CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Cyber Resilience Review (CRR)	External Dependency Management (EDM) Assessment	Cyber Infrastructure Survey (CIS)	Onsite Cyber Security Evaluation Tool (CSET) Assessment
Purpose and Value Proposition	Identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.	Assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.	Identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.	Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance
Scope	Critical Service view	Critical Service view	Critical Service view	Information Technology and Operational Technology systems
Time to Execute/ Availability	5 to 6 Hours / Within 2 – 4 weeks	3 – 4 Hours / Within 2 – 4 weeks	2 ½ to 4 Hours / Within 2 – 4 weeks	Varies greatly (min 2 Hours) / N/A (self-assessment)
Information Sought	Capabilities and maturity indicators in 10 security domains	Capabilities and maturity indicators across third party relationship management lifecycle domains	Protective measures in-place	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	Planning call to scope evaluation	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and utilized locally
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager, Continuity Planner, with Contract Management	IT/Security Manager	Operators, engineers, IT staff, policy/ management personnel, and subject matter experts
All Assessments Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services			

Name	Validated Architecture Design Review (VADR)	Phishing Campaign Assessment (PCA)	Vulnerability Scanning (Formally Cyber Hygiene)	Remote Penetration Test (RPT)	Network Risk and Vulnerability Assessment (RVA)
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and device relationships and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Identify public-facing Internet security risks, through service enumeration and vulnerability scanning	Perform external penetration testing and security services to identify risks and externally exploitable pathways into systems, networks and applications.	Perform penetration testing and security services to identify risks and vulnerabilities within IT systems, networks and applications
Scope	Industrial Control Systems / Network Architecture/ Network Traffic	Organization / Business Unit / Email Service	Public-Facing, Network-Based IT Service	Organization / Business Unit / Network-Based IT Service	Organization / Business Unit / Network-Based IT Service
Time to Execute / Availability	Variable (Hours to Days) / Case by case	Approximately 6 Weeks / Within 2-6 months	Continuous / Within 2-3 days	Up to 6 weeks / 3 – 6 months	Two weeks of testing / 9 – 15 months
Information Sought	Network design, system configurations, log files, interdependencies, and its applications	Phishing "click rate" metrics compared to attach sophistication	Network service and vulnerability information	Network, Database, Application scope and/or access to be tested with various security tools	Network, Database, Application scope and/or access to be tested with various security tools
Preparation	Coordinated via Email. Planning calls	Formal rules of engagement and pre-planning	Signed agreement letter and IP address scope to be tested	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and OT personnel	IT/Security Manager, Network Administrators, end users	IT/Security Manager and Network Administrators	Management stakeholders, IT/Security Manager, Network Administrators & System Owners.	Management stakeholders, IT/Security Manager, Network Administrators, and System Owners.
Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services				