



## CYBER RESILIENCE REVIEW

The Department of Homeland Security (DHS) offers the Cyber Resilience Review (CRR) on a voluntary, no-cost basis for critical infrastructure organizations and state, local, tribal, and territorial governments. Provided by regionally-located Cybersecurity Advisors, the CRR offers insights into an organization’s operational resilience and cybersecurity capabilities.

### FORMAT AND GOAL

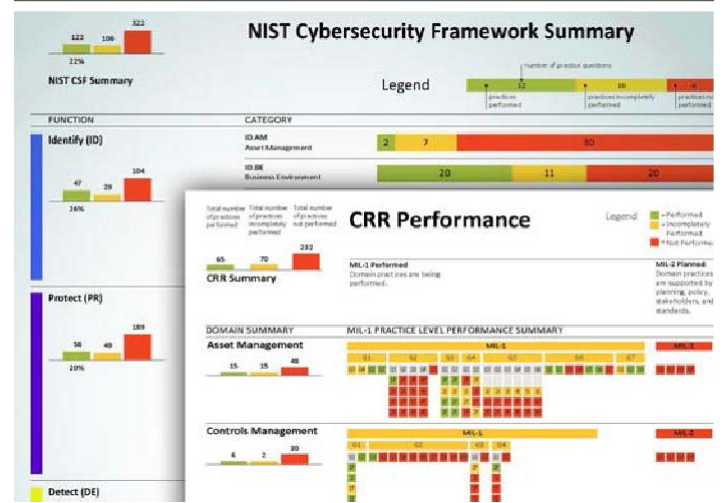
DHS offers two options for the CRR: a downloadable self-assessment and a facilitated six-hour session with trained DHS representatives at your location.

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



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

## 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)



# Homeland Security

## BENEFITS AND OUTCOMES

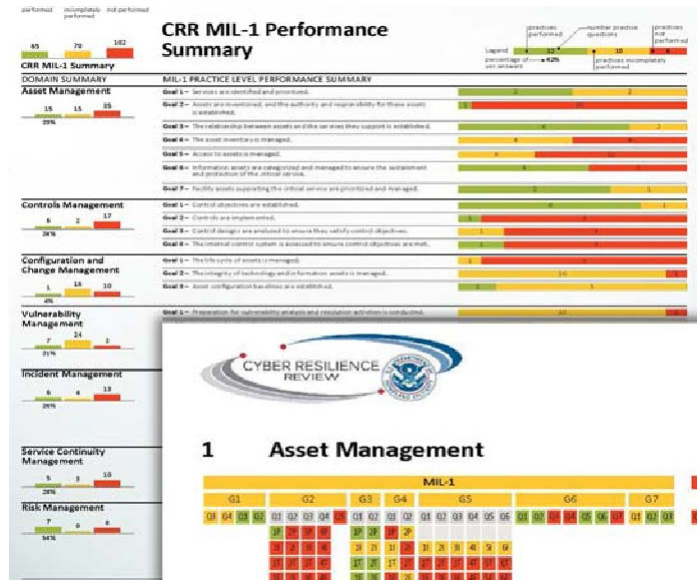
The CRR provides a better understanding of an organization's cybersecurity posture. The review provides an improved organization-wide awareness of the need for effective cybersecurity management; a review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis; a verification of management success; a catalyst for dialog between participants from different functional areas within your organization; and 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.

## 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. 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. To learn more, please visit [www.dhs.gov/pcii](http://www.dhs.gov/pcii).

## 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, recommended improvement efforts. 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.



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

## ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

For more information on DHS cyber programs, visit [www.dhs.gov/cyber](http://www.dhs.gov/cyber).

To schedule the facilitated Cyber Resilience Review or for other resources, email [cyberadvisor@hq.dhs.gov](mailto:cyberadvisor@hq.dhs.gov).

Download the CRR self-assessment at [www.us-cert.gov/ccubedvp/](http://www.us-cert.gov/ccubedvp/).