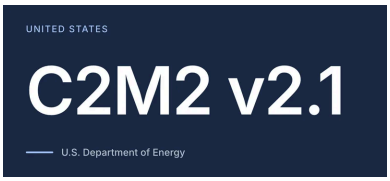
SmartSuite

Framework / Cybersecurity / C2M2

C2M2 v2.1

C2M2 v2.1 is the U.S. Department of Energy's cybersecurity capability maturity model: ten domains scored on four maturity indicator levels, MIL0 to MIL3.



What it is

The Cybersecurity Capability Maturity Model (C2M2) Version 2.1 is a voluntary maturity model from the U.S. Department of Energy that lets an organization score its cybersecurity practices across ten domains on four maturity indicator levels, MIL0 to MIL3. Version 2.1 was published in June 2022 and was developed by the U.S. energy industry, but any organization of any size can use it.

The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) publishes the model and provides a self-evaluation tool at c2m2.doe.gov, with no-cost self-evaluation support for U.S. energy organizations. Nothing in the model binds an organization legally or leads to certification.

At a glance

PUBLISHER U.S. Department of Energy (DOE)	TYPE Framework	VERSION Version 2.1
EFFECTIVE June 2022	DOMAIN Cybersecurity	FAMILY C2M2
REGION United States	INDUSTRY Energy & Utilities	ADOPTION MODEL Voluntary
IMPLEMENTATION COMPLEXITY Medium		

Source: energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Why it matters

- **Domain-by-domain scoring** The MILs apply independently to each domain, so an organization can be at MIL1 in one domain and MIL3 in another (section 4.2).
- **Targets instead of a pass mark** Organizations set a target MIL per domain, because striving for the highest level everywhere may not be optimal (section 4.2).
- **Every size can start** The model was designed so that companies of any size can achieve MIL1 across all domains (section 4.2).
- **IT and OT together** Practices address IT, OT and information assets, which matters for energy, utilities and industrial operators (section 3.3).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports C2M2 v2.1

Ten-Domain Practice Library

Load the ten domains with their objectives and practices as linked records, each carrying its MIL level.

Self-Evaluation Scoring

Record the response for each practice, such as Fully Implemented or Largely Implemented, and roll it up to a MIL per domain.

Target MIL and Gap Analysis

Set a target MIL for each domain and list the practices that separate the current from the target level.

Improvement Plan and Ownership

Turn gaps into tasks with owners, milestones and due dates, and track them to closure.

Evidence for Management Practices

Attach the documents, policies and assigned responsibilities that show MIL2 and MIL3 management characteristics.

Reevaluation and Progress Reporting

Run the periodic reevaluation as a new assessment and show maturity by domain and over time on dashboards.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-171 Rev. 3 | NIST 800-53 Rev.5

Official resources

Cybersecurity Capability Maturity Model (C2M2) v2.1

Provides an official framework for evaluating and improving cybersecurity capabilities across sectors.

c2m2.doe.gov

C2M2 Implementation Guidance

Outlines best practices for implementing C2M2 in organizations to enhance cybersecurity posture.

c2m2.doe.gov/implementation-guidance

C2M2 Assessment Tools

Describes self-evaluation tools for conducting maturity assessments according to the C2M2 framework.

c2m2.doe.gov/assessment-tools

C2M2 Overview

Defines the core concepts and components of the C2M2 framework for cybersecurity improvement.

c2m2.doe.gov/overview

Frequently asked questions

What is the C2M2 and who publishes it?

The Cybersecurity Capability Maturity Model is a voluntary maturity model published by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response. Version 2.1 was released in June 2022 and was developed by the U.S. energy industry.

What are the ten C2M2 domains?

ASSET, THREAT, RISK, ACCESS, SITUATION, RESPONSE, THIRD-PARTIES, WORKFORCE, ARCHITECTURE and PROGRAM, covering asset and configuration management, threat and vulnerability management, risk management, identity and access management, situational awareness, incident response and continuity, third-party risk, workforce, cybersecurity architecture and program management.

What do the maturity indicator levels mean?

MIL0 means practices are not performed and MIL1 means initial practices are performed, possibly ad hoc. At MIL2 practices are documented and adequately resourced, and at MIL3 activities are guided by policy, responsibility is assigned, staff have the skills and effectiveness is tracked. Levels are cumulative and rated per domain (section 4.2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Is C2M2 mandatory or certifiable?

No. It is a voluntary self-evaluation model with no certification. The Department of Energy offers no-cost self-evaluation support to U.S. energy sector organizations, and any organization can use the model.

How do you use C2M2 in practice?

The model describes four steps: perform a self-evaluation, analyze the identified gaps, prioritize and plan, then implement plans and periodically reevaluate (sections 5.1 to 5.4). Organizations set a target MIL for each domain instead of aiming for the highest level everywhere.

License included / downloadable: Yes The C2M2 model and self-evaluation tool are published free by the U.S. Department of Energy and are included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/c2m2-v21-cybersecurity-capability-maturity-model

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.