



CROSSROADS • ISSUE 3 • JUNE 20, 2026 • ~24 MIN READ

Five Maturity Models, One Question: Which One Actually Tells You Whether Your OT Cybersecurity Program Is Strong?

1. Why the framework you pick changes the answer
2. C2M2 — the DOE energy-sector reference
3. CMMC 2.0 — the federal procurement gate
4. ISA/IEC 62443 — the parts you actually need
5. MILs — the underlying capability-maturity construct
6. SANS ICS 5 Critical Controls — the threat-driven outcomes framework
7. Side-by-side: what each model does and does not measure
8. The strongest maturity model for OT
9. How to analyze a company's OT cybersecurity maturity level
10. Three observations CIP Sentinel takes from comparing the five
11. Sources

Why the framework you pick changes the answer

"Maturity" in cybersecurity is a loaded word. In the SSE-CMM lineage it means how well a process is performed, documented, managed, and continuously improved — not whether a particular control exists. In CMMC parlance it means whether a contractor has implemented a specified list of NIST 800-171 or 800-172 practices well enough to pass an assessment. In SANS parlance it means whether your program would actually slow down or stop the attacks the community has already seen in the field. Three different definitions of the same word, all reasonable, none interchangeable.

That definitional drift matters because the model you choose determines the answer you get. A company with a score of MIL2 across all ten C2M2 domains and a passing CMMC Level 2 self-assessment can still have no ICS-specific incident-response plan, no defensible network architecture, no protocol-aware OT monitoring, and no inventory of remote-access pathways into the control system — which is to say, can still fail every one of the SANS ICS 5 Critical Controls. The C2M2 + CMMC pairing answers "is the management system in place?" The SANS Five answer "would the management system actually stop a real OT attack?" Both questions are worth asking. They are not the same question.

C2M2 — the DOE energy-sector reference

The [Cybersecurity Capability Maturity Model](#)¹ was developed in 2012 by the U.S. Department of Energy with industry input and is now maintained by the [Office of Cybersecurity, Energy Security, and Emergency Response](#)². Version 2.1 is the current release. It is free, self-administered, and explicitly designed to evaluate both IT and OT cybersecurity practices across critical infrastructure.



The model is structured around 10 domains: 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; and Cybersecurity Program Management. Each domain contains practices grouped into objectives, and each practice is scored against a Maturity Indicator Level scale.

The MIL scale in C2M2 v2.1, per the [official DOE cheat sheet](#)³, has four levels: MIL0 (Incomplete — MIL1 has not been achieved in the domain); MIL1 (Initiated — initial practices are performed but may be ad hoc, depending on individual initiative); MIL2 (Performed — practices are documented and adequately resourced); and MIL3 (Managed — practices are guided by policy, performance objectives are defined, governance is in place, and practices are reviewed for effectiveness). A handful of secondary write-ups incorrectly cite five MILs in C2M2; the DOE reference is the authoritative count.

C2M2 is the right answer when the question is “where is our enterprise cybersecurity program weakest, by domain, today?” It is widely used, well-instrumented, free, and has been adapted into sector-specific variants — the Dams Sector C2M2 (Dams-C2M2), the Oil and Natural Gas C2M2 (ONG-C2M2), and the Electricity Subsector C2M2 (ES-C2M2) are published examples. It is not designed to answer “would we catch a live Volt Typhoon implant on a substation jump host?”

CMMC 2.0 — the federal procurement gate

The Cybersecurity Maturity Model Certification program exists for one reason: the U.S. Department of Defense wanted a verifiable cybersecurity posture across the defense industrial base before awarding contracts that involve Federal Contract Information or Controlled Unclassified Information. The current iteration is CMMC 2.0, codified in [32 CFR Part 170](#)⁴, which was published in the Federal Register on October 15, 2024 and became effective December 16, 2024. The companion DFARS rule (48 CFR) that puts CMMC into actual contract clauses became effective [November 10, 2025](#)⁵, kicking off a four-phase rollout that runs through November 10, 2028.

CMMC 2.0 has three levels:

- Level 1 (Foundational) — 17 basic safeguarding practices from FAR 52.204-21. Required for contractors handling only Federal Contract Information. Annual self-assessment.
- Level 2 (Advanced) — 110 practices from NIST SP 800-171 Rev 2. Required for contractors handling Controlled Unclassified Information. Either self-assessment or assessment by a CMMC Third-Party Assessment Organization (C3PAO) depending on contract sensitivity.
- Level 3 (Expert) — the Level 2 baseline plus 24 selected NIST SP 800-172 controls. Required for contractors handling the most sensitive CUI. Assessed by the DoD’s Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every three years.

CMMC is not an OT-specific model. It is a general-purpose information-security gate written around 800-171 and 800-172, both of which were designed for IT-centric CUI protection in the defense supply chain. Its relevance to a NERC-regulated utility is indirect — most U.S. transmission and generation operators are not DoD contractors at the bulk-power level — but it matters for two reasons. First, several large utilities have defense-contract entities (research divisions, security-equipment supply, IT services to DoD bases) that pull CMMC inside the enterprise boundary, and 32 CFR Part 170 flows down through subcontracts. Second, the rest of the federal procurement world is increasingly mirroring the CMMC structure: GSA, DHS, and DOE acquisition programs are watching CMMC’s assessment ecosystem closely and may extend its model to non-DoD critical-infrastructure contracts in time.



CMMC 2.0 is the right answer when the question is “can our company legally bid on this DoD contract?” It is not the right answer to any OT defensive-posture question.

ISA/IEC 62443 — the parts you actually need

The [ISA/IEC 62443 series](#)⁶ is the only consensus-based international standard family dedicated to the cybersecurity of Industrial Automation and Control Systems. The series is organized into four groups — General (62443-1-x), Policies and Procedures (62443-2-x), System (62443-3-x), and Component (62443-4-x) — and addresses four stakeholder roles: asset owners, product suppliers, system integrators, and maintenance service providers. Treating 62443 as a single monolithic standard is the most common mistake practitioners make when they first encounter it. The five parts below are the ones that do useful work in an asset-owner maturity assessment; the rest of the catalog supports them.

Part	Audience	What it does for a maturity assessment
62443-2-1:2024	Asset owner	Security program requirements for the asset owner’s own IACS cybersecurity management system. The 2024 revision introduces a 4-level maturity scale (Initial, Managed, Defined/Practiced, Improving) for measuring conformance to each Security Program Element. This is the asset-owner anchor of the family.
62443-2-4	Service provider (integrators, maintainers)	Security program requirements for IACS service providers across 12 functional areas (assurance, architecture, wireless, security engineering systems, configuration management, remote access, event management & logging, user management, malware protection, patch management, backup & recovery, project staffing). Annex A scores each requirement on a 4-level maturity scale. Use this to set contract language and audit your integrators.
62443-3-3	System level (asset owner + integrator)	System security requirements and Security Levels (SL 0–4). Defines the seven Foundational Requirements (Identification and Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events, Resource Availability). This is where the asset owner picks a target SL for a control system and an integrator demonstrates how it was achieved.
62443-4-1	Product supplier	Secure product development lifecycle requirements for IACS product suppliers: threat modeling, secure design, secure implementation, security verification and validation testing, defect management, patch management, product end-of-life. This is the part to cite in OEM RFPs when you want evidence that the device firmware you are about to deploy was developed under a credible SDLC.



Part	Audience	What it does for a maturity assessment
62443-4-2	Product supplier (technical)	Technical security requirements for IACS components: embedded devices, network devices, host devices, software applications. Translates the 62443-3-3 Foundational Requirements into device-level capabilities so a PLC, HMI, or switch can be certified against a target Security Level (ISASecure CSA certification is built on this part).

The Security Level construct in 62443-3-3 is the one most often confused with a maturity model. It is not. Security Levels (SL 0–4) describe the strength of the threat the system is intended to resist; they are not a measure of how well a process is performed.

- SL 0 — no special protection required.
- SL 1 — protection against casual or coincidental violation.
- SL 2 — protection against intentional violation using simple means with low resources, generic skills, low motivation.
- SL 3 — protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, moderate motivation.
- SL 4 — protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, high motivation (the nation-state envelope).

The maturity question for 62443 is therefore two-dimensional: which Security Level is the system targeted at (a design choice), and how mature is the program around the Security Level decision (the 4-level scale in 2-1 and 2-4 Annex A). Both numbers matter. A program that targets SL 3 for a substation control system but executes the 2-1 program at maturity level 1 is fooling itself.

The five parts above are enough to cover an asset owner’s realistic 62443 exposure: 2-1 for the asset owner’s own program, 2-4 for service-provider contracts, 3-3 for system-level Security Level targeting, and 4-1/4-2 for OEM and component diligence. The rest of the catalog — 62443-1-1 (concepts and models), 62443-2-3 (patch management), 62443-2-2 (program implementation guidance), 62443-3-2 (security risk assessment for system design) — is useful supporting reference material but not where an asset owner’s maturity score lives.

MILs — the underlying capability-maturity construct, not a standalone model

The user’s short list referred to MILs as if they were a separate model. They are not. Maturity Indicator Levels are the underlying capability-maturity scoring construct, inherited from the ISO/IEC 21827 Systems Security Engineering Capability Maturity Model (SSE-CMM), that several models embed inside themselves to score practices.

The clearest way to think about it: C2M2 uses MILs (0–3). 62443-2-1:2024 uses four maturity levels (1–4) that are functionally equivalent. 62443-2-4’s Annex A scores each requirement on the same 4-level scale. The original CMMC 1.0 used five maturity levels until DoD compressed the model into the three-level CMMC 2.0. Even Dams-C2M2, ONG-C2M2, and ES-C2M2 all use the same MIL construct.

The reason MILs keep showing up is that they answer a question simple checklists cannot: how well is this practice performed, not just whether it is performed. A MIL2 practice is documented and adequately resourced. A MIL3 practice is also governed by policy, has defined performance objectives, and is reviewed for effectiveness. That progression maps cleanly to the lived experience of OT program



managers — first you do the thing, then you write it down, then you measure whether the writing-it-down is making things better — which is why the MIL idea has survived four decades of cybersecurity-framework churn.

SANS ICS 5 Critical Controls — the threat-driven outcomes framework

The [Five ICS Cybersecurity Critical Controls](#)⁷, published by SANS in November 2022 by Robert M. Lee and Tim Conway, is a deliberate counterpoint to checklist-driven maturity frameworks. The whitepaper opens with a finding that on average 60–95% of the guidance in well-known cybersecurity frameworks is preventive in nature, and argues that ICS environments need a smaller, threat-informed set of controls that account for adversary tradecraft observed in real industrial attacks.

The five controls are:

1. ICS-specific Incident Response Plan — operations-informed IR plan that prioritizes system integrity and recovery during an attack, with exercises tailored to ICS scenarios.
2. Defensible ICS Network Architecture — architectures that support visibility, log collection, asset identification, industrial DMZs, and process-communication enforcement.
3. ICS Network Visibility and Monitoring — continuous network security monitoring of the ICS environment with protocol-aware toolsets and system-of-systems interaction analysis.
4. ICS Secure Remote Access — identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host capabilities used to inform operations of potential risks.
5. Risk-Based ICS Vulnerability Management — understanding cyber digital controls in place and device operating conditions to inform risk-based vulnerability decisions to patch, mitigate impact, or monitor for exploitation.

SANS' framing is explicit that these are minimums for community and national security, derived from the attacks that have already been seen in the field — not aspirational targets. The Five Controls are designed to be implemented in order: an IR-driven strategy first, then the architecture and monitoring needed to execute it, then the access controls and vulnerability management that compound the value of the first three.

The SANS Five do not include a maturity-scoring rubric in the whitepaper. Dragos' [OT Cybersecurity Benchmarking Guide](#)⁸ overlays a three-stage progression on the Five Controls — Implement (foundational controls), Operationalize (key use cases and integration with IT security), and Optimize (risk-based investment tuning and expanded coverage). That overlay is what most practitioners use when they need to put a maturity number on top of the SANS framework.

Side-by-side: what each model does and does not measure

The table below lines up the five frameworks against the dimensions practitioners care about. The point of the comparison is not that any one model is uniformly better — it is that the models are answering different questions and the right one depends on what you are being asked to demonstrate.



Publisher

C2M2 v2.1	U.S. DOE CESER
CMMC 2.0	U.S. DoD (32 CFR Part 170)
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	ISA + IEC TC65
MILs (as construct)	Originated in ISO/IEC 21827 SSE-CMM
SANS ICS 5 Critical Controls	SANS Institute

Primary audience

C2M2 v2.1	Energy-sector asset owners; any CI operator
CMMC 2.0	U.S. defense-industrial-base contractors
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	All four IACS roles (asset owner, service provider, system integrator, product supplier)
MILs (as construct)	Any framework that needs capability scoring
SANS ICS 5 Critical Controls	ICS/OT asset owners and defenders

OT-specific?

C2M2 v2.1	Yes — explicitly covers IT and OT
CMMC 2.0	No — IT-centric (800-171 / 800-172)
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	Yes — designed for IACS
MILs (as construct)	Construct only — no OT-specific content
SANS ICS 5 Critical Controls	Yes — purpose-built for ICS/OT

Scale used

C2M2 v2.1	MIL0-MIL3 (4 levels)
CMMC 2.0	Level 1, 2, 3
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	2 axes: SL 0-4 (threat strength) + 4-level maturity (program quality)
MILs (as construct)	Variable; typically 4 (1-4) or 5 (0-4)
SANS ICS 5 Critical Controls	None native; Dragos overlay uses 3 stages



Scope

C2M2 v2.1	10 domains spanning enterprise cyber program
CMMC 2.0	17 / 110 / 110+24 practice sets
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	Full IACS lifecycle: asset-owner program (2-1), service-provider capabilities (2-4), system security (3-3), product SDLC (4-1), component technical reqs (4-2)
MILs (as construct)	Scoring layer; no scope of its own
SANS ICS 5 Critical Controls	5 outcome-focused controls

Assessment

C2M2 v2.1	Self-assessment, free toolkit
CMMC 2.0	Self / C3PAO / DIBCAC depending on level
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	Self + third-party certification (ISASecure for 4-1/4-2 and CSA component cert)
MILs (as construct)	Whatever the host framework specifies
SANS ICS 5 Critical Controls	Self-assessment, often via Dragos benchmarking guide

Cost

C2M2 v2.1	Free
CMMC 2.0	Self-assessment free; C3PAO/DIBCAC paid
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	Standard documents paid; ISASecure cert paid
MILs (as construct)	Free construct
SANS ICS 5 Critical Controls	Free whitepaper; Dragos guide free

Legally binding?

C2M2 v2.1	No
CMMC 2.0	Yes — DoD contract condition starting Nov 10, 2025
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	Voluntary unless cited in a contract or regulation
MILs (as construct)	No
SANS ICS 5 Critical Controls	No



Threat-informed?

C2M2 v2.1	Indirectly — via threat & vuln mgmt domain
CMMC 2.0	No — control-list-based
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	Partially — via SL targeting
MILs (as construct)	N/A (scoring construct only)
SANS ICS 5 Critical Controls	Yes — explicitly built from observed ICS attacks

Best at answering

C2M2 v2.1	Where is our enterprise cyber program weakest by domain?
CMMC 2.0	Can we legally bid on this DoD contract?
ISA/IEC 62443 (2-1, 2-4, 3-3, 4-1, 4-2)	What threat strength is this system designed to resist, and is the surrounding program mature enough to maintain it?
MILs (as construct)	How well is this individual practice performed?
SANS ICS 5 Critical Controls	Would our defenses actually stop a real OT attack?

Where the models overlap is in the SSE-CMM lineage. C2M2's MILs, 62443-2-1's and 2-4's maturity levels, the original CMMC 1.0's five-level scale, and the Dragos overlay on the SANS Five all use some form of "ad hoc → documented → managed → improving" progression. Where they diverge is in scope: C2M2 covers the whole enterprise cyber program at a domain level; CMMC 2.0 enforces a specific control list inherited from NIST 800-171 and 800-172; the 62443 parts each cover a slice of the IACS lifecycle (asset-owner program, service-provider capabilities, system security, product SDLC, component technical requirements); and the SANS Five name the five outcomes that, when implemented well, defeat the largest share of observed real-world ICS attacks.

The strongest maturity model for OT

The honest answer is that no single model is strongest at everything. The honest practical answer is that for measuring real OT defensive maturity — would this program actually slow down or stop an attack of the kind the community has already seen — the strongest combination is:

SANS ICS 5 Critical Controls as the outcome model, scored using the C2M2 MIL construct (or the Dragos three-stage overlay), with ISA/IEC 62443 as the technical and contractual scaffold — 62443-2-1 for the asset-owner program, 62443-2-4 for service-provider contracts, 62443-3-3 for system-level Security Level targeting, and 62443-4-1 / 4-2 for OEM and component diligence.

Three reasons that combination is stronger than any of the five alone:

1. Threat coverage is the right anchor. The SANS Five were derived from the analysis of real industrial attacks. They are the smallest set of controls that, implemented well, defeat the largest share of observed adversary tradecraft. Any maturity scoring system needs to be anchored in what actually matters operationally; the SANS Five are the cleanest expression of that anchor in the public literature.
2. MILs answer "how well" not just "whether." Scoring the SANS Five against MIL0-MIL3 from C2M2 (or the Dragos Implement / Operationalize / Optimize stages) turns each control from a binary yes/no into a four-point progression. That progression maps to investment decisions: an MIL1 ICS-specific IR plan needs documentation work; an MIL2 plan needs tabletop exercising; an MIL3 plan needs measurement against



scenario fidelity. The same logic applies to each of the other four controls.

3. 62443 closes the technical and supply-chain gaps. A maturity score on the SANS Five says “our program is good.” 62443-3-3 forces the next question: at what Security Level? An SL 3 substation control system needs different technical capabilities than an SL 1 corporate-side historian, and 62443-3-3’s seven Foundational Requirements give you the language to specify that difference. 62443-4-1 and 4-2 extend the question to the embedded devices in the system — was the firmware developed under a credible SDLC, can the component meet its target SL, is there an ISASecure certification you can point to? And 62443-2-4 closes the supply-chain loop: the audited, monitored program is undermined the moment a third-party integrator with weaker security capabilities is granted maintenance access to the same control system. Asset owners regulated under NERC CIP-003-9 will recognize this pattern: the new Section 6 vendor electronic remote access requirements approved in 2023 are the regulatory expression of the same supply-chain concern that 62443-2-4 has codified for a decade.

C2M2 alone is the strongest single model if you need a defensible enterprise-wide self-assessment with a free toolkit. CMMC 2.0 is the strongest if you need to bid on DoD contracts. 62443 alone is the strongest if you need an international consensus standard with technical depth at every level from asset-owner program to embedded component. The SANS Five alone are the strongest if you are starting a program from scratch and need the highest ROI on the first five investments. The combination is what gives a registered entity or critical-infrastructure operator a complete picture of OT defensive posture in a way that no single model does.

How to analyze a company’s OT cybersecurity maturity level — a seven-step guide

This is the workflow CIP Sentinel uses to translate the framework discussion above into an actual maturity assessment. It assumes you have ~4–8 weeks of staff time, access to the company’s OT environment (or representative documentation), and a reading of the company’s applicable regulatory drivers (NERC CIP, TSA Security Directives, NIS2, sector-specific guidance, contractual flow-downs).

Step 1 — Establish scope, drivers, target Security Level, and crown jewels

Identify the OT systems in scope: which sites, which control-system architectures, which Purdue levels, and which BES Cyber Systems or equivalent regulatory groupings. List the regulatory drivers that apply (NERC CIP-002 through CIP-015, TSA SD2 / Pipeline SD, NIS2, 32 CFR Part 170 if DoD-adjacent, IEC 62443 if contractually flowed down). For each in-scope control system, pick a target ISA/IEC 62443-3-3 Security Level (SL 1, 2, 3, or 4) based on the credible threat actor for that asset — SL 3 is the practical floor for most substation, generation control, and pipeline SCADA environments today; SL 4 is reserved for the most safety-critical or nation-state-targeted assets. Identify the company’s crown-jewel assets — the systems whose loss or manipulation would produce an unacceptable safety, operational, or financial outcome. SANS Control 1 work depends on naming the crown jewels first; the rest of the assessment depends on knowing what scope, threat-model, and Security Level target are being measured.

Step 2 — Inventory what already exists

Pull the existing artifacts: cybersecurity policy library, ICS-specific incident response plan (or general IR plan with an ICS appendix), network architecture diagrams, asset inventories, log-collection inventories, remote-access pathway lists, vulnerability-management process documentation, supplier security certifications (especially ISASecure 4-1 / 4-2 attestations from OEMs), service-provider master agreements, and the most recent internal audits or third-party assessments. Document gaps in what exists separately from gaps in what works. Many programs have the first kind of gap masquerading as the second.



Step 3 — Score each SANS Critical Control against the MIL scale

For each of the five SANS controls, rate the company at MIL0, MIL1, MIL2, or MIL3 using C2M2 definitions:

- MIL0 — the practice is not consistently performed; capability is not yet developed.
- MIL1 — the practice is performed but may be ad hoc, depending on individual initiative or experience.
- MIL2 — the practice is documented; adequate people, funding, and tools are provided to support it.
- MIL3 — the practice is guided by policy, has defined performance objectives, governance exists, and effectiveness is reviewed.

Score the five controls independently. Score honestly — the most common error is rating a control at MIL2 because a document exists when the document has not been exercised, updated, or operationalized.

Step 4 — Map third-party and OEM exposure against 62443-2-4 and 4-1/4-2

Identify every IACS service provider, integrator, OEM remote-access pathway, and managed-service relationship that touches the in-scope OT environment. For each service provider, document which of the 62443-2-4 functional areas (assurance, architecture, wireless, configuration management, remote access, event management and logging, user management, malware protection, patch management, backup & recovery, project staffing, security engineering systems) are addressed in the current contract or master services agreement. For each major OEM, document whether the supplier has 62443-4-1 SDLC attestation and whether the deployed components have ISASecure CSA certification against a target Security Level under 62443-4-2. Gaps in these maps are gaps in the company's OT supply-chain security posture. For NERC-regulated entities, this work also feeds directly into the CIP-003-9 Section 6 vendor electronic remote access security plan.

Step 5 — Cross-check against the relevant compliance baseline and the 62443-3-3 SL target

For each MIL score in Step 3, verify that the score is consistent with the company's mandatory compliance baseline and with the Security Level targeted in Step 1. For NERC-regulated entities, that means CIP-002 through CIP-015. For DoD contractors, that means CMMC at the level required by their contract portfolio. For water utilities, that means EPA Cybersecurity Evaluation expectations. For pipelines, that means the TSA pipeline Security Directives. A SANS Control 3 MIL2 score should not coexist with a failed CIP-007 R4 logging audit or with an SL 3 design target that lacks the 62443-3-3 SR 6.1 audit log management capability; if any of those conflict, the assessment must be reconciled before it is finalized.

Step 6 — Build the gap profile and prioritize

The simplest visualization is a 5-row table: each row is a SANS Critical Control, columns are current MIL, target MIL, supporting 62443-3-3 Foundational Requirement(s), gap statement, and recommended next investment. Prioritize MIL0 ratings first — these are blind spots that no other control can compensate for. Prioritize controls in the order SANS recommends (incident response, defensible architecture, monitoring, remote access, vulnerability management); each earlier control compounds the value of the later ones. Avoid the trap of optimizing one control to MIL3 while leaving another at MIL0 — the program's effective maturity is the floor, not the average.



Step 7 — Report in two languages

Executives need a one-page summary in business language: current maturity floor, top three gaps, target Security Level vs. current technical posture, investment ranges, and risk reduction expected. Practitioners need the underlying table with MIL ratings, evidence notes, control-by-control gap statements, mapped 62443 Foundational Requirements, supplier-side 4-1/4-2 attestation status, and a 12-to-24-month investment roadmap. Both should reference the regulatory drivers identified in Step 1 so the assessment ties into the program's mandatory compliance posture — not as a substitute for it.

Re-run the assessment annually at minimum, and after every material change to the OT environment (acquisition, new site commissioning, control-system upgrade, major integrator change, regulatory standard revision). Maturity is not a snapshot. It is a trend.

Three observations CIP Sentinel takes from comparing the five

First, the strongest model is rarely the most popular one. C2M2 is the most widely adopted in the U.S. energy sector because it is free, federally backed, and reasonably comprehensive — not because it is best at measuring OT defensive posture. CMMC 2.0 is the most talked-about because it has a regulatory deadline attached to it. The SANS ICS 5 Critical Controls are the model whose top score most closely correlates with whether a program would actually defeat a real attack, and they remain less widely adopted than either of the two compliance-driven frameworks.

Second, the maturity-level construct is more durable than any single framework. MILs survived the SSE-CMM, the CMMI, C2M2 v1.0 and v2.x, CMMC 1.0 and 2.0, and 62443-2-1's 2024 revision. Whatever the next federal critical-infrastructure framework looks like, it will almost certainly include a four-or-five-level maturity scoring construct of the same shape. Investing in the construct — teaching staff to think about practices in terms of ad hoc vs. documented vs. measured — pays off across frameworks in a way that investing in a specific framework rarely does.

Third, supply chain is where most programs leak. The CIP-003-9 Section 6 vendor electronic remote access requirements approved in 2023, the 62443-2-4 service-provider capabilities standard, the 62443-4-1 supplier SDLC requirements, the CMMC subcontract flow-down obligations, and the recurring third-party-oversight findings in FERC's 2025 CIP audit lessons-learned report all converge on the same point: the strongest internal maturity assessment can be undone by the weakest integrator or OEM with maintenance access to the same control system. The five-model comparison reinforces what the regulators have already concluded — supply-chain maturity is no longer an extra; it is part of the maturity floor.

Sources

- U.S. Department of Energy, [Cybersecurity Capability Maturity Model \(C2M2\)](#)¹ (CESER program page).
- DOE C2M2 Program Office, [About C2M2](#)² and [C2M2 Version 2.1 Cheat Sheet](#)³ (PDF) — MIL definitions.
- U.S. Department of Defense, [CMMC Program Final Rule \(32 CFR Part 170\)](#)⁴, Federal Register, October 15, 2024 (effective December 16, 2024).
- U.S. Department of Defense, [DFARS CMMC Final Rule \(48 CFR\)](#)⁵, Federal Register, September 10, 2025 (effective November 10, 2025).
- International Society of Automation, [ISA/IEC 62443 Series of Standards](#)⁶ — reference page for all parts including 62443-2-1 (asset owner program), 62443-2-4 (service providers), 62443-3-3 (system security requirements and Security Levels), 62443-4-1 (secure product development lifecycle), and 62443-4-2 (technical security requirements for IACS components).
- Wikipedia (citing IEC TC65 publications), [IEC 62443](#)⁹ — 62443-2-4 twelve-functional-area structure.



- Industrial Cyber, [The Essential Guide to the IEC 62443 Industrial Cybersecurity Standards](#)¹⁰.
- Robert M. Lee & Tim Conway, SANS Institute, [The Five ICS Cybersecurity Critical Controls](#)⁷, November 2022.
- Dragos, [Benchmarking Guide: Assess Your OT Cybersecurity Maturity](#)⁸ — three-stage overlay on the SANS Five.
- Dragos, [Assessing OT Cybersecurity Maturity with the SANS ICS 5 Critical Controls](#)¹¹, June 2024.
- NIST, [NIST Cybersecurity Framework](#)¹² — cross-mapping reference.

Crossroads is independent public-source analysis. Opinions are the author's own and do not represent any employer or registered entity. No utility or operating-company names are used.

Sources & references

1. Cybersecurity Capability Maturity Model
<https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>
2. Office of Cybersecurity, Energy Security, and Emergency Response
<https://c2m2.doe.gov/about>
3. official DOE cheat sheet
<https://c2m2.doe.gov/C2M2%20V2.1%20Cheat%20Sheet.pdf>
4. 32 CFR Part 170
<https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program>
5. November 10, 2025
<https://www.federalregister.gov/documents/2025/09/10/2025-17409/cybersecurity-maturity-model-certification-cmmc-program>
6. ISA/IEC 62443 series
<https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
7. Five ICS Cybersecurity Critical Controls
<https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls>
8. OT Cybersecurity Benchmarking Guide
<https://hub.dragos.com/guide/secure-industrial-operations-sans-five-critical-controls>
9. IEC 62443
https://en.wikipedia.org/wiki/IEC_62443
10. The Essential Guide to the IEC 62443 Industrial Cybersecurity Standards
<https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/>
11. Assessing OT Cybersecurity Maturity with the SANS ICS 5 Critical Controls
<https://www.dragos.com/blog/assessing-ot-cybersecurity-maturity-with-the-sans-ics-5-critical-controls>
12. NIST Cybersecurity Framework
<https://www.nist.gov/cyberframework>