Homeland Security

Cyber Resilience Review

Frequently Asked Questions (FAQ)

Department of Homeland Security
Office of Cybersecurity and Communications
National Cyber Security Division
Cyber Security Evaluation Program
October 2011

Frequently Asked Questions

1. What is the Cyber Resilience Review (CRR)?

Answer: The CRR is a review of the overall practice, integration, and health of an organization's cyber security program. The CRR seeks to understand cyber security management of services (and associated assets) critical for an organization's mission success by focusing on protection and sustainment practices within key areas that typically contribute to the overall cyber resilience of an organization. The CRR is based on the CERT Resilience Management Model (CERT-RMM).

2. What is the goal of the CRR?

Answer: The goal of the CRR is to develop an understanding and measurement of process-based cyber security capabilities to provide meaningful indicators of an organization's operational resilience and ability to manage cyber risk to its critical services and its related assets (information, technology, resources, and personnel) during normal operations and during times of operational stress and crises.

3. What is the CERT Resilience Management Model (RMM), and how it is used in the CRR?

Answer: The CERT-RMM is a capability model developed by Carnegie Mellon University's Software Engineering Institute for managing and improving operational resilience. This model is meant to:

- Guide the implementation and management of operational resilience activities;
- Converge key operational risks management activities;
- Define maturity through capability levels;
- Enable measurement; and
- Improve confidence in how an organization responds in times of operational stress.

The CERT-RMM is composed of 26 process areas across four key categories (Enterprise Management, Operations Management, Engineering, and Process Management). The CERT-RMM provides a framework for conducting the CRR, and the domains addressed in the CRR are derived from these CERT-RMM process areas. For more information on the CERT-RMM, please visit: http://www.cert.org/resilience/rmm.html.

4. How is the CRR different from other audits, surveys, assessments, reviews, etc.?

Answer: The CRR is designed to start a constructive dialogue between the participating organization and the DHS, with the goal of cooperative improvement. The CRR…

- …is NOT a control-based audit or technical evaluation of an organization's cyber security posture;
- …is NOT meant to measure the effectiveness cyber security controls in place;
- … will NOT be used for regulatory purposes
- …does NOT satisfy compliance towards any specific regulation, standard, or model; and
- …does NOT compel an organization to take corrective action.

5. What subjects are covered during the CRR?

Answer: The CRR seeks to understand cyber security management of services (and associated assets) critical for an organization's mission success by focusing on protection and sustainment practices within ten key domains that contribute to the overall cyber resilience of an organization. These domains are:

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

Participants will be asked to identify capacities and capabilities in defining, managing, and measuring cyber security practices and behavior in each of these ten domains.

6. What are the benefits of participating in the CRR?

Answer: Benefits of participating in the CRR include:

- An opportunity for organizations to better understand their role in critical infrastructure as well as the strength of their cyber security posture in support of their mission and functions.
- Organizations benefit from a review of those capabilities that are most important to ensuring the continuity of critical services during times of operational stress.
- Organizations can verify management success and are provided with areas for targeted improvement.
- A tailored report that provides insight into an organization's cyber security management and results that identify opportunities for improvement in cyber security management to reduce operational risks related to cybersecurity.
- A DHS resource for information and insight into other NCSD programs and services.

7. Is participation in the CRR mandatory?

Answer: No, the CRR is voluntary (i.e., participation is not federally mandated).

8. Does participation in the CRR create a cost my organization?

Answer: There is no direct monetary cost to the participating organization. The organization only needs to make the appropriate personnel available to participate in the CRR.

9. What preparation is required for the CRR?

Answer: The organization will be asked in advance of the on-site visit to:

- Provide a list (with their name, title, and email) of the CRR participants;
- Participate in a conference call(s) to discuss the service-based aspect of the CRR in order to determine an appropriate scope; and
- Complete a CRR Preparation Questionnaire related to the ten domains covered in the CRR.

10. Which organizations can participate in the CRR?

Answer: Organizations within Critical Infrastructure and Key Resources (CIKR) sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments, within the United States (and its territories). The DHS National Infrastructure Protection Plan (NIPP) identifies the 18 CIKR sectors. The CRR is one tool utilized by the DHS to better understand the protection levels of the CIKR entities required to guard and sustain cyber assets that contribute to the Nation's critical infrastructure. For more information on the NIPP, please visit: http://www.dhs.gov/files/programs/editorial_0827.shtm.

11. Which personnel from my organization should participate in the CRR?

Answer: The CRR seeks participation from key cyber security personnel. These may include personnel serving in the following roles within their organization:

- Chief Information Officer (CIO);
- Chief Information Security Officer (CISO);
- Chief Security Officer (CSO);
- Chief Technology Officer (CTO);
- Director of Information Technology (IT); and/or
- Those responsible for the management of IT Security, IT Operations, and Business Continuity.

12. How long does it take to conduct the CRR?

Answer: The CRR requires one business day (typically 6 – 8 hours) to execute the on-site portion.

13. Where is the CRR conducted?

Answer: The CRR is conducted in a conference room at an on-site location specified by the participating organization. The team conducting the CRR will travel to the organization's designated site.

14. Who conducts the CRR?

Answer: The CRR is conducted by representatives from the Cyber Security Evaluation Program (CSEP) within DHS' National Cyber Security Division (NCSD), as well as representatives from the Carnegie Mellon University (CMU) Software Engineering Institute (SEI). The CRR team typically consists of one CSEP member and one CMU SEI member.

15. Does the CRR require my organization to suspend or terminate any active operations?

Answer: No. There is no need for organizations to suspend or terminate operations to participate in a CRR. The on-site portion of the CRR is designed to be non-intrusive, and there is no need for personnel within the organization to travel to participate in the CRR.

16. Does the CRR probe or scan my systems and network?

Answer: No. The CRR does not require access to networks; and technical probing, scanning, and testing of an organization's networks and systems are **not** performed as part of the CRR. However, evidence of such testing performed by the organization may be valuable to substantiate responses to the CRR questions.

17. What happens after the CRR?

Answer: DHS will review and analyze the results and produce a CRR report containing the following:

- Maturity Indicator Levels by Domain;
- CRR questions and the organization's responses by Domain;
- Options for consideration aimed at providing general guidelines or activities as to how the organization can improve its cyber security posture and preparedness; and
- A list of applicable resources.

If desired, CSEP can explain the reports and its results to the organization via a conference call, or return on-site to conduct an out-brief or follow-up review.

18. How long after the CRR can our organization expect a report?

Answer: A draft version of CRR Report is delivered within 45 calendar days after the on-site execution to the organization's designated Point of Contact for review. If DHS does not receive comments within thirty days of the delivery of the draft report, we will finalize and certify the report as PCII, and subsequently issue a final CRR Report to the organization.

19. Can I share my CRR Report with other individuals, organizations, or third parties?

Answer: Yes, the decision to share your organization's CRR Report is up to each individual organization.

20. Does DHS offer any protections for the information provided during the CRR?

Answer: All information provided during the CRR is afforded protections under the DHS Protected Critical Infrastructure Information (PCII) Program. DHS cannot disseminate information designated as PCII, and this information is not subject to Freedom of Information Act requests, State and local disclosure laws, and use in civil litigation. PCII cannot be used for regulatory purposes and can only be accessed only in accordance with strict safeguarding and handling requirements. For more information, please visit: http://www.dhs.gov/pcii. DHS employees (and its contractors) handling information designated as PCII are certified as a PCII Authorized Users. CRR Reports are typically delivered in a password-protected PDF via email, with the password separately transmitted.

21. Does DHS retain or share the information provided during the CRR?

Answer: DHS retains data collected during the CRR (and CRR Report generated as a result of that data) in order to enhance the CRR program and enable analysis of results to produce aggregated National, regional, or sector-level reporting. As the data gathered during the CRR is protected under the DHS PCII Program, DHS will ensure that any aggregated reports are not attributable to specific organizations (i.e., participant names, and their organizations, will not be identified).

22. Who do I contact for CRR-related questions or concerns?

Answer: Please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov.