ASSESSMENT EVALUATION AND STANDARDIZATION (AES)

High Value Asset (HVA) Qualification Policy

CISA Vulnerability Management (VM) Branch
September 2023

Table of Contents

1 Introduction

The Department of Homeland Security (DHS) Cybersecurity Infrastructure and Security Agency (CISA) offers Assessment Evaluation and Standardization (AES) High Value Asset (HVA) assessment training to federal, state, local, tribal, territorial, critical infrastructure, and private sectors to promote education and qualification in the areas of cyber assessments, resilience, and sound cybersecurity practices. This document describes CISA's policy for becoming a qualified AES HVA assessor.

2 Scope

The AES HVA Qualification Policy (the Policy) applies to all AES HVA courses, whether virtual or in-person, offered in the AES program. The Policy and all statements are applicable to registered and enrolled students, observers and, in some situations, AES instructors.

3 Acknowledgement

All students and prospective students must read and understand the Policy.

4 AES HVA Qualification

4.1 Student Profile

- AES students must enter and/or update all required data on the student profile within the Moodle Learning Management System (LMS).

4.2 Self-Registration/Enrollment

- AES students must self-register for a Moodle LMS account through the designated URL provided by DHS CISA, located on CISA.gov/AES.
- AES students must self-enroll in prerequisite(s) and courses within the designated time to ensure a seat in the course.

4.3 Academic Integrity and Cheating

- All students and prospective students must acknowledge that they have read and understand the AES Code of Ethics and Compliance, located in Moodle.
- Students must perform all course exercises, evaluations, and capstone exams alone, unless the course allows group[1] activity.
- Course instructors, students, points of contact (POCs), and observers must report suspected or proven cheating to CISA.

4.4 Assessor Qualification

- AES students must perform all prerequisite work, enroll in the course, successfully complete the course, and pass both parts of the capstone exam: the multiple choice and the final report.
- AES students must be in attendance for all course instruction.
- AES HVA students are no longer required to submit a field report after they pass both parts of the AES HVA capstone exam to be deemed qualified to conduct non-tier 1 (NT1) HVA assessments.
- All students will be qualified to perform a CISA assessment upon successful completion of the AES course associated with that specific assessment.
- AES students will receive notification of their qualification status by receiving a certificate of qualification.
- AES students who do not successfully complete the capstone exam or other course requirements as determined by CISA for any AES course will receive a Did Not Pass (DNP) letter through email.

[1] AES Instructors will inform students when group activities are necessary.

4.5 LMS

- AES requires all AES students to create an account for the training portal, Moodle, that is accessible on-demand.
- AES students must perform all course work through the LMS.
- AES students must use only course links and materials available in the LMS.
- AES students are enabled to view all past and current course training modules, background information, and reference materials at their convenience.
- AES provides AES qualification policy and procedures on the LMS for students to review.

4.6 Communication

- For all questions and correspondence on this policy or the AES Qualification Program, please email AEStraining@hq.dhs.gov.
- For questions on the NT1 report submittals, please email HVAPMO@cisa.dhs.gov.

5 Related Practices and Supporting Documents

None