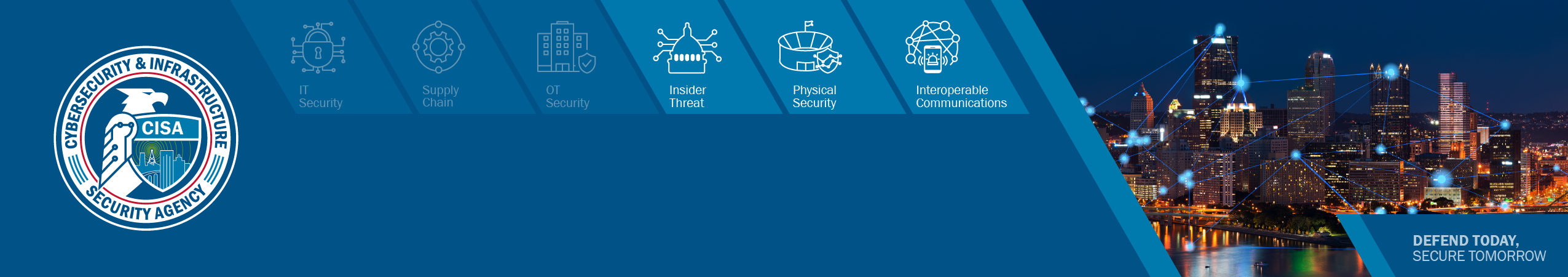
AES Fact Sheet

The Assessment Evaluation and Standardization (AES) Program qualifies individuals to conduct Cybersecurity and Infrastructure Security Agency (CISA) assessments in the active engagement of securing the Nation's physical and cyber infrastructure against threats.

## Objectives

* The role and mission of the Assessment Evaluation and Standardization program is to increase the quality and quantity of cyber professionals who can execute CISA cyber assessments.
* Training and qualifying 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 will assist all .GOV, .MIL, Critical Infrastructure to include SLTT, Public and Private Organizations.

## Assessments

AES offers training for the following assessments.

**Cyber Resilience Review (CRR)** Evaluates operational resilience and cybersecurity practices through an interview-based assessment.

**Cybersecurity Performance Goals (CPG)** Evaluates 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.

**External Dependency Management (EDM)** Evaluates management of external dependencies through an interview-based assessment.

**High Value Assets (HVA)** Evaluates the HVA security architecture to identify potential risks from technical concerns (for non-Tier 1 HVAs only)

**Incident Management Review (IMR)** Evaluates the processes used to identify and analyze events, declare incidents, determine a response, and improve an organization’s incident management capability

**Risk and Vulnerability Assessment (RVA)** Evaluates on-site data and national threats and vulnerabilities to identify potential exploitation of network security controls

**Validated Architecture Design Review (VADR)** Evaluates systems, networks, and security services to determine their reliability and resiliency of design, construction, and operation

## Training Process

All AES training courses share a common process.

The AES Training Process, showing rectangles with the following steps. 

Prerequisites
1. Orientation
2. Registration
3. Candidate Evaluation (CE) exam
3a. RVA Operator Role Only - Operator Skills Test

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

Figure 1: The AES Training Process

Each phase must be passed before the next phase will become available.

1. **Orientation: AES Program Overview Video** – Provides an overview of the AES Program, qualification process and details of the course offerings.
2. **Registration: Self-Enrollment** – Allows students to register for Learning Management System (LMS) accounts, enroll in AES prerequisites, and enroll in AES courses provided they meet the qualification requirements.
3. **Candidate Evaluation** – Evaluates whether an applicant has the pre-requisite knowledge and skills to succeed in an AES course. Applicants receive preparatory materials, and can try up to three times to score 70% or higher to pass the exam. **3a. RVA Operator Skills Test** – Evaluates whether an applicant has the pre-requisite knowledge and skills to succeed in the RVA Operator role only.
4. **Instruction and Exercises** – Provide a detailed overview of the assessment process and includes exercises that allow students to practice assessment activities. Courses are virtual.
5. **Capstone** **Exam** – Varies by course but, in general, covers all phases of the assessment, and administered individually at the end of each course. Candidates must score 70% or higher to pass the exam.
6. **Course Completion** – Confirms that the candidate has completed the course successfully and passed the Capstone Exam.
7. **Certificate of Qualification** – Demonstrates that candidates are qualified as Assessors after successful completion of the course and the Capstone Exam. The student receives a Certificate of Qualification.

## About Vulnerability Management

Vulnerability Management (VM) brings together vulnerability-focused teams throughout CISA’s Cybersecurity Division to reduce the attack surface of Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies, and enable customers and stakeholders to make data-driven decisions to manage their own risk portfolios. VM’s mission is to enable stakeholders to understand and manage vulnerabilities in our Nation’s critical infrastructure. Our vision is to be the premier, trusted partner for identifying and managing vulnerabilities by achieving the following goals:

* reduce stakeholder vulnerabilities
* increase national resilience
* enable data-driven decisions
* influence operational behaviors
* responsible disclosure of vulnerabilities

## Get Started

Email [AEStraining@hq.dhs.gov](mailto:AEStraining@hq.dhs.gov) or visit the [AES Program web page](https://www.cisa.gov/aes) to learn how your organization can benefit from participating in AES training.