U.S. DEPARTMENT OF
ENERGY

Office of Electricity Delivery
and Energy Reliability

Cybersecurity Capability Maturity Model (C2M2)

Cybersecurity Capability Maturity Model (C2M2)
Frequently Asked Questions

1) *What is the C2M2 model?*

   The C2M2 is a voluntary evaluation process utilizing industry-accepted cybersecurity practices that can be used to measure the maturity of an organization's cybersecurity capabilities. The C2M2 is designed to measure both the sophistication and sustainment of a cyber security program. The model was identified, organized, and documented by energy sector subject matter experts from both public and private organizations.

2) *What is the goal of the C2M2?*

   The goal of the C2M2 is to develop an logical understanding and measurement of the policies, processes, and procedures involved in the development of an organization's cyber security posture. The model provides maturity indicator levels (MILs) designed to discuss an organization's operational capabilities and management of cybersecurity risk during both normal operations and times of crises.

3) *How is the C2M2 different than other audits, surveys, or reviews? Is the C2M2 a regulatory requirement?*

   The C2M2 is a voluntary public-private partnership program, the development of which is not associated with any compliance requirements. There is no intent or desire for use of the maturity model to be regulated.

   The C2M2 self-assessment is not an audit, controls assessment, or a penetration test. The model is used to evaluate the maturity and sophistication of the organization's cybersecurity risk management approach at a strategic and holistic level.

   The C2M2 model document is publicly available on the DOE website and may be adopted by any organization. Moreover, the C2M2 toolkit files are also provided by DOE upon request The DOE offers C2M2 facilitated self-assessments as a free service for the energy sector organizations. These facilitated self-assessments are not a DOE requirement.

4) *Does the Department of Energy collect or use the information discussed or generated during a facilitated self-assessment?*

   No, DOE does not record or retain any information or results from C2M2 facilitated self-assessments. DOE prefers to run the C2M2 toolkit on the private sector organization's laptop. We are currently seeking feedback from the energy sector regarding the value of benchmarking data across the body of C2M2 participants.

5) *How does the C2M2 model align with the Risk Management Process Guideline (RMP)?*
Both the RMP and the C2M2 are tools developed by the DOE with public-private partnerships. These documents map to the Department's goal of strengthening assessing and monitoring of risks; and are specifically tailored for the unique and diverse organizations of the electric sector.

The RMP guideline provides a scalable process for framing, assessing, responding, and monitoring risks whereas the C2M2 serves as a tool for evaluating the maturity of the organizations cyber security capabilities. This awareness of maturity level across different areas enables organizations to apply their cyber security risk management process and investment in weak areas.

6) *What subjects are covered in a C2M2 evaluation?*
The C2M2 seeks to understand the cybersecurity capabilities across an organization’s mission by focusing on practices within ten key domains that contribute to the overall cyber security posture of an organization. These domains are:

- Risk Management
- Asset, change, and configuration management
- Identity and access management
- Threat and vulnerability management
- Situational Awareness
- Information sharing and communications
- Event and incident response, continuity of operations
- Supply chain and external dependencies management
- Workforce management
- Cybersecurity program management

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

7) *Who from my organization should participate in a C2M2 self-assessment?*
An C2M2 evaluation requires participation of representative(s) from the organization’s cybersecurity team that can speak to the practices in each of the ten domains listed above. The participants will need to have management level knowledge of their function/departments’ practices. Key cybersecurity personnel may also include the:

- 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, Business Continuity, and other relevant business functions. For the electricity subsector, this may include Distribution/Transmission/Generation Operations. For the oil and natural gas subsector, this would include relevant down/mid/upstream operations.

8) *What should my organization expect with regard to a DOE facilitated C2M2 self-assessment meeting?*

- The DOE team will coordinate logistics and schedule ahead of time. The team will also answer any questions that the organization has with regard to the day of the facilitated self evaluation
- A 2-3 member team of DOE employees and contractors will visit your organization.
- The site visit will be a one-full-day (typically 6-8 hours) activity and require minimal preparation. Unlike evidence based audits, the C2M2 evaluation is based on interviews with the relevant stakeholders. The only preparation required is reading the C2M2 model document.
- The meeting will comprise of the different stakeholders answering questions relevant to their functions. The C2M2 has over 300 questions in total which will generate dialogue between the participants and help the stakeholders understand the maturity of the cybersecurity capabilities.
- Organization will have to arrange for a laptop, projector and internet access.
  - If a DOE laptop is used, the data is deleted at the end of the day.
  - DOE Team will not collect or retain any evaluation data.
- At the end of the day a C2M2 report will be generated that will provide the organization with a visual analysis on the maturity of its cybersecurity program.

9) *Is there more guidance for self-assessments without a DOE facilitator?*

DOE, in partnership with Carnegie Mellon University, has produced a Facilitator’s Guide for the C2M2. It can be accessed at the main C2M2 site, found here: energy.gov

10) *What happens after a DOE facilitated C2M2 self-assessment?*

DOE will work with the organization to review the results and immediately produce a C2M2 report containing the organization’s C2M2 results across the ten domains. The report will also provide relevant resources to help mitigate process gaps and help with programmatic cybersecurity improvements.

11) *Who should I contact for more information on the C2M2?*

Please email the C2M2 support team at C2M2@doe.gov.