SmartSuite

Framework / Cybersecurity / C2M2

C2M2 v2.1

C2M2 is a maturity model that helps organizations assess and improve their cybersecurity capabilities and risk management.

What it is

C2M2 v2.1 (Cybersecurity Capability Maturity Model) is a cybersecurity maturity assessment framework that enables organizations to evaluate and improve their cybersecurity capabilities across multiple operational domains. The model provides a structured approach for identifying strengths and gaps in cybersecurity practices, supporting continuous improvement and risk management.

Developed and published by the U.S. Department of Energy, C2M2 is aimed at critical infrastructure sectors, such as energy, but is broadly applicable to organizations seeking to enhance their cybersecurity posture. The model covers key areas including risk management, incident response, asset and information management, and supply chain security, and can complement other standards like NIST Cybersecurity Framework or ISO 27001.

At a glance

PUBLISHER U.S. Department of Energy (DOE)	TYPE Framework	VERSION C2M2 v2.1
EFFECTIVE 2016	DOMAIN Cybersecurity	FAMILY C2M2
REGION United States	INDUSTRY Energy & Utilities	ADOPTION MODEL Risk Management
IMPLEMENTATION COMPLEXITY Moderate		

Source: https://c2m2.doe.gov/

Why it matters

- **Strengthen cybersecurity governance** Establish consistent practices for oversight and accountability across operational areas, improving decision-making at all organizational levels.
- **Improve risk management effectiveness** Support identification and prioritization of cybersecurity risks, enabling targeted risk reduction initiatives and better resource allocation.
- **Enhance supply chain security** Address third-party risks by assessing and improving vendor and supply chain cybersecurity practices aligned with industry benchmarks.
- **Support regulatory and audit readiness** Align internal controls with industry standards, simplifying compliance efforts and preparing organizations for regulatory reviews or audits.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports C2M2 v2.1

Capability Assessments by Domain
Run maturity assessments across C2M2 domains with consistent scoring.

Improvement Roadmap and Ownership
Turn gaps into a prioritized roadmap with owners, milestones, and deadlines.

Evidence and Practice Documentation
Attach proof that practices are performed and repeatable across teams.

Maturity Progression Tracking
Track maturity progression over time with measurable indicators.

Risk-Based Prioritization
Link improvements to mission impact and risk to focus investment.

Executive Reporting
Provide leadership reporting on maturity, gaps, and progress.

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 C2M2 v2.1 used for?
C2M2 v2.1 is used to assess and improve the maturity of an organization’s cybersecurity capabilities. It helps organizations identify strengths and weaknesses across cybersecurity domains, informing risk management and strategic security planning.

Is C2M2 v2.1 a mandatory or certifiable framework?
C2M2 v2.1 is a voluntary assessment tool and does not offer formal certification. It is not mandated by law but is widely adopted in critical infrastructure sectors to support compliance with other regulatory and cybersecurity standards.

Who should use C2M2 v2.1, and what is its scope?
C2M2 v2.1 is designed for organizations within critical infrastructure sectors—such as energy, utilities, and related industries—but is applicable to any organization aiming to enhance cybersecurity maturity. Its scope covers risk management, incident response, asset management, and supply chain security.

What are the key domains and maturity indicators in C2M2 v2.1?
C2M2 v2.1 covers domains such as risk management, situational awareness, cybersecurity program management, and others. The model uses defined maturity indicator levels (MILs) to measure cybersecurity capabilities, offering a structured progression from foundational to advanced practices.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How is C2M2 v2.1 implemented in organizations?

Organizations implement C2M2 v2.1 by conducting baseline assessments using the model's criteria, scoring maturity levels across each domain, and performing gap analyses. Results are used to prioritize improvements, allocate resources, and integrate cybersecurity enhancements into governance processes.

How does C2M2 v2.1 relate to frameworks like NIST CSF or ISO 27001?

C2M2 v2.1 is complementary to other frameworks such as NIST CSF and ISO 27001, providing a sector-specific focus and maturity-based approach. Organizations often use C2M2 alongside these frameworks to guide the development and maturity of their cybersecurity programs.

What are the ongoing compliance requirements for C2M2 v2.1?

Maintaining alignment with C2M2 v2.1 involves regular maturity assessments, continuous monitoring of controls, and periodic reviews of cybersecurity program progress. Organizations must document improvements, track risk mitigation activities, and update governance practices as new threats and technologies emerge.

How would SmartSuite support C2M2 v2.1?

SmartSuite streamlines C2M2 v2.1 management by enabling organizations to import control libraries, track risks centrally, and manage control implementation. The platform supports evidence collection, ensures audit readiness, and automates remediation workflows, while providing dashboards and reporting to facilitate compliance monitoring and executive oversight.

License included / downloadable: Yes The C2M2 framework is published by the U.S. Department of Energy and is publicly available through official DOE resources.

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

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.