Cyber Resilience Review

Description

The Department of Homeland Security (DHS) Cybersecurity Advisor (CSA) Program offers the Cyber Resilience Review (CRR) on a voluntary, no-cost basis for critical infrastructure organizations, to include state, local, tribal, and territorial governments. Through the CRR, your organization can gain insights into your operational resilience and cybersecurity capabilities.

Formats

DHS offers two options for the CRR. Trained DHS representatives can facilitate a six-hour session at a location of your choosing, or your organization can conduct a self-assessment using a downloadable tool.

Goal

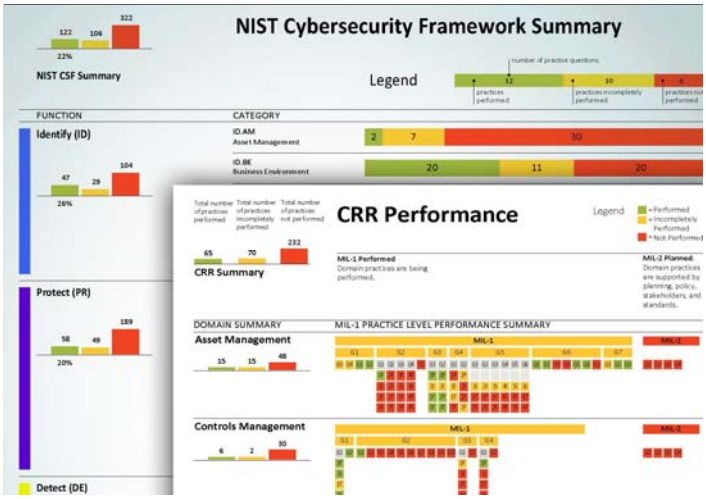
Through the CRR, your organization will develop an understanding of its operational resilience and ability to manage cyber risk during normal operations and times of operational stress and crisis.

Approach

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across 10 domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

DHS has applied and refined the CRR in supporting hundreds of CRR assessments for leading private and public organizations.



The CRR results can be used to assess your organization's capabilities against the Cybersecurity Framework.

Association to the Cybersecurity Framework

The principles and recommended practices within the CRR align closely with the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). After performing a CRR, your organization can compare the results to the criteria of the NIST CSF to identify gaps and where appropriate improvement efforts are needed. A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR self-assessment kit. An organization's assessment of CRR practices and capabilities may or may not indicate that the organization is fully aligned to the NIST CSF.

Participants

To conduct a CRR, DHS recommends that you involve a cross-functional team representing business, operations, security, information technology, and maintenance areas, including those responsible for the functions shown in the following table:

IT Policy and Governance (e.g., Chief Information Security Officer)	**Business Operations** (e.g., Operations Manager)
IT Security Planning and Management (e.g., Director of Information Technology)	**Business Continuity and Disaster Recovery Planning** (e.g., BC/DR Manager)
IT Infrastructure (e.g., Network/System Administrator)	**Risk Management** (e.g., Enterprise/Operations Risk Manager)
IT Operations (e.g., Configuration/Change Managers)	**Procurement and Vendor Management** (e.g., Contracts and Legal Support Managers)

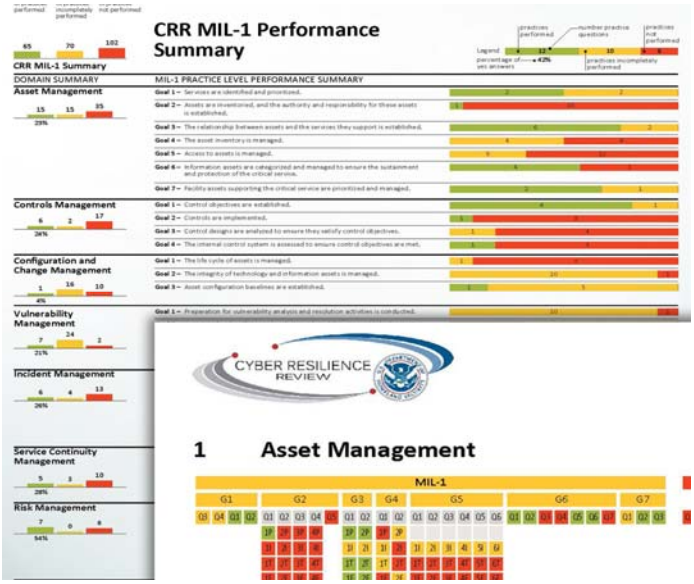
Benefits and Outcomes

Through a CRR, your organization will gain a better understanding of your cybersecurity posture. The review provides:

- An improved organization-wide awareness of the need for effective cybersecurity management
- A review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis
- A verification of management success
- A catalyst for dialog between participants from different functional areas within your organization
- A comprehensive final report that maps the relative maturity of the organizational resilience processes in each of the 10 domains, and that includes improvement options for consideration, using recognized standards and best practices as well as references to the CERT-RMM.

About the Cybersecurity Advisor (CSA) Program

CSA personnel are located in major cities throughout the United States. CSAs cultivate partnerships with and deliver services to organizations within these cities and the surrounding areas. They also act as liaisons between critical infrastructure and DHS cyber programs and leadership.



A final report will graphically map your organization's results and provides improvement options for consideration.

Data Privacy

The CRR report is created exclusively for your organization's internal use. All data collected and analysis performed during a CRR assessment is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program (www.dhs.gov/pcii). PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes.

For Information and Scheduling

The Cyber Resilience Review Assessment is facilitated by regional personnel of the Cybersecurity Advisor (CSA) Program.

Email cyberadvisor@hq.dhs.gov to schedule or receive more information on the Cyber Resilience Review and other cybersecurity resources DHS may offer.

CRR self-assessment materials can be downloaded from www.us-cert.gov/ccubedvp/.