CYBER ASSESSMENT FACT SHEET
Risk and Vulnerability Assessment

February 2022

OVERVIEW

CISA's Risk and Vulnerability Assessment (RVA) is a one-on-one engagement with stakeholders. RVAs combine open-source national threat and vulnerability information with data that the CISA RVA team collects through remote and onsite stakeholder assessment activities. The team uses this combined information collection to provide the customer with an actionable risk analysis report containing remediation recommendations prioritized by severity and risk.

RVA service includes:

- **Penetration Testing** to determine susceptibility to an actual attack by infiltrating the target environment, using current, real-world tactics, techniques, and procedures. Specific types of testing and assessments include network, web application, wireless, war dial, and social engineering in the form of an email phishing campaign.
- **Configuration Review** of operating system and database settings and configurations—which the team compares to industry standards, guidelines, and best practices—to identify security issues.

OBJECTIVES

- Identify weaknesses through network, system, and application penetration testing.
- Test stakeholders, using a standard, repeatable methodology to deliver actionable findings and recommendations.
- Analyze collected data to identify security trends across all RVA stakeholder environments.

PHASES

Pre-Planning	Planning	Execution	Post-Execution
Stakeholder: • Requests service. • Receives RVA briefing. • Signs and returns documents.	**CISA:** • Confirms schedule. • Establishes stakeholder trusted points of contact. • Determines RVA services, scope, and logistics with stakeholder.	**CISA:** • Performs one-week external testing. • Performs one-week internal testing.	**CISA:** • Briefs initial findings. • Provides final review and report within 10 days of RVA completion. • Follows up with stakeholder on remediation actions.

HOW TO GET STARTED

Contact vulnerability@cisa.dhs.gov to get started. Please keep in mind:

- CISA's assessments are available to both public and private organizations at no cost.
- Service availability is limited; service delivery timelines are available upon request. CISA prioritizes service delivery queues on a continuous basis to ensure no stakeholder/sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.