AL	Assessment Lead
CE	Candidate Evaluation Exam
CERT	Community Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
COBIT	Control Objectives for Information and Related Technologies
CPG	Cybersecurity Performance Goals
CRISC	Certified in Risk and Information System Control
CRR	Cyber Resilience Review
CSF	Cyber Security Framework (NIST)

Acronym	Meaning
CSA	Cyber Security Advisor
CSET	Cyber Security Evaluation Tool
DHS	U.S. Department of Homeland Security
EDM	External Dependency Management
GDSA	GIAC Defensible Security Architecture
GIAC	Global Information Assurance Certification
GPEN	GIAC Certified Penetration Tester
HACS	Highly Adaptive Cybersecurity Services
HVA	High Value Asset
ILT	Instructor-Led Training
IEC	International Electrotechnical Commission

Acronyms – 2

Acronym	Meaning
ISACA	Information Systems Audit and Control Association
ISACA CISA	ISACA Certified Information Systems Auditor
ISO	International Organization for Standardization
ISSAP	Information Systems Security Architecture Professional
IT	Information Technology
LMS	Learning Management System
NIST	National Institute of Standards and Technology
OP	Operator
OSCE	Offensive Security Certified Expert
OSCP	Offensive Security Certified Professional
OST	Operator Skills Test
OT	Operational Technology

Acronym	Meaning
POC	Point of Contact
RMF	Risk Management Framework (NIST)
RMM	Resilience Management Model
RVA	Risk and Vulnerability Assessment
SLTT	State, Local, Tribal, & Territorial Governments
S-SME	Sector-Specific Subject Matter Expert
TEM	Technical Exchange Meeting
TL	Technical Lead
TTP	Tactics, Techniques, and Procedures
VADR	Validated Architecture Design Review

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA