ASSESSMENT EVALUATION AND STANDARDIZATION (AES)

PROGRAM OVERVIEW

Agenda

1. AES Program
2. AES Training Process
3. AES Qualification Process
4. AES CPG Overview
5. AES CRR EDM Overview
6. AES HVA Overview
7. AES RVA Overview
8. AES VADR Overview
9. AES IMR Overview

1. AES PROGRAM

Assessment Evaluation and Standardization (AES) Program

- The role and mission of the Assessment Evaluation and Standardization (AES) program is to increase the quality and quantity of cyber professionals who can execute CISA cyber assessments
- Training assessors to conduct CISA standard Cyber Risk Assessment methodologies is a major step in setting up an ecosystem that is critical to the success of performing cyber assessments, and in providing national-level data views that drive initiatives to reduce risk
- The approach assists all .GOV and .MIL and critical Infrastructure to include SLTT, Public, and Private Organizations

Current AES Training Courses – 1

Assessment	Assessment Purpose	Course Length	Mode
Cybersecurity Performance Goals (CPGs)	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	3 hours	Instructor Led Virtual Training
Cyber Resilience Review (CRR) External Dependency Management (EDM)	Conduct an interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices Conduct an interview-based assessment to evaluate an organization's management of external dependencies	5 days	Instructor Led Virtual Training
*High Value Asset (HVA) *Currently focused on Non-Tier 1 HVAs only	Assess the HVA security architecture to identify technical concerns that could expose the organization to risk	5 days	Instructor Led Virtual Training

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

Current AES Training Courses – 2

Assessment	Assessment Purpose	Course Length	Mode
Risk and Vulnerability Assessment (RVA)	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	5 days	Instructor Led Virtual Training
Validated Architecture Design Review (VADR)	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 ▪ to identify anomalous and potentially suspicious communication flows	5 days	Instructor Led Virtual Training
Incident Management Review (IMR)	Evaluate the processes used to identify and analyze events, declare incidents, determine a response, and improve an organization's incident management capability	—	On Demand

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, CRR, EDM, HVA, IMR, and VADR assessments

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
- 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 are

- 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 recommends that applicants hold one or more nationally recognized information systems or cybersecurity certifications, for example

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

Prerequisites for AES RVA Operator Role – 1

The minimum skills for an applicant are

- 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
- A minimum of three years of **all** the following experience:
  - Performing authorized pen testing on enterprise networks
  - Gaining access to targeted networks
  - Applying expertise to enable new exploitation and maintaining access

Prerequisites for AES RVA Operator Role – 2

- A minimum of three years of **all** the following experience *(continued)*
  - 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

2. AES TRAINING PROCESS

AES Training Process Steps

Prerequisites

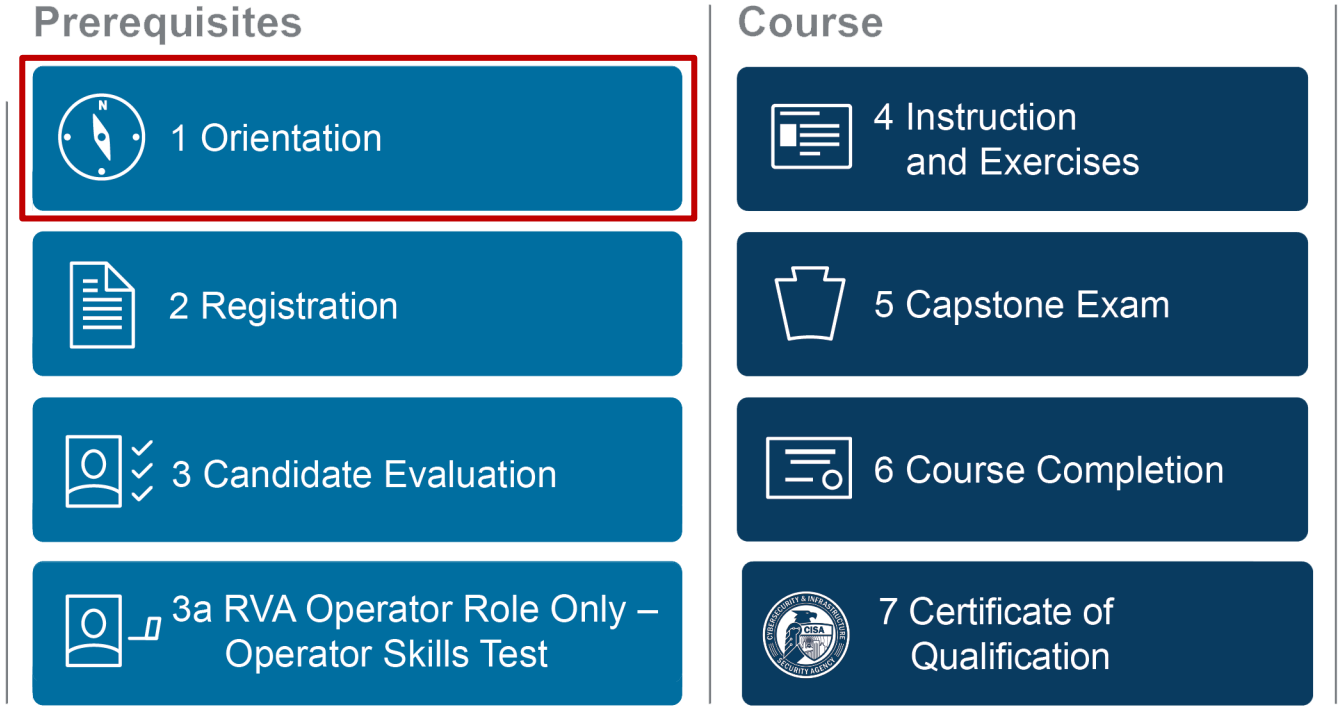
- 1 Orientation
- 2 Registration
- 3 Candidate Evaluation
- 3a RVA Operator Role Only – Operator Skills Test

Course

- 4 Instruction and Exercises
- 5 Capstone Exam
- 6 Course Completion
- 7 Certificate of Qualification

Step 1: Orientation

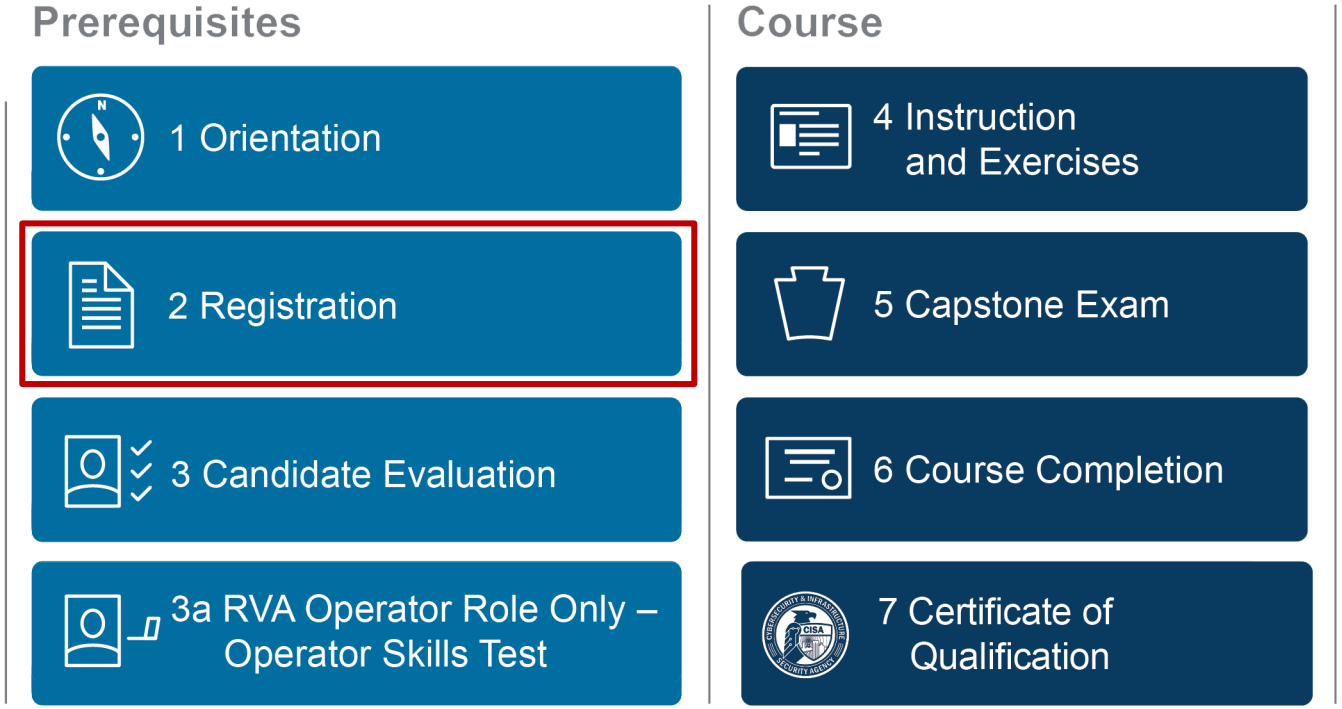
- Ensures mutual understanding of process
- CISA presents an overview of AES program
  - AES process
  - Roles
  - Requirements for successful completion



Step 2: Registration

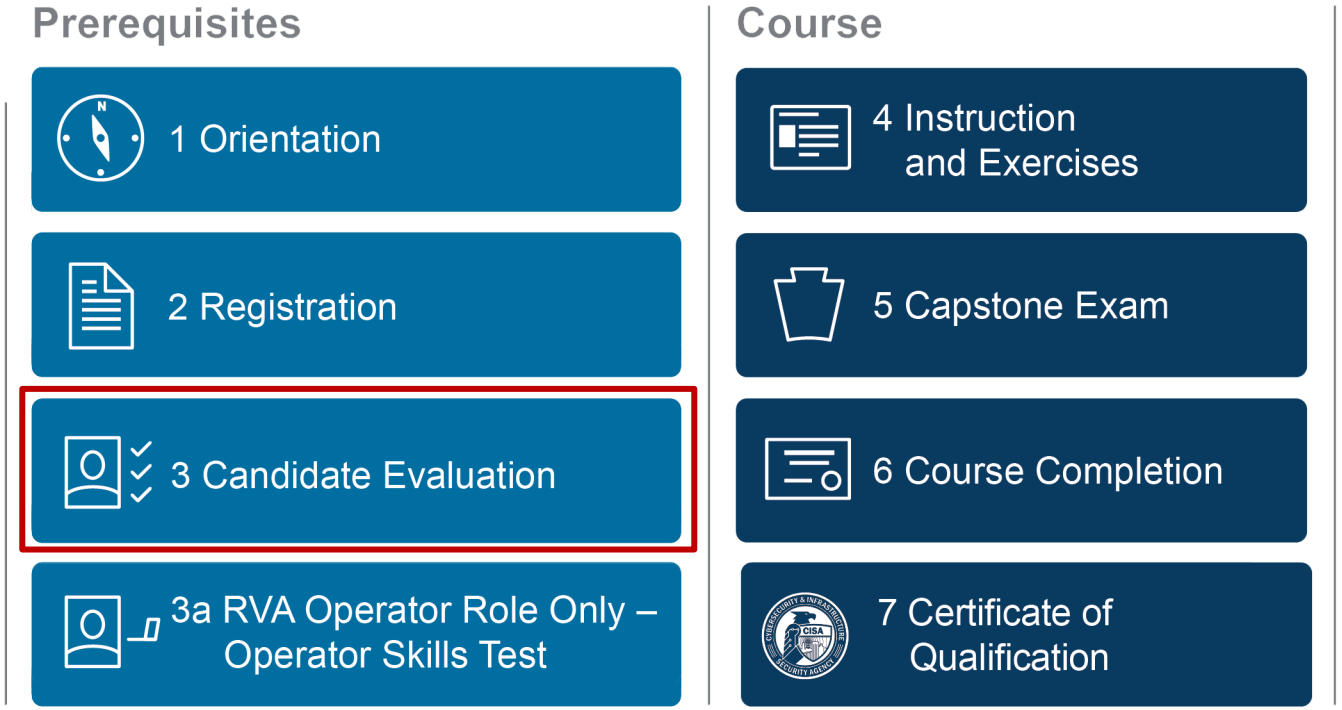
Participants

- Self-register in the Moodle learning management system 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



Step 3: Candidate Evaluation (CE) Exam

- Confirmation that all applicants have a baseline cybersecurity knowledge to be successful in the course
- Individual administration, on-line
- Machine-scoreable questions
- Passing score: 70%
- Passing score required to take the course
- Limited to three attempts



Step 3: CE Exam

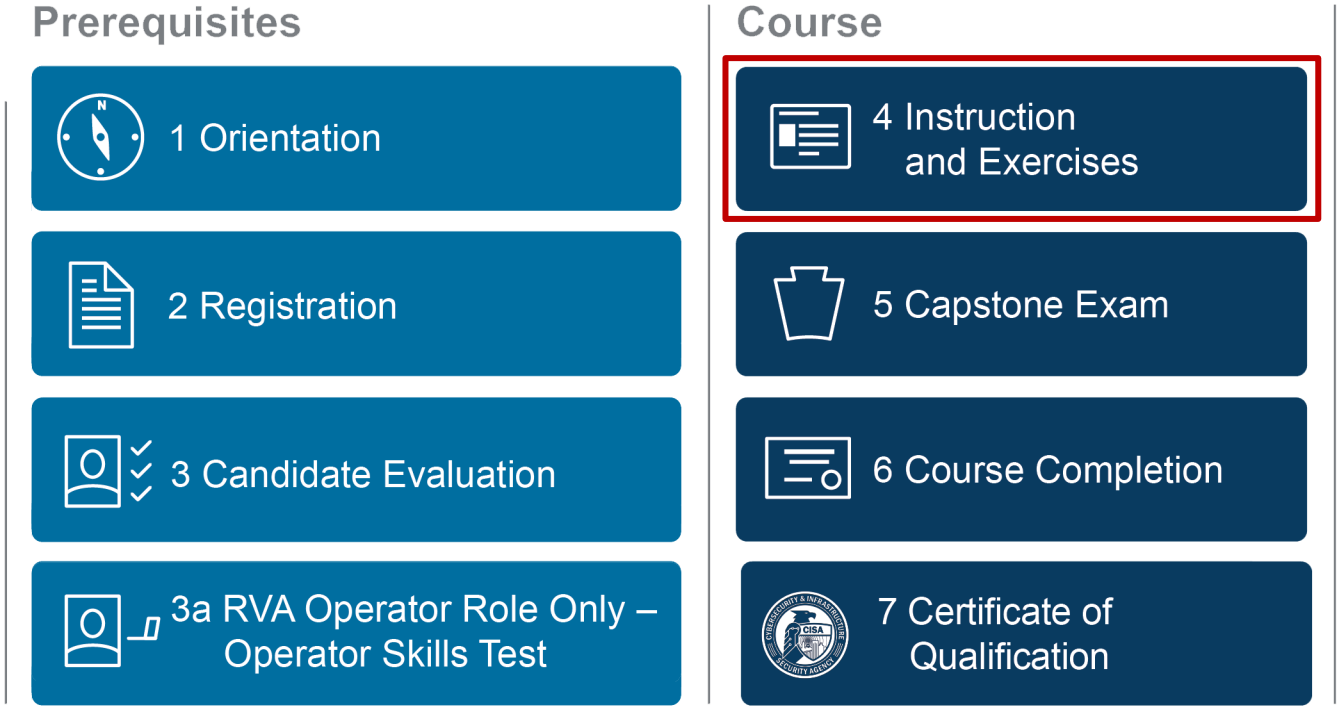
- AES applicants must read and acknowledge AES Code of Ethics and Compliance to proceed to the CE exam
- To be admitted to a course, AES students must perform all prerequisite work and obtain a passing score of 70% or higher 30 days before the course start date. After completing these requirements, a student has access to enroll in course(s). No exceptions will be made
- Successful CE exam results are valid for six months. After enrollment eligibility has lapsed, applicants may reregister for the course and repeat (retake) the prerequisite
- After successful course enrollment, all course materials are made available for review and use during course delivery

Step 3a: Operator Skill Test (OST): RVA Operator Only

- Additional prerequisite evaluation required for all assessors who will be RVA operators
- Individual, timed evaluation
  - Limited to three attempts in a 24-hour period
- Lab and quiz that evaluates penetration testing skills

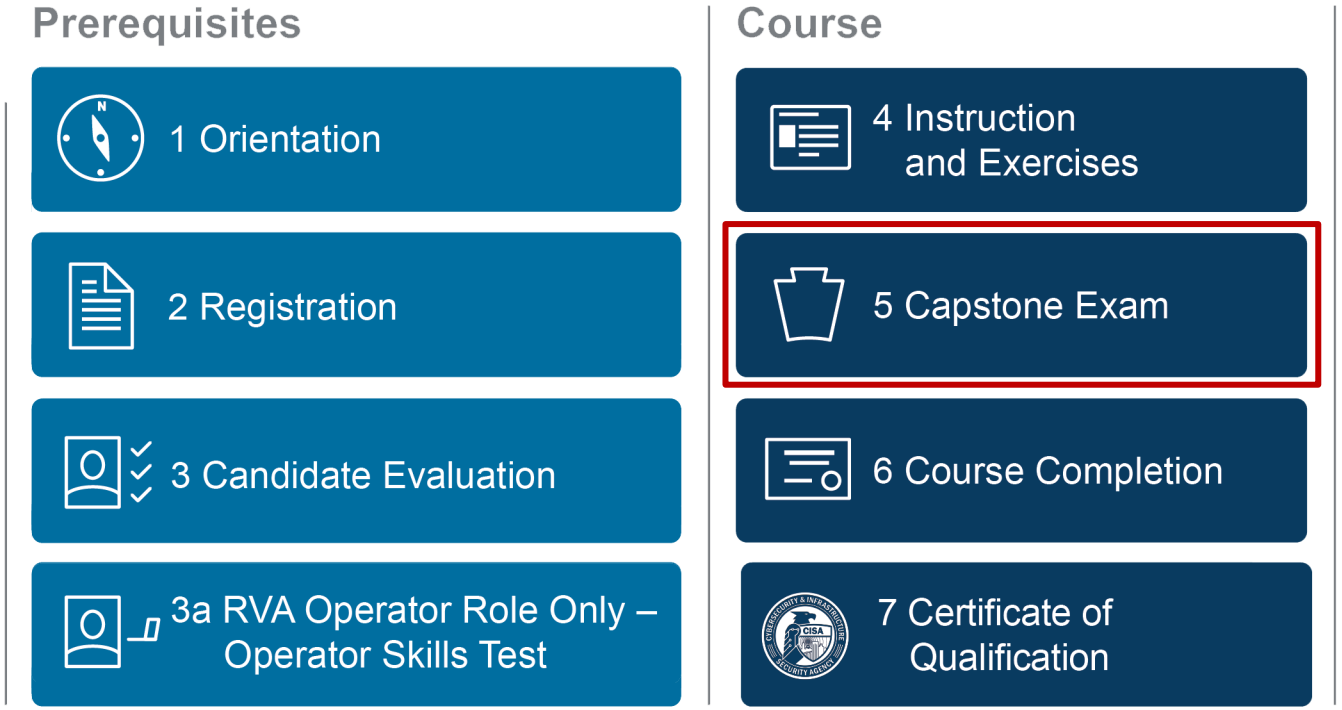
Step 4: Instruction and Exercises

- Length of most courses is five days, except for
  - CPG – three hours
  - IMR – on demand
- Exercises allow students to practice assessment activities
- Instructor-led and delivered via collaboration platform (e.g., Zoom for Government) and learning management system (LMS) (e.g., Moodle)
- Class attendance is monitored



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%



Step 6: Course Completion

After completing the course and the Capstone Exam

- Successful candidate receives an email with “Pass” information
- Unsuccessful candidate receives an email with “Did Not Pass” information

3. AES QUALIFICATION PROCESS

Step 7: 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

4. AES CPG OVERVIEW

CPG Assessment Overview

- 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)
- 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) observed by CISA and its government and industry partners
- By implementing these goals, owners and operators will reduce risks to both critical infrastructure operations and to the American people.
- The assessment process depends on in-person interviews leveraging CSET to track responses, conduct posture analysis, and generate a report

AES CPG Assessment Role

Assessment Lead (AL)

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

5. AES CRR EDM OVERVIEW

CRR Assessment Overview

- 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

- 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)

- Primary Duties
  - Serves as primary assessment team POC
  - Leads the assessment team
  - Manages the overall assessment execution
  - Debriefs and delivers the assessment report
- An individual or a team conducts each CRR EDM assessment
- Role in the CPG, CRR, EDM, HVA, IMR, and VADR assessments

AES CRR EDM Combined Training Course Agenda

- Five-Day AES CRR EDM training course
  - Day 1: Background, resilience management, critical service, CRR and EDM methodology
  - Day 2: Assessment process and assessment domains
  - Day 3: Assessment domains
  - Day 4: Final report preparation and debrief
  - Day 5: Conclusion and Capstone exam
- Audience
  - Primary Stakeholders (**.**gov and **.**mil)
    - Cyber Security Advisors (CSAs)
    - Departments and Agencies
  - Indirect Stakeholders (primary stakeholder sponsorship required)
    - Contractors

6. AES HVA OVERVIEW

AES HVA Assessment Overview

- 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
- Key deliverable is the HVA Assessment Final Report

AES HVA 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, CRR, EDM, HVA, IMR, and VADR assessments

Technical Lead (TL)

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

- Either an HVA individual or team conducts each assessment
- Individual HVA assessors are trained or qualified for a particular role

AES HVA Training Course Agenda

- Five-Day AES HVA training course
  - Day 1 – Background, HVA roles, methodology (planning)
  - Day 2 – Methodology (execution), Discussion Topics
  - Day 3 – Methodology (execution), (post-execution)
  - Day 4 – Methodology (post-execution)
  - Day 5 – Capstone
- Audience
  - Primary Stakeholders (.gov and .mil)
    - Departments and Agencies
    - National Guard
  - Indirect Stakeholders (primary stakeholder sponsorship required)
    - Contractors

7. AES RVA OVERVIEW

AES RVA Assessment Overview

- 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

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

AES RVA Training Course Agenda

- Five-Day AES RVA training course
  - Day 1 – Background, RVA roles, methodology (planning, execution)
  - Day 2 – Methodology (post-assessment)
  - Day 3 – Team capstone exercise introduction
  - Day 4 – Team capstone exercise
  - Day 5 – Capstone outbrief presentation and final report
- Audience
  - Primary Stakeholders (.gov and .mil)
    - Departments and Agencies
    - National Guard
  - Indirect Stakeholders (primary stakeholder sponsorship required)
    - Contractors

8. AES VADR OVERVIEW

AES VADR Assessment Overview – 1

- Empowers assessors to evaluate Operational Technology systems within critical infrastructure networks for secure design and operational intent
- Encompasses architecture and design review, system configuration and log file review, along with sophisticated analysis of network traffic
- Develops a detailed representation of the communications, flows, and relationships between devices designed to identify anomalous, and potentially suspicious communication flows
- Verifies that successful students are able to assess the design of the system accurately and to inform organizational leadership how to manage the risk effectively, which is inherent in its selected design methods and cybersecurity solutions

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

AES VADR Assessment Overview – 2

- Depends on in-person interviews, documentation review, and in-depth technical analysis
- Uses best practices, including the Purdue model, NIST 800-53, and the CISA Recommended Secure Architecture
- Not intended to be a comprehensive audit; instead, it helps an organization identify the most significant weaknesses and make recommendations to mitigate them to improve an organization's overall cybersecurity posture

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

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
- Role in CPG, CRR, EDM, HVA, IMR, and VADR assessments

Sector Subject Matter Expert (S-SME)

- Requires a minimum of five 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

AES VADR Training Course Agenda

- Five-Day AES VADR training course
  - Day 1 – Pre-execution activities (scoping, intake, OSINT)
  - Day 2 – Network analysis and execution activities (validation of captures, interviewing techniques and subjects)
  - Day 3 – Execution activities and post-execution (cont. interviews, outbriefing, reporting)
  - Day 4 – Test and capstone
  - Day 5 – 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

9. AES IMR OVERVIEW

IMR Assessment Overview

- Part of a U.S. Department of Homeland Security (DHS) initiative intended to help the nation's critical infrastructure providers assess and provide a measure of an organization's event and incident handling capabilities
- Assesses enterprise programs and practices across a range of six domains including event detection and handling, incident declaration, handling and response, post-incident analysis and testing, integration of organization capabilities, protection and sustainment of the incident management function, and preparation of incident response
- Consists of 88 questions in a facilitated interview-based review typically delivered in a three-to-four-hour workshop
- All IMR questions have three possible responses: "Yes," "No," and "Incomplete"

AES IMR Assessment Role

Assessment Lead (AL)

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

AES IMR Training Course Agenda

- On-demand AES IMR training course
  - Part 1: Introduction, critical services, background, pre-assessment, facilitation
  - Part 2: Event handling, incident response, post-incident, organizational capabilities, protection and sustainment, preparation for incident response
  - Part 3: Reporting, IMR vignettes, capstone
- Audience
  - Primary Stakeholders (.gov and .mil)
    - Cyber Security Advisors (CSAs)
    - Departments and agencies
  - Indirect Stakeholders (primary stakeholder sponsorship required)
    - Contractors

Contact us soon to get started!

Email AEStraining@hq.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 Systems 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
IMR	Incident Management Review
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, and 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