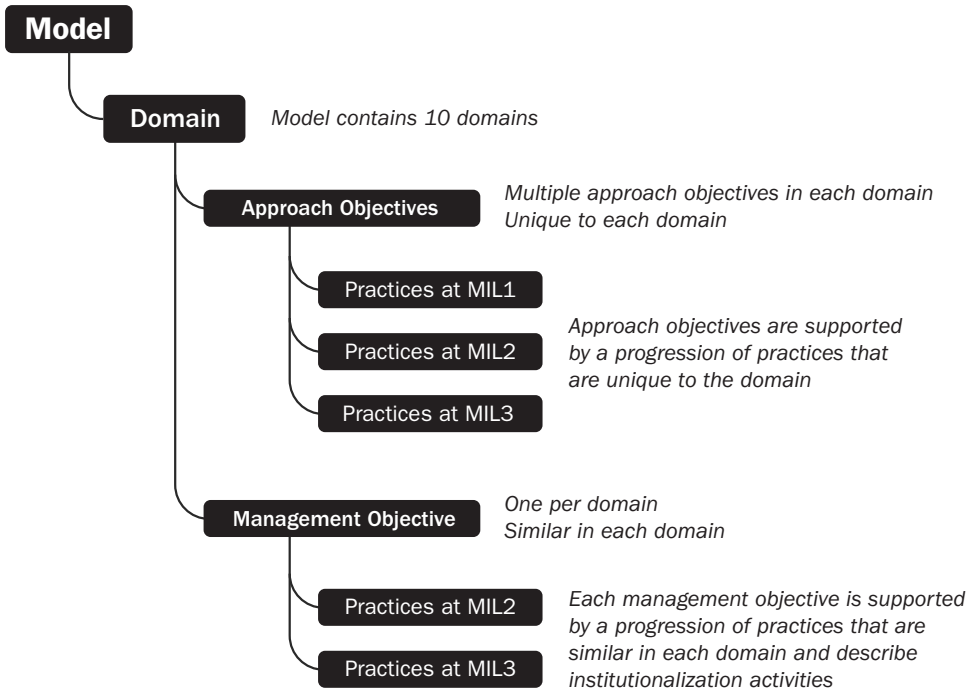
Version 2.1 Self-Evaluation Cheat Sheet

C2M2 | Cybersecurity Capability Maturity Model

Model Architecture



Maturity Indicator Levels (MILs)

MIL0: Incomplete—MIL1 has not been achieved in the domain.

MIL1: Initiated—Initial practices are performed but may be ad hoc. Practices are performed in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of a prescribed plan, policy, or training.

MIL2: Performed—Practices are more complete or advanced than at MIL1.

- Practices are documented.
- Adequate resources are provided to support performance of the practices in the domain (people, funding, and tools).

MIL3: Managed—Practices are more complete or advanced than at MIL2.

- Activities are guided by policies (or other organizational directives).
- Responsibility, accountability, and authority for performance of the practices in the domain are assigned to personnel.
- Personnel performing the practices in the domain have adequate skills and knowledge.
- The effectiveness of activities is evaluated and tracked

Domains

Asset, Change, and Configuration Management (ASSET)
Manage the organization's IT and OT assets, including both hardware and software, and information assets commensurate with the risk to critical infrastructure and organizational objectives.

Threat and Vulnerability Management (THREAT)
Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives.

Risk Management (RISK)
Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Identity and Access Management (ACCESS)
Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

Situational Awareness (SITUATION)
Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.

Event and Incident Response, Continuity of Operations (RESPONSE)
Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.

Third-Party Risk Management (THIRD-PARTIES)
Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives.

Workforce Management (WORKFORCE)
Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

Cybersecurity Architecture (ARCHITECTURE)
Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.

Cybersecurity Program Management (PROGRAM)
Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.

Self-Evaluation Response Options

Fully Implemented
Complete; the practice is performed as written

Largely Implemented
Complete but with a recognized opportunity for improvement

Partially Implemented
Incomplete; there are multiple opportunities for improvement

Not Implemented
Absent; the practice is not performed by the organization

Scope of the Self-Evaluation

Function

This is the part of the organization that is being evaluated based on the model. A self-evaluation may be performed for an organization, an enterprise, or a subset of those.

Organization

An administrative structure of any size or complexity that is charged with carrying out an assigned mission and business processes. In the context of the model, the organization is the administrative structure in which the function selected for self-evaluation resides. The organization itself might be positioned within a broader enterprise.

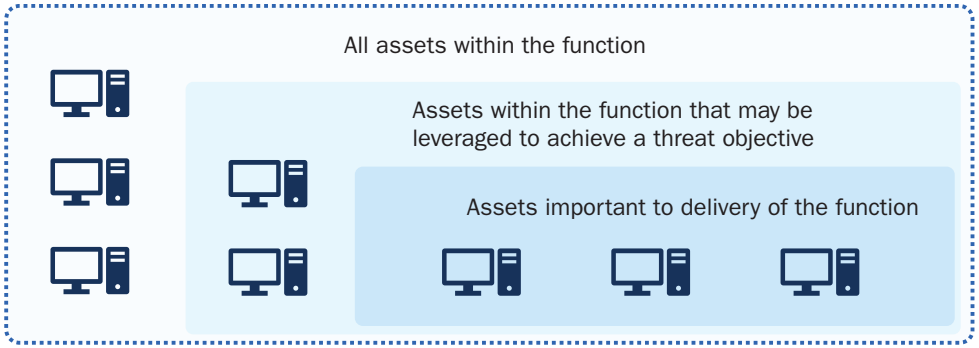
Enterprise

The largest (that is, highest level) organizational entity to which the organization participating in the C2M2 self-evaluation belongs. Some enterprises may consist of multiple organizations (e.g., a holding company with one or more operating companies). Other organizations may have a more homogeneous structure that does not necessitate any differentiation between the terms enterprise and organization. For those organizations, enterprise and organization may be used interchangeably.

How to provide responses for practices performed outside the function

Some C2M2 practices may be performed on behalf of the function by a third party or by those outside of the function. For these practices, provide a response using the normal scale of Fully Implemented, Largely Implemented, Partially Implemented or Not Implemented. In other words, focus should be placed on the level of implementation regardless of whether the practice is implemented by those in the function or others. To ensure accuracy, responses should be provided by someone familiar with the way in which practices are implemented.

C2M2 Asset Subgroupings



All assets within the function
All assets that operate or are used within the function. These assets may not be considered important to the delivery of the function and may not be likely to be leveraged to achieve a threat objective (for example, printers, radios, badge readers, and telephones).

Assets within the function that may be leveraged to achieve a threat objective
Assets that may be used in the pursuit of the tactics or goals of a threat actor (e.g., public-facing assets, assets with administrative rights). This extends the scope of the inventory to include assets that would be of concern when thinking from the perspective of an adversary.

Assets that are important to the delivery of the function
Assets that are required for a normal state of operation of the function and output of the function's products or services. Loss of an asset that is considered important to the delivery of the function may not directly result in an inability to deliver the function but could result in operations being degraded.

Log on to **energy.gov/c2m2** to learn more.

U.S. DEPARTMENT OF ENERGY

Office of Cybersecurity, Energy Security, and Emergency Response