CISA Cyber Assessment Qualification Initiative

The Cybersecurity and Infrastructure Security Agency (CISA) supports federal, state, local, tribal and territorial governments and critical infrastructure partners by providing proactive testing and assessment services.

CISA Cyber Assessment Qualification Initiative (CQI) qualifies teams to conduct assessments following CISA standards and methodologies. CQI is a four-day course that enables organizational teams to learn and apply offered CISA assessment methodologies using the CERT Simulated, Training, and Exercise Platform (STEPfwd). CQI will initially focus on CISA's Risk and Vulnerability Assessments (RVAs) and expand to encompass all CISA Cyber Assessment capabilities.

CQI OBJECTIVES

- Qualify teams to conduct assessments in a consistent manner.
- Provide CISA with non-attributable data that will aide in informing the creation and improvement of cybersecurity policies through data-driven decision-making.
- Standardize CISA-offered assessments across its stakeholders for third-party and self-assessment implementation.

CQI PHASES AND TIMELINE

Planning and Pre-Qualification

- Sponsored team candidate registers with CISA
- Candidate Technical Evaluation (CTE) is scheduled
- Candidate takes CTE

CQI Methodology Training

- Sponsored team attend in-person four-day training
  - Two days of instructor-led training and exercises
  - One day of Capstone exercises
  - One day report writing

CQI Qualification

- Sponsored team is qualified upon successful completion of the training

Qualification Maintenance

- Inform CISA of any upcoming assessments 30 days prior to start date
- Submit data* within 30 days of the completion of the assessment
- Perform at least one CISA assessment annually
- Qualified organization is subject to an audit a minimum of every two years
  - Organizations must re-qualify every 3 years

*CISA does not share collected information without written consent from the stakeholder. The data is used to develop a non-attributed annual report for trending and analysis purposes. A copy of the latest report is available upon request.

ABOUT VULNERABILITY MANAGEMENT

Vulnerability Management brings together vulnerability focused teams across 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.

Our goals are:

- **Reduce Stakeholder Vulnerabilities**
- **Increase National Resilience**
- **Enable Data-Driven Decisions**
- **Influence Operational Behaviors**
- **Responsible Disclosure of Vulnerabilities**

Additional Information

CISA Cyber Assessment Qualification Initiative is available at no cost. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Training availability is limited. Contact us at **CSD_VM_Methodology@cisa.dhs.gov** to get started.

MISSION AND VISION

Mission: *Enabling stakeholders to understand and manage vulnerabilities in our Nation's critical infrastructure.*

Vision: *To be the premier, trusted partner for identifying and managing vulnerabilities.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CISA Cyber Assessment Qualification Initiative

Candidate Knowledge Skills and Abilities Minimal Requirements

The Cybersecurity and Infrastructure Security Agency (CISA) supports federal, state, local, tribal and territorial governments and critical infrastructure partners by providing proactive testing and assessment services.

CISA Cyber Assessment Qualification Initiative (CQI) qualifies teams to conduct assessments following CISA standards and methodologies. CQI is a four-day course that enables organizational teams to learn and apply offered CISA assessment methodologies using the CERT Simulated, Training, and Exercise Platform (STEPfwd). CQI will initially focus on CISA's Risk and Vulnerability Assessments (RVAs) and expand to encompass all CISA Cyber Assessment capabilities.

ASSUMPTIONS

- The CQI program assumes that each member of the assessment team already possesses basic penetration (pen) testing knowledge and skills. To evaluate this assumption all team members, referred to as Candidates in this program, will take a Candidate Technical Evaluation (CTE)..

CANDIDATE TECHNICAL EVALUATION

- The objective of the CTE is to ensure that all members of an assessment team have the fundamental skillset required to both understand the content of the training and provide a quality assessment. Very limited time is spent during the training covering pen testing skills and knowledge. These topics are only covered in the context of the methodology.
- The CTE examines basic pen testing technical skills, such as enumeration, exploitation, privilege escalation, and pivoting within a network. Completion of the CTE is required of all team members prior to attending training.
- Each member of the assessment team completes the evaluation individually and results will be reported to each Candidate.
- The CTE is not intended to be a thorough technical qualification process.

CTE PROCESS

- During the evaluation, the candidate connects to the test network using the instructions provided by the Evaluation Team. The candidate is required to scan, enumerate, and compromise as many systems as possible within an eight-hour time period.

- For each compromised system, the candidate must demonstrate proof-of-compromise, e.g., modifying local.txt or proof.txt on the compromised user's desktop.

- 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.

ELIGIBILITY

The following eligibility criteria are defined as part of the application process. The candidate:

- has the primary job function of pen testing
- must be affiliated with a federal, state, tribal, local government agency, or organization that provides critical infrastructure
- must have the approval of the sponsor agency's security office to access the agency's IT infrastructure
  - Acceptable approval can include adequate granted access privileges/permissions on IT infrastructure and a need-to-know.
  - Other forms of approval are considered on a case by case basis.

MINIMAL SKILLS

The following is a list of minimal skills that are desirable to complete the certification process successfully. Lacking one or more skills reduces the likelihood that the candidate can successfully complete this certification process.

- 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 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
- Current holder of one or more nationally recognized pen testing certifications is highly desired, for example:
    - Offensive Security Certified Professional (OSCP)
    - Offensive Security Certified Expert (OSCE)
    - SANS GIAC Penetration Tester (GPEN)
    - SANS GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

Note: Candidates who do not have the required certifications must have the offensive mindset and technical skills required for these certifications.

By the completion of the CQI training, candidates must demonstrate pen testing skills that align with the requirements outlined in this document, and write a report that identifies technical requirement gaps.