Technical Paper

Reconcile & Harmonize Cyber Maturity Models

OT Cybersecurity Maturity Journey (OT CMJ) Deliverable 1

Author: **Donovan Tindill, CISSP, GICSP**
Director, OT Cybersecurity | DeNexus

https://www.linkedin.com/in/donovantindill/
www.denexus.io | OT Cyber Risk Quantification

Revision: 3.0
Publish Date: 1/30/2026

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to harmonize and reconcile the existing CMMI, NIST CSF, and C2M2 maturity models in the public domain to allow effortless mapping, conversion, or adoption of the harmonized OT cyber maturity journey framework.

Starting in the late 1980s, capability maturity models were beginning development as guidance to help organizations for developing or improving business processes. Over the ensuing decades, multiple maturity models have appeared including Capability Maturity Model Integration (CMMI), NIST Cyber Security Framework (NIST CSF), Cyber Security Capability Maturity Model (DoE C2M2), Capability Maturity Model Certification (DoD CMMC), ISA/ISO/IEC 62443-2-4 Service Provider capabilities, and more.

Depending on the application or scope, security professionals may choose one or more of these maturity frameworks for their assignment. **That is when the first challenge appears**: picking the right maturity framework for the problem. For example:

- CMMI v1.3 – can be used for measuring the maturity of any business process, including a cybersecurity program, using a scale of 5 levels (1-5). CMMI v2.0 exists, but must be licensed and not available in the public domain.
- NIST CSF – focused on cybersecurity for the measurement of risk management in 4 tiers (1-4). NIST CSF also contains cybersecurity requirements.
- C2M2 v2.0 – focused on cybersecurity for the energy sector, defining maturity indicator levels (MIL) in 3 levels (1-3). C2M2 also contains cybersecurity requirements, calibrated against the maturity indicator levels.
- CMMC – focused on certification of contractors and suppliers to US Department of Defense.
- 62443-2-1:2024 – It includes a maturity model, but follows CMMI v1.3. All 62443 documents must be licensed and not available in the public domain.
- 62443-2-4:2018 – focused on requirements for ICS/OT Service Providers, such as field service or manage service providers (MSPs), supporting an automation system. All 62443 documents must be licensed and not available in the public domain.

For the purposes of an asset owner's ICS/OT cybersecurity program, there are three (3) maturity models available in the public domain to choose from: CMMI v1.3, NIST CSF, and C2M2. Across the asset owner and consulting community, all three are used regularly and no single framework has emerged as the industry leading choice. Largely because each provides their own unique benefits, and followers are forced to do their own proprietary mapping and conversion between them for greater benefit.

The purpose of this document is to harmonize and reconcile the existing CMMI, NIST CSF, and C2M2 maturity models to allow effortless mapping, conversion, or adoption of these cyber maturity frameworks. The goal is not to invent a fourth maturity framework, it is to identify on behalf of the global community and make available publicly, this mapping between these frameworks. At first glance our deliverables may appear as a new framework, but it is harmonization of existing frameworks.

Privately, organizations and consultants have already performed this mapping between the maturity frameworks. All have agreed it is a problem they felt necessary to solve for their own internal uses or with

customers. The problem is, they chose to keep the results proprietary, or the market has labelled their efforts as proprietary, and this has impeded any widespread adoption, consistency, or advancement in the global cybersecurity community.

By this document releasing in the public domain, with well-known industry contributors having extensive experience across multiple maturity frameworks, we hope to overcome any bias of the deliverables being considered proprietary. This document shall be placed in the public domain, without a license, free for use or redistribution in hopes to accelerate global adoption. If our vision is accurate, then after a period of widespread adoption any lessons learned can be used to improve cybersecurity maturity frameworks in the future including NIST CSF 3.x, C2M2 v3.x, 62443, and others.

2 EXISTING MATURITY FRAMEWORKS IN THE PUBLIC DOMAIN

The purpose of this section is to provide a summary of the existing cybersecurity frameworks applicable to those developing or assessing an ICS/OT cybersecurity program.

Scope: Those frameworks not intended for assessing an asset owners' cybersecurity program (e.g., 62443-2-4, DoD CMMC), or require a license fee to obtain the documents (e.g., 62443-2-1, ISACA CMMI v2.0), are excluded from below.

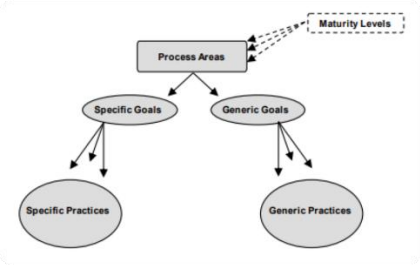
2.1 CMMI v1.3

Download: CMMI-SVC v1.3 from CMU-SEI.

Originally developed by Carnegie Mellon University (CMU) starting in 1987 for process improvement. Version 1.3 was published in 2010 and is the last available for free in the public domain. Intellectual property transferred to CMMI Institute in 2013 and ISACA acquired the CMMI Institute in 2016. ISACA published version 2.x, but is only available under license and subscription fees.

CMMI v1.3 is the most widely recognized and adopted. There is limited evidence of widespread ISACA v2.0 adoption. For the remainder of this document, this will simply be referred to as CMMI.

The CMMI framework consists of 5 maturity levels, with requirements across 24 process areas. Each of these process areas have both generic & specific goals & practices.



	Name	Abbr.	ML	CL1	CL2	CL3
2-Managed	Configuration Management	CM	2		Target Profile 2	
	Measurement and Analysis	MA	2			
	Process and Product Quality Assurance	PPQA	2			
	Requirements Management	REQM	2			
	Supplier Agreement Management	SAM	2			
	Service Delivery	SD	2			
	Work Monitoring and Control	WMC	2			
	Work Planning	WP	2			
3-Defined	Capacity and Availability Management	CAM	3			
	Decision Analysis and Resolution	DAR	3			
	Incident Resolution and Prevention	IRP	3			
	Integrated Work Management	IWM	3			
	Organizational Process Definition	OPD	3			
	Organizational Process Focus	OPF	3			
	Organizational Training	OT	3			
	Risk Management	RSKM	3			
	Service Continuity	SCON	3			
	Service System Development[12]	SSD	3			
	Service System Transition	SST	3			
	Strategic Service Management	STSM	3			
	Organizational Process Performance	OPP	4			Target Profile 4
	Quantitative Work Management	QWM	4			
	Causal Analysis and Resolution	CAR	5			Target Profile 5
	Organizational Performance Management	OPM	5			

In its most simplified implementation, to achieve a specified maturity level requires the fulfillment of **all** applicable goals and practices, across **all** applicable process areas for that level. For example, CMMI maturity level 2 (ML2) 'Managed' requires the fulfillment of 8 process areas and their goals/practices. CMMI maturity level 3 (ML3)

requires 12 more process areas, ML4 adds 2 more. The maturity level is achieved once all the process area goals, practices, and requirements are fulfilled.

Key Takeaway: It is not possible to achieve CMMI ML3 without first fulfilling all of ML2. This means that if a single requirement in ML2 is incomplete, the entity must self-assess themselves as the lower level where work remains. CMMI provides specific guidance on what is required to achieve the next level, which will be used in Deliverable 2 of this task force.

CMMI v1.3 supports two representations:

- **Staged representation** → focuses on overall organizational maturity measured by maturity levels (1–5).
- **Continuous representation** → focuses on process area capability measured by capability levels (0–3).

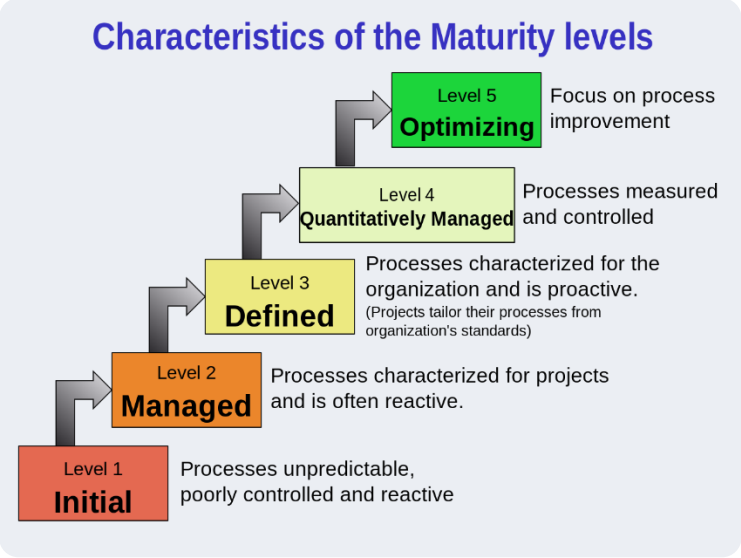
In the **staged** representation, maturity levels represent an evolutionary path for improving organizational processes across a defined set of process areas; levels are also used as appraisal rating outcomes and can support benchmarking.

CMMI Staged Representation	Detailed definition
1 Initial	At maturity level 1, processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment to support processes. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. In spite of this chaos, maturity level 1 organizations provide services that often work, but they frequently exceed the budget and schedule documented in their plans. Maturity level 1 organizations are characterized by a tendency to overcommit, abandon their processes in a time of crisis, and be unable to repeat their successes.
2 Managed	At maturity level 2, work groups establish the foundation for an organization to become an effective service provider by institutionalizing selected Project and Work Management, Support, and Service Establishment and Delivery processes. Work groups define a service strategy, create work plans, and monitor and control the work to ensure the service is delivered as planned. The service provider establishes agreements with customers and develops and manages customer and contractual requirements. Configuration management and process and product quality assurance are institutionalized, and the service provider also develops the capability to measure and analyze process performance. Also at maturity level 2, work groups, work activities, processes, work products, and services are managed. The service provider ensures that processes are planned in accordance with policy. To execute the process, the service provider provides adequate resources, assigns responsibility for performing the process, trains people on the process, and ensures the designated work products of the process are under appropriate levels of configuration management. The service provider identifies and involves relevant stakeholders and periodically monitors and controls the process. Process adherence is periodically evaluated and process performance is shared with senior management. The process discipline reflected by maturity level 2 helps to ensure that existing practices are retained during times of stress.

CMMI Staged Representation	Detailed definition
3 Defined	At maturity level 3, service providers use defined processes for managing work. They embed tenets of project and work management and services best practices, such as service continuity and incident resolution and prevention, into the standard process set. The service provider verifies that selected work products meet their requirements and validates services to ensure they meet the needs of the customer and end user. These processes are well characterized and understood and are described in standards, procedures, tools, and methods. The organization's set of standard processes, which is the basis for maturity level 3, is established and improved over time. These standard processes are used to establish consistency across the organization. Work groups establish their defined processes by tailoring the organization's set of standard processes according to tailoring guidelines. (See the definition of "organization's set of standard processes" in the glossary.) A critical distinction between maturity levels 2 and 3 is the scope of standards, process descriptions, and procedures. At maturity level 2, the standards, process descriptions, and procedures can be quite different in each specific instance of the process (i.e., used by a particular work group). At maturity level 3, the standards, process descriptions, and work procedures are tailored from the organization's set of standard processes to suit a particular work group or organizational unit and therefore are more consistent except for the differences allowed by the tailoring guidelines. Another critical distinction is that at maturity level 3, processes are typically described more rigorously than at maturity level 2. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. At maturity level 3, processes are managed more proactively using an understanding of the interrelationships of process activities and detailed measures of the process, its work products, and its services. At maturity level 3, the organization further improves its processes that are related to the maturity level 2 process areas. Generic practices associated with generic goal 3 that were not addressed at maturity level 2 are applied to achieve maturity level 3.
4 Quantitatively Managed	At maturity level 4, service providers establish quantitative objectives for quality and process performance and use them as criteria in managing processes. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers. Quality and process performance is understood in statistical terms and is managed throughout the life of processes. For selected subprocesses, specific measures of process performance are collected and statistically analyzed. When selecting subprocesses for analyses, it is critical to understand the relationships between different subprocesses and their impact on achieving the objectives for quality and process performance. Such an approach helps to ensure that subprocess monitoring using statistical and other quantitative techniques is applied to where it has the most overall value to the business. Process performance baselines and models can be used to help set quality and process performance objectives that help achieve business objectives. A critical distinction between maturity levels 3 and 4 is the predictability of process performance. At maturity level 4, the performance of processes is controlled using statistical and other quantitative techniques and predictions are based, in part, on a statistical analysis of fine-grained process data.

CMMI Staged Representation	Detailed definition
5 Optimizing	At maturity level 5, an organization continually improves its processes based on a quantitative understanding of its business objectives and performance needs. The organization uses a quantitative approach to understand the variation inherent in the process and the causes of process outcomes. Maturity level 5 focuses on continually improving process performance through incremental and innovative process and technological improvements. The organization's quality and process performance objectives are established, continually revised to reflect changing business objectives and organizational performance, and used as criteria in managing process improvement. The effects of deployed process improvements are measured using statistical and other quantitative techniques and compared to quality and process performance objectives. The defined processes, the organization's set of standard processes, and supporting technology are targets of measurable improvement activities. A critical distinction between maturity levels 4 and 5 is the focus on managing and improving organizational performance. At maturity level 4, the organization and work groups focus on understanding and controlling performance at the subprocess level and using the results to manage projects. At maturity level 5, the organization is concerned with overall organizational performance using data collected from multiple work groups. Analysis of the data identifies shortfalls or gaps in performance. These gaps are used to drive organizational process improvement that generates measurable improvement in performance.

The following diagram is a well-known simplification of CMMI v1.3.



Have they been used, or should they be used, as maturity levels? Yes—this is explicitly how the staged representation is designed. CMMI describes maturity levels as characterizing organizational improvement across multiple process areas, and notes that this capability/maturity dimension is used for benchmarking and appraisal activities (i.e., producing a maturity level rating).

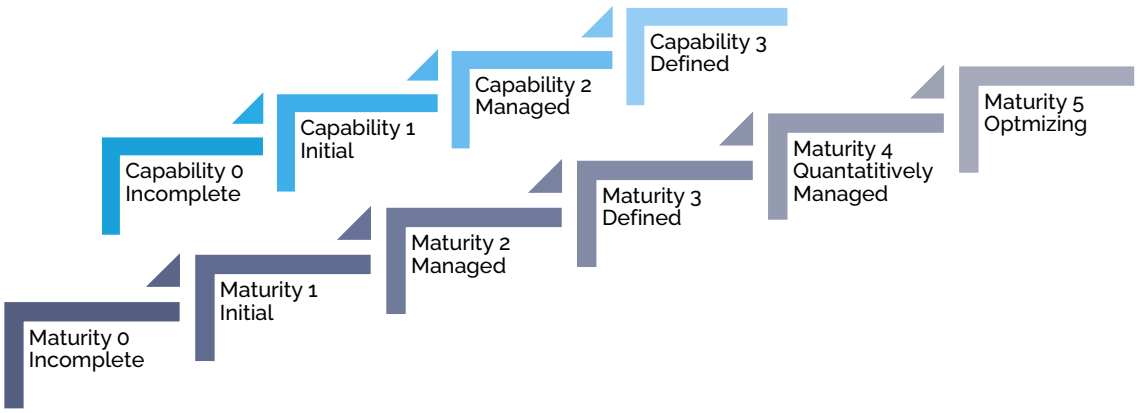
How they should be used (aligned to CMMI intent):

- Treat CMMI maturity levels as process institutionalization maturity (how consistently and rigorously organizational processes are defined, managed, measured, and improved)—not as a direct measure of "security controls implemented" or "technical security effectiveness."
- Avoid collapsing continuous capability levels into a staged-style single score unless you are deliberately using staged appraisal logic; CMMI distinguishes these two improvement paths for a reason. DeNexus recommends using the staged representation.
- In an OT/ICS cybersecurity maturity context, CMMI can be applied to with its maturity-level semantics (e.g., "Managed/Defined/Quantitatively Managed/Optimizing") to help measure each cybersecurity category and domain.

2.1.1 CMMI v2.x

In 2016, ISACA acquired the CMMI Institute (a former Carnegie Mellon University project) including retention of the CMMI intellectual property. Version 1.3 of CMMI is the last version available in the public domain. CMMI V2.x content is provided via an online platform rather than a free PDF, through an annual subscription that grants access to the Model Viewer or an Enterprise license.

From CMMI Institute, the CMMI 2.x model has continued to evolve, but the fundamental framework remains the same.



Capability Levels apply to individual process areas or capabilities and describe how well that specific capability is implemented and institutionalized. **Maturity Levels** apply to the organization's broader set of processes and reflect collective process institutionalization and performance across multiple areas (typically determined via a staged assessment).

In early CMMI 1.x versions, "continuous" and "staged" representations were separate, with capability levels tied to continuous representation and maturity levels tied to staged representation. In CMMI 2.x, the framework is unified, and while the concept of capability progression remains, the primary focus for organizational appraisal is the maturity level progression outlined above.

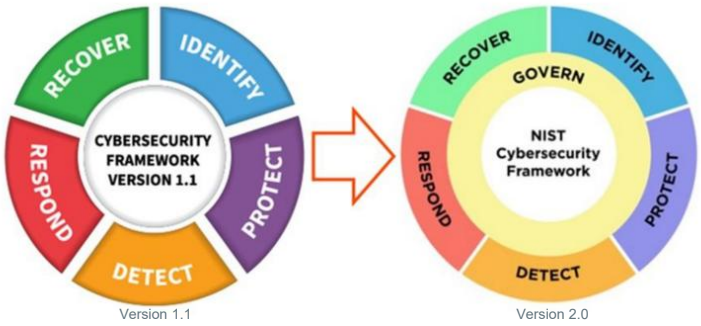
The details of CMMI 2 could not be included in a harmonized maturity model due the commercialization of this framework and IP restrictions.

2.2 NIST CSF v2.0

Download: NIST CSF v1.1 and NIST CSF v2.0.

The NIST Cybersecurity Framework (CSF) 2.0 is a NIST-published, sector-agnostic framework intended to help organizations manage cybersecurity risk. It provides a taxonomy of high-level cybersecurity outcomes (the "CSF Core") that organizations can use to understand, assess, prioritize, and communicate cybersecurity efforts; it does not prescribe specific controls or exactly how outcomes must be achieved.

CSF 2.0 is organized around six Functions: **Govern, Identify, Protect, Detect, Respond, Recover**, providing an end-to-end view of cybersecurity risk management.



In addition to the Core, CSF 2.0 includes:

- **Organizational Profiles** (Current and Target) to describe the organization's cybersecurity posture in terms of CSF outcomes, and
- **CSF Tiers** to characterize the rigor of cybersecurity risk governance and management practices and to provide context for how the organization manages risk.

CSF 2.0 defines four Tiers—a progression from informal/ad hoc to agile, risk-informed, and continuously improving risk governance and management.

NIST CSF 2.0 Tiers	Cybersecurity Risk Governance	Cybersecurity Risk Management
1: Partial	Strategy and prioritization is ad hoc	Limited awareness, irregular, case-by-case, no information sharing processes, unaware of risks
2: Risk-Informed	Approved by management, not organization-wide, prioritization informed by risk	Organizational risk awareness, not organization-wide, some but not all levels of organization, assessment occurs occasionally, informal sharing of information, aware of risks but responses are not consistent or formal
3: Repeatable	Formally approved and expressed in policy, risk-informed policies are implemented throughout program, reviewed, regular updates in response to business requirements or threats	Organization-wide approach, routine information sharing, consistent methods, personnel have sufficient skills, consistently monitors risks, executives communicate regularly and considered in all lines of business, personnel respond to risks, continuously monitored and reviewed
4: Adaptive	Organization-wide, risk-informed decision making, cyber and financial decisions made together in context, budget based on current and predicted risks, risk management embedded in culture, lessons learned, continuous improvement	Adapts policies from past activities, lessons learned and predictive indicators, continuous improvement, advanced technologies, advanced practices, adapts to changing landscape and evolving threats, near real-time information for risk decision-making, constant information sharing and with third-parties

Many practitioners, vendors, and assessments commonly refer to CSF Tiers as “maturity levels,” even though this typically compresses multiple dimensions (governance, process institutionalization, and integration with enterprise risk) into a single label.

Should they be used as maturity levels (per NIST intent)? The CSF 2.0 text positions Tiers as risk governance and risk management rigor descriptors, used to inform Current/Target Profiles and set the “tone” for how cybersecurity risk is managed—not as a control-by-control capability maturity model.

2.3 C2M2 v2.1

Download: Cybersecurity Capability Maturity Model (C2M2) v2.1.

The Cybersecurity Capability Maturity Model (C2M2) is a U.S. Department of Energy (DOE) maturity model and accompanying self-evaluation tooling intended to help organizations evaluate cybersecurity capabilities and prioritize/optimize security investments. It is built from industry-vetted practices that explicitly consider both IT and OT environments.

C2M2 is:

- **Descriptive, not prescriptive**—it describes practices and maturity attributes to support improvement planning rather than mandating specific control implementations.
- Structured around **~350 practices** grouped into **10 domains**, each containing objectives and practices sequenced by maturity.

C2M2 uses Maturity Indicator Levels (MILs) 0–3, applied independently to each domain. The model describes MILs as a dual progression (an "approach progression" and a "management progression"), and MILs are cumulative within a domain (i.e., to achieve MIL2 you must satisfy MIL1+MIL2 practices).

C2M2 MIL	Detailed definition
MIL0	Practices are not performed.
MIL1	Initial practices are performed, but may be ad hoc.
MIL2	Management characteristics: • Practices are documented • Adequate resources are provided to support the process. Approach characteristic: • practices are more complete or advanced than MIL1.
MIL3	Management characteristics: • Activities are guided by policies (or other organizational directives); • Responsibility, accountability, and authority for performing the practices are assigned; • Personnel perform the practices have adequate skills and knowledge; • The effectiveness of activities is evaluated and tracked. Approach characteristic: • Practices are more complete or advanced than at MIL2.

Should they be used, as "maturity levels"? Yes—this is their explicit purpose. C2M2 is a maturity model, and MILs are the defined maturity scale used to measure progression within each domain.

How C2Ms MIL should be used (per model intent):

- **Per-domain maturity, not a single enterprise "score**." C2M2 explicitly notes an organization may be at different MILs across different domains.
- **Target-setting and prioritization**. The model recommends establishing target MILs per domain and focusing gap analysis and improvement efforts accordingly.
- **"Highest everywhere" is not the goal**. C2M2 cautions that striving for the highest MIL across all domains may not be optimal; targets should align to business objectives and cybersecurity strategy, with costs weighed against benefits.

The last point of interest is that the C2M2 was developed in collaboration with Carnegie Mellon University's Software Engineering Institute (SEI). The CMI-CEI is the origin of the CMMI (capability maturity model integration) released in the 1990s, now known as CMMI v1.3 and 2.0.

3 KNOWN ISSUES WITH EXISTING MATURITY FRAMEWORKS

The purpose of this section is to catalog known issues and shortcomings that cybersecurity professionals have faced trying to use these existing maturity frameworks with their leadership, co-workers, or customers.

As much as possible, this document hopes to reduce or eliminate these issues.

Bias: Maturity assessments often reflect the biases of the framework, assessor, and organization being assessed.

- **Framework bias:** Many frameworks originated in IT governance or a specific sector; they can overweight documentation and process artifacts relative to operational feasibility and safety constraints in OT.
- **Assessor bias:** Two qualified assessors can arrive at different ratings due to differences in interpretation, risk tolerance, and prior industry experience.
- **Organizational bias:** Asset owners may "grade themselves generously" when assessments are tied to funding, audit outcomes, or executive reporting; conversely, teams may underrate maturity to justify investment.

Subjectivity: Many maturity models rely on qualitative judgment and self-attestation, especially where requirements are expressed as outcomes rather than measurable criteria.

- **Self-evaluation dependence:** Some models are explicitly designed around facilitated workshops where participants collectively decide ratings, which is valuable for alignment but introduces subjectivity and variability based on who is in the room.
- **Evidence ambiguity:** "Repeatable," "risk-informed," "adaptive," and similar terms can be interpreted very differently across sites, business units, and regions.
- **OT reality:** In ICS environments, compensating controls, operational workarounds, and vendor-managed constraints are common; subjective judgments increase when there is no clear "control present/control absent" answer.

Inconsistency and Room for Interpretation: Broad language enables flexibility, but also enables inconsistent scoring and "check-the-box" implementations.

- **Interpretation gaps:** When a model lacks defined criteria for what "good" looks like at each level, teams create local scoring rubrics, undermining benchmarking.
- **Vocabulary mismatch:** Even within a single model implementation, terminology conflicts between the model and the organization can drive inconsistent scoring unless explicitly reconciled (models themselves call out the need to identify vocabulary conflicts).
- **Tier misuse:** The NIST CSF Implementation Tiers are explicitly *not* intended to be maturity levels; they describe how cybersecurity risk management is integrated with enterprise risk management, not the quality of specific controls. Practical consequence: organizations routinely use CSF tiers as if they were a control maturity score, which creates false comparability and inconsistent results.

Low Recognition of "Building the Program" (the formative phase): Many frameworks do not adequately distinguish between: (1) not started, (2) actively building, and (3) implemented but immature.

- **Why it matters:** OT security programs often spend meaningful time in architecture, tooling deployment, process definition, and workforce enablement before benefits are measurable. From DeNexus' experience inputting customer's maturity levels, they are often in the 'partial' phase for several years.
- **Common failure mode:** leadership sees "still low maturity" despite major effort, because the model does not credit formative progress (planning, designing, piloting, training, tooling rollout).

Assumes Highest Maturity is the Goal: Many maturity scales implicitly suggest that "higher is better" everywhere, which can be counterproductive in OT.

- **Risk and mission should set the target:** NIST's guidance emphasizes that moving to higher tiers should be driven by risk reduction and cost-effectiveness—not maturity for its own sake.
- **Better framing:** "Target maturity" should be domain-specific and justified by criticality, consequence, and threat exposure (i.e., high maturity where it matters most).

Specific Requirements and Controls: There is persistent confusion between *maturity* (how well a capability is performed and institutionalized) and *controls* (what is implemented).

- **Control lists without maturity guidance:** Some approaches are rich in control requirements but weak on describing how those controls mature over time.
- **Maturity without control specificity:** Conversely, models that describe maturity states may not provide enough prescriptive detail for "what comes next," forcing consultants and asset owners to create proprietary roadmaps.

This gap is a primary reason mapping and harmonization are valuable: users want both (a) a defensible maturity scale and (b) actionable next steps.

Benchmarking Limitations: If one organization uses CMMI, another uses C2M2, another uses a hybrid, their interpretation of levels, the number of levels, and their alignment make it difficult to create benchmarks across regions and industries. Benchmarking is attractive, but becomes unreliable when:

- organizations tailor interpretations differently,
- evidence standards differ,
- maturity is aggregated differently (site vs enterprise),
- sector context differs (low maturity in one sector, is high in another).

Conclusion: Collectively, these issues reduce the credibility and comparability of maturity results, impede executive decision-making, and force asset owners and consultants to create proprietary scoring rubrics and mappings. The purpose of this document is to reduce these shortcomings by harmonizing level definitions, clarifying "building-phase" progress, reducing interpretation variance through common keywords and evidence expectations, and enabling consistent mapping between widely used public-domain frameworks.

4 METHODOLOGY

The purpose of this section is to describe the steps and rigor followed to reconcile and harmonize the maturity level definitions from CMMI v1.3, NIST CSF, and C2M2 into a single OT Cyber Maturity Journey (CMJ). This methodology follows common maturity model development lifecycle guidance (i.e., establish scope, design the model, populate it with source content, test/iterate, and maintain), adapted to the specific goal of producing a **public-domain crosswalk** that enables mapping and conversion between widely used maturity models.

4.1 SCOPE AND SOURCE SELECTION

The purpose of this step is to ensure the reconciliation remains practical and repeatable for asset owners.

- Scope: This effort is focused on maturity frameworks used to assess an **asset owner's ICS/OT cybersecurity program**, and excludes frameworks that (a) are not intended for asset-owner program maturity or (b) require paid licensing to obtain the source documents.
- Selected source models: CMMI v1.3, NIST CSF, and C2M2 were selected because they are widely used, relevant to the cybersecurity community, and (for the versions referenced) available in the public domain.

Key Takeaway: This project is not intended to "invent a fourth maturity framework," but to publish an evidence-based reconciliation and mapping of the existing frameworks in a way that is non-proprietary and reusable.

4.2 STEP 1 — EXTRACT "KEYWORDS" AND NORMALIZE MATURITY SEMANTICS (KEYWORD ANALYSIS)

The purpose of this step is to reduce ambiguity and "room for interpretation" by extracting the English-language action words and maturity descriptors used by each framework to describe progression.

- Keyword extraction: Maturity-level definitions and related descriptive language were reviewed to extract and normalize the action-oriented descriptors (e.g., ad hoc, managed, defined, measured, optimizing).
- Consolidation: These keywords were consolidated into a comparable vocabulary across frameworks to support subsequent level alignment and definition drafting.

This work is captured in Table 1 Maturity Model Keywords.

Key Takeaway: A harmonized maturity model cannot be consistently applied if each assessor or organization must first invent their own "interpretation dictionary." Keyword normalization is used here as a practical control to improve repeatability.

4.3 Step 2 — Decompose CMMI structure into analyzable components (Process Areas and Generic Goals/Practices)

The purpose of this step is to introduce rigor and sequencing logic using CMMI's detailed, cumulative maturity structure as the "backbone" for requirements.

- CMMI decomposition: CMMI v1.3 process areas and generic goals/practices were "exploded" by maturity level to allow further keyword analysis and to make the underlying requirements visible for harmonization.
- Output: This decomposition is captured in Table 2 CMMI Process Areas and Generic Goals/Practices.

Key Takeaway: CMMI includes explicit cumulative logic—ML3 cannot be claimed unless ML2 is satisfied first. This cumulative property is a key contributor to scoring rigor and was intentionally preserved in the harmonized model.

4.4 Step 3 — Simplify CMMI requirements into level-by-level maturity requirements

The purpose of this step is to translate CMMI's generic goals/practices into a simplified requirement set that can be used alongside other frameworks' maturity language.

- Simplification: CMMI's process maturity expectations were simplified into plain-language requirements (e.g., responsibility assigned, policy established, process documented, training started, objectively evaluated, measured and data-driven, lessons learned and improvement loop).
- Output: These simplified requirements are captured in Table 3 Simplified CMMI Requirements.

Key Takeaway: Many cybersecurity maturity models provide descriptive maturity language but do not clearly state "what must be true" to claim a level. The simplified CMMI requirements were used to strengthen level definitions and reduce subjective scoring.

4.5 Step 4 — Reconcile and align maturity levels across frameworks (Crosswalk and gap identification)

The purpose of this step is to match maturity levels that are materially equivalent across different frameworks and to identify discontinuities where a framework lacks an operationally important "state" in the journey.

- Reconciliation: Levels were aligned using (a) the normalized keyword corpus (Table 1) and (b) the simplified cumulative requirements (Table 3).
- Output: The resulting crosswalk is captured in Table 4 Harmonizing Maturity Models Together.

Key Takeaway: This alignment is specifically intended to enable mapping and conversion (e.g., translate a level stated in one model into an equivalent level in another), reducing the need for proprietary mappings.

4.6 Step 5 — Introduce a "Developing" level (1.5) to represent the formative building phase

The purpose of this step is to explicitly recognize and score the "under construction" phase that commonly occurs in ICS/OT security programs (planning started, tooling being deployed, training initiated), which is often not well represented in existing maturity scales.

- New level insertion: A new level, **1.5 "Developing"**, was introduced to address the low recognition of "building the program" discussed in the Known Issues section. From our experience, an organization might be in the partial or ad hoc phases for years, until they achieve the requirements of the next level. The Developing stage is explicitly intended to recognize organizations proactively taking steps to build their program.
- Placement logic: The new level is positioned between ad hoc execution and basic managed implementation, and is defined using the same cumulative maturity logic as the rest of the model (i.e., you must achieve all the requirements of the prior level).

Key Takeaway: This reduces a common failure mode where multi-year program buildout effort is not reflected in maturity reporting, creating executive perception of "no progress."

4.7 Step 6 — Produce harmonized written definitions and harmonized requirements

The purpose of this step is to produce the two practical outputs needed for adoption: (1) a consistent written definition of each maturity level, and (2) an associated set of requirements that constrain scoring.

- Harmonized level definitions: The final keywords and simplified requirements were combined to develop a written definition for each harmonized maturity level. Output is captured in Table 5 Harmonized Maturity Requirements.
- Harmonized maturity requirements: CMMI-derived rigor (Table 3) was combined with the maturity semantics (Table 1) to define what must be true to claim each harmonized level. Output is captured in Table 6 (Harmonized Maturity Requirements).

Key Takeaway: The harmonized model is cumulative: **Must accomplish all requirements of the lower level. No rounding up.**

4.8 Step 7 — Intent Preservation and Scoring Controls (Reducing Misuse)

The purpose of this step is to preserve each framework's stated intent and prevent common misapplication during mapping.

- NIST CSF tiers: CSF tiers are preserved as risk governance / risk management integration descriptors, and are not treated as control-by-control maturity levels. (This is a frequent industry misuse that increases inconsistency.)
- C2M2 MILs: C2M2 is treated as a domain-level maturity model (MILs by domain), consistent with its structure and stated usage.
- CMMI cumulative logic: CMMI sequencing rigor is used as a quality control to constrain scoring inflation and support repeatability across assessors and organizations.

Key Takeaway: Preserving intent is essential; otherwise, the mapping becomes a "forced equivalency" exercise that produces false confidence and weak comparability.

4.9 Step 8 — Traceability and Maintainability (Future Revisions)

The purpose of this step is to ensure this Cybersecurity Maturity Journey (CMJ) can evolve without breaking its ability to map between frameworks.

- Traceability: Each harmonized maturity definition and requirement is traceable to the inputs in Tables 1–3 and the reconciliation logic in Table 4, and is expressed in Tables 5–6.
- Maintainability: Additional public-domain frameworks can be incorporated by repeating Steps 1–6, re-validating equivalencies in the reconciliation crosswalk, and updating the harmonized definitions/requirements accordingly. This aligns with established maturity model lifecycle guidance that emphasizes iterative improvement and periodic revision.

Key Takeaway: It is likely that new maturity frameworks will be released into the public domain, or applicable to asset owners, or part of future regulations and standards. The transparency of this analysis is intended to compliment, influence, and maybe even help standardize the next iteration of cybersecurity maturity models.

5 KEYWORD ANALYSIS

The purpose of this section is to extract the English language action words (aka., verbs) from existing maturity framework definitions, at the same time reconciling and harmonizing these frameworks.

Table 1 Maturity Model Keywords

Maturity Level	0	1	2	3	4	5
CMMI v1.3 Keywords	-	initial, unpredictable, uncontrolled, reactive, delayed, over budget,	managed, project management, reactive, not organization-wide (varies by facility/project),	defined, proactive, project-specific tailoring from org standards, organization-wide,	quantitatively managed, measured, controlled, data-driven, predictable, stakeholder needs alignment,	optimizing, improving, pivot, respond to opportunity and change, stability, agile, innovative,
Others like CMMI	-	crisis mode, fire fighting, heroic efforts, irreplaceable staff "unicorns",	standardized project planning, establishing a baseline	standardized techniques, standardized deliverables, baseline established,	project histories, historical estimates, metrics, repository of metrics, key learnings, lessons learned,	project review, project assessment, metric review & feedback, closed loop process of execution, measurement, and improvement, continuously use measurement feedback,
COBIT Keywords	non-existent, lacking, incomplete, may not meet intent,	initial, intuitive, intuition, may achieve its purpose, incomplete set, performed,	performed, achieves purpose, basic, complete, managed, approved, in place,	organized, well-defined, more organized, organizational-wide assets, typically well defined, established, approved, in place, communicated,	quantitatively measured, well defined, performance is measured, predictable, metrics, measurement,	continuous improvement performance measured to improve, pursuit of improvement, optimizing
C2M2 MIL Keywords	MIL0, not initiated, incomplete,	MIL1, initiated, adhoc	MIL2, performed, documented, adequate resources	MIL3, managed, guided by policy or directives, RACI, personnel have sufficient skills, effectiveness evaluation, effectiveness tracking	-	-

Maturity Level	0	1	2	3	4	5
NIST CSF Keywords	not initiated,	partial, not formalized, adhoc, sometimes reactive, not informed directly, limited awareness, irregular, case-by-case, varied experience, may not have processes,	risk informed, not established organization wide, needs are directly informed, informal, some consideration of security at some org levels, not repeatable, not reoccuring,	repeatable, formally approved, expressed in policy, regularly updated to changes, organization-wide approach, risk-informed, reviewed, consistent methods, personnel have skills to do their job, consistent, regular communication of cyber risk,	adaptive, adapts to changes, lessons learned, predictive, continuous improvement, advanced technologies, advanced practices, timely response, cyber and org objectives understood, cyber and financial risk managed together, budget is risk-based, predictive risk environment, risk tolerance, business unit and org alignment, organizational culture, lessons learned evolution, quick decision making	-
DoE OIG 24-17	-	adhoc, not formalized, reactive	defined, formalized, documented, inconsistent,	consistently implemented, lacking effectiveness measures	managed, measurable, quantitative measures, qualitative measures, organization-wide,	optimized, institutionalized, repeatable, self-generating, regularly updated, based on changing threat and technology landscape
RESULTS: Similar maturity keywords	**not initiated, incomplete, unpredictable, uncontrolled,**	**initial, partial, adhoc, initiated, reactive, incomplete, limited awareness, formative,**	**managed, basic, basic project management, performed, documented, site-specific (not organization-wide),**	**defined, proactive, standardized, baselined, organized, well-defined, organization-wide, formally approved, regularly updated to change, sufficient resources,**	**quantitatively managed, measured, controlled, data-driven, historical data, metrics, adaptive, lessons learned,**	**optimizing, continuous improvement**

In the following table, the process areas, goals, and practices from CMMI v1.3 are exploded into their respective maturity levels, to allow additional keyword analysis.

Table 2 CMMI Process Areas and Generic Goals/Practices

Maturity Level	1 Initial	2 Managed	3 Defined	4 Quantitatively Managed	5 Optimizing
CMMI v1.3 Process Areas	No process areas are defined at the Initial maturity level. *It can be implied that all process areas at the 'Managed' level are partial and in development.*	• Configuration Mgmt (CM) • Measurement & Analysis (MA) • Process and Product Quality Assurance (PPQA) • Supplier Agreement Mgmt (SAM) • Service Delivery (SD) • Requirements Mgmt (REQM) • Work Monitoring & Control (WMC) • Work Planning (WP)	• Capacity & Availability Mgmt (CAM) • Decision Analysis & Resolution (DAR) • Incident Resolution & Prevention (IRP) • Integrated Work Management (IWM) • Organizational Process Definition (OPD) • Organizational Process Focus (OPF) • Organizational Training (OT) • Risk Management (RISKM) • Service Continuity (SCON) • Service System Development (SSD) • Service System Transition (SST) • Strategic Service Mgmt (STSM)	• Organizational Process Performance (OPP) • Quantitative Work Management (QWM)	• Casual Analysis & Resolution (CAR) • Organizational Performance Management (OPM)

CMMI v1.3 Generic Goals/Practices	• Responsibility is assigned
	• Process is performed
	• Process goals are defined
	• Organizational expectations are established in policy
	• Policy is established
	• Define and document the plan for performing the process (i.e., standards, dependencies, resources, responsibilities, training, work products, measurement, etc.
	• Define and document the process description
	• Tools/technology are acquired & implemented (see Process Areas for details)
	• Start training
	• Identify stakeholders
		• Review the plan with relevant stakeholders and get their agreement
		• Revise the plan as necessary
		• Minimum resources provided (e.g., funding, physical facilities, skilled people, tools, technology, etc.)
		• Basic training program
		• Involve stakeholders
		• Establish a defined process
		• Process is managed
		• Monitoring and control the process and work products
			• Specialized training
			• Objectively evaluate adherence (relies on PPQA)
			• Review Status with Higher Level Management
			  ○ Executive sponsor/owner assigned
			• Collect process related experiences
			• Capacity & availability monitoring and reporting
			• Other
			  ○ Proactive
			  ○ Formal training cirriculum
			  ○ Understand and leverage importance/criticality in decision-making
			  ○ Identify and analyze risk
			  ○ Mitigate risk
			  ○ Non-conformance identification, control, and mitigation
			  ○ Organization-wide Standardization
				• Trends
				• Lessons learned
				• Cost and benefits of improvements
				• Data quality objectives
				• Performance objectives
					• Root cause analysis
					• Remedy root causes
					• Elicit suggestions
					• Validate improvements
					• Implement improvements
					• Evaluate improvement effects

In the following table, the Process Areas and Generic Goals/Practices from CMMI v1.3 are simplified into requirements for each maturity level.

Table 3 Simplified CMMI Requirements

Maturity Level	1 Initial	2 Managed	3 Defined	4 Quantitatively Managed	5 Optimizing
RESULTS: Simplified Goals & Practices (includes maturity keywords from above, where applicable)	• Responsibility is assigned • Process is performed • Process goals are defined • Policy is established • Process is documented • Tools are implemented • Stakeholders identified • Training started	• Stakeholder agreement • Minimum resources provided • Staff trained • Site-specific standards • Process established • Process is managed • Process is monitored • Process is controlled • Basic work management	• Executive sponsorship & regular review • Criticality/Risk-based decision making • Proactive processes • Company-wide standardization • Baseline • Well-defined & updated regularly with change • Sufficient resources provided • Objectively and regularly evaluated • Formal training • Capacity & availability mgmt	• Data quality objectives • Measured and data-driven • Historical data and trends • Lessons learned • Performance targets • Cost-benefit analysis	• Root cause analysis • Regular review & assessment • Innovative & agile • Continuous monitoring of outcome-based metrics • Elicit suggestions • Validate improvements • Implement improvements • Evaluate improvement effects

6 RECONCILIATION

The purpose of this section is to reconcile the levels across different maturity frameworks, match those that appear the same, and introduce new levels where they might be different.

Table 4 Harmonizing Maturity Models Together

Maturity Level	0	1	1.5	2	3	4	5
CMMI v1.3	-	Initial-	-	Managed	Defined	Quantitatively Managed	Optimizing
DoE OIG	-	Adhoc	-	Defined	Consistently Implemented	Managed & Measurable	Optimized
C2M2	MIL0	MIL1	-	MIL2	MIL3	-	-
NIST CSF	-	Partial	-	Risk-Informed	Repeatable	Adaptive	-
Long Label	**Don't Know / Not Started**	**Adhoc / As Needed / No Plan**	**Developing / Informal / Under Construction**	**Basic / Managed / Complete**	**Organized / Well-Defined / Company-wide**	**Quantitatively Managed / Measured / Adaptive**	**Optimizing / Continuous Improvement**
Tiny UI Label	Don't Know	Adhoc	Developing	Basic	Defined	Measured	Optimizing
Final Keywords (for use in definition)	don't know, not started, unaware, naive,	initiated, limited awareness, adhoc, reactive, irregular, incomplete, firefighting, delayed, overbudget,	initial, partial, adhoc, reactive, incomplete, developing, not formalized, case-by-case, inconsistent, formative	managed, basic, basic project management, performed, site-specific (not organization-wide), achieves purpose, complete	defined, proactive, standardized, organized, well-defined, organization-wide, formally approved, regularly updated, sufficient resources, well communicated,	quantitatively managed, measured, controlled, data-driven, historical data, metrics adaptive, lessons learned, predictable, forecasting,	optimizing, improving, pivoting, responsive, agile, innovative, closed loop process of execution, measurement, and improvement, institutionalized, self-generating, updated based on changing threat and technology

In the table above, a new level called 'Developing' has been added to explicitly address the shortcoming in other maturity models discussed in section 3 'Low Recognition of "Building the Program" (the formative phase)'.

In the table below, the CMMI requirements are used alongside other frameworks' keywords to produce harmonized requirements.

Table 5 Harmonized Maturity Requirements

Maturity Level	0	1	1.5	2	3	4	5
Tiny UI Label	**Don't Know**	**Adhoc**	**Developing**	**Basic**	**Defined**	**Measured**	**Optimizing**
Final Process Requirements Must accomplish all requirements of the lower level. *No rounding up*.	• None	• Goals established • Responsibility is assigned • Process is performed • Process goals are defined	• Requirements gathered • Policy is established • Process is documented • Tools & technology are implemented (or re-architected) • Stakeholders identified • Third-party guidance is followed (e.g., SANS top 20) • Training started • Evaluation & planning started	• Stakeholder agreement • Approved • Process established & operationalized • Minimum resources provided • Basic project management (requirements, monitoring, review) • Process is managed • Configuration baseline established • Change management • Process is monitored & controlled • Basic training and resources • Site-specific standards • Basic work management • *CMMI ML2 Process Areas fully implemented*	• Executive sponsorship & regular review • Criticality/Risk-based decision making • Proactive processes • Company-wide standardization • Performance measured • Well-defined & updated regularly to changes • Sufficient resources provided • Drills, testing, and verification • Objectively and regularly evaluated • Formal training • Well communicated • Cyber in engineering & cyber acceptance testing • *CMMI ML3 Process Areas fully implemented*	• Data quality objectives • Measured, baselined, and data-driven • Historical data and trends • Historical effort estimates • Outcome-based metrics • Performance analyzed • Performance targets • Cost-benefit analysis • Forecasting • *CMMI ML4 Process Areas fully implemented*	• Continuously use of KPIs • Regular review & assessment • Manage new threats and technology • Lessons learned • Root cause analysis • New ideas elicitation • Validate improvements • Improvements regularly implemented • Evaluate improvement effects • *CMMI ML5 Process Areas fully implemented*

In the table below, the final keywords have been used, along with the simplified CMMI requirements, to develop a written definition for each harmonized maturity level.

Table 6 Harmonized Maturity Level Definition

Maturity Level	0	1	1.5	2	3	4	5
Tiny UI Label	**Don't Know**	**Adhoc**	**Developing**	**Basic**	**Defined**	**Measured**	**Optimizing**
Written Definition (based on keywords and requirements)	Process or technical control has not started or entirely unknown.	Process or technical control occurs as needed in an adhoc, unplanned, and limited way as an assumed duty of existing personnel.	Process or technical control is being performed in an informal way, planning has started, policies/processes are still being developed, tools are being deployed, and training has started.	Process or technical control is implemented, but managed, monitored, and controlled in a basic way. Standardized (per-facility) with basic project management, requirements, work management, training, and completion.	Process or technical control is well-defined, standardized company-wide, sufficient resources, with performance measured. Decision making is criticality and risk-based. It is objectively evaluated, proactive, tested, verified, and well communicated with stakeholders & Executives.	Process or technical control is measured, data-driven, with data quality objectives, historical trends, and performance targets. Performance is analyzed, compared to targets/baselines, anomalies detected, and improvements identified. Allows more accurate estimating, forecasting, responsiveness, adaptive to change, and risk-based decision-making.	Process or technical control has a closed loop of process execution, measurement, and improvement. It is continuously improving, agile, and responsive to change. Opportunities to improve come from new threats, new technology, root cause analysis, lessons learned, elicitation of ideas, and are formally validated, regularly implemented, and improvements evaluated.

6.1 SUMMARIZED RESULT

	0	1	1.5	2	3	4	5
CMMI	Unknown	Initial	Construction in Progress (% complete)	Managed	Defined	Quantitatively Managed	Optimizing
C2M2	MIL0	MIL1		MIL2	MIL3	-	-
CSF	-	Partial		Risk-Informed	Repeatable	Adaptive	-
	Don't Know / Not Started	**Adhoc / As Needed / No Plan**	**Developing / Informal / Under Construction**	**Basic / Managed / Complete**	**Organized / Well-Defined / Company-wide**	**Quantitatively Managed / Measured / Adaptive**	**Optimizing / Continuous Improvement**
Definitions	Process or technical control has not started or entirely unknown.	Process or technical control occurs as needed in an adhoc, unplanned, and limited way as an assumed duty of existing personnel.	Process or technical control is being performed in an informal way, planning has started, policies/processes are still being developed, tools are being deployed, and training has started.	Process or technical control is implemented, but managed, monitored, and controlled in a basic way. Standardized (per-facility) with basic project management, requirements, work management, training, and completion.	Process or technical control is well-defined, standardized company-wide, sufficient resources, with performance baselines. Decision making is criticality and risk-based. It is objectively evaluated, proactive, tested, verified, and well communicated with stakeholders & Executives.	Process or technical control is measured, data-driven, with data quality objectives, historical trends, and performance targets. Performance is analyzed, compared to targets/baselines, and improvements identified. Allows more accurate estimating, forecasting, and risk-based decision-making.	Process or technical control has a closed loop of process execution, measurement, and improvement. It is continuously improving, agile, and responsive to change. Opportunities to improve come from new threats, new technologies, root cause analysis, lessons learned, elicitation of ideas, and are formally validated, regularly implemented, and improvements evaluated.
Requirements Checklist	❑ None	❑ Goals established ❑ Responsibility is assigned ❑ Process is performed ❑ Process goals are defined	❑ Requirements gathered ❑ Policy is established ❑ Process is documented ❑ Tools & technology are implemented (or re-architected) ❑ Stakeholders identified ❑ Third-party guidance is followed ❑ Training started ❑ Evaluation & planning started	❑ Stakeholder agreement ❑ Approved ❑ Process established & operationalized ❑ Minimum resources provided ❑ Basic project management (requirements, monitoring, review) ❑ Process is managed ❑ Configuration baseline established ❑ Change management ❑ Process is monitored ❑ Process is controlled ❑ Basic training and resources ❑ Site-specific standards ❑ Basic work management ❑ *CMMI ML2 Process Areas fully implemented*	❑ Executive sponsorship & regular review ❑ Criticality/Risk-based decision making ❑ Proactive processes ❑ Company-wide standardization ❑ Performance baseline established ❑ Well-defined & updated regularly to changes ❑ Sufficient resources provided ❑ Drills, testing, and verification ❑ Objectively and regularly evaluated ❑ Formal training ❑ Well communicated ❑ Cyber in engineering & cyber acceptance testing ❑ *CMMI ML3 Process Areas fully implemented*	❑ Data quality objectives ❑ Measured and data-driven ❑ Historical data and trends ❑ Historical effort estimates ❑ Outcome-based metrics ❑ Performance analyzed ❑ Performance targets ❑ Cost-benefit analysis ❑ Forecasting ❑ *CMMI ML4 Process Areas fully implemented*	❑ Continuously use of KPIs ❑ Regular review & assessment ❑ Manage new threats & technologies ❑ Lessons learned ❑ Root cause analysis ❑ New ideas elicitation ❑ Validate improvements ❑ Improvements regularly implemented ❑ Evaluate improvement effects ❑ *CMMI ML5 Process Areas fully implemented*
		Implementing / Building Checklist-based, Doing the Obvious, Catching up, Basic Hygiene, Tooling			**Operationalize, Optimize** Tipping Point: Start of Risk-based Decision-making		

7 APPLICATION AND USE

The primary intent of creating this harmonization document, is similar to the intent of the NIST CSF. It is to create a common framework for communicating cybersecurity maturity, regardless of the framework chosen. Multiple use-cases can apply this harmonized maturity model in the real-world.

7.1 USE-CASES FOR OT CMJ (HARMONIZED OT CYBERSECURITY MATURITY JOURNEY)

The purpose of this section is to outline practical, defensible ways to apply the OT CMJ now that a more robust, consistent and harmonized maturity scale, definitions, and crosswalk exist.

1. **Translation and benchmarking across organizations using different maturity models**
   OT CMJ enables a consistent "translation layer" between maturity models (e.g., CMMI, C2M2 MILs, and NIST CSF Tiers) so asset owners can benchmark peers, business units, and sites even when different frameworks are used. This aligns with how C2M2 is positioned: enabling organizations to evaluate capabilities consistently, communicate levels meaningfully, and benchmark progress over time.

2. **Standardization and a starting point for future iterations (reducing maturity-model proliferation)**
   OT CMJ provides a practical baseline: rather than creating yet another maturity model, new sector- or company-specific efforts can begin from a harmonized vocabulary, level definitions, and mapping logic.

3. **Risk-informed target setting and roadmap planning (enterprise, site, and domain)**
   OT CMJ supports establishing *target maturity* by site/system criticality and then building a multi-year roadmap to close gaps. This mirrors best practice usage of maturity models: use the assessment to prioritize improvement actions and investments rather than to produce a one-time "grade."

4. **Executive reporting and governance (Current vs. Target posture, in one language)**
   OT CMJ can be used to produce a clear "Current vs Target" maturity story for leadership and boards, including a prioritized plan to close gaps. This pairs well with NIST CSF's concept of Organizational Profiles (Current and Target) as a mechanism to assess, prioritize, and communicate cybersecurity outcomes and improvement priorities.

5. **Capital planning and investment justification (cost/benefit narratives)**
   OT CMJ enables structured justification for funding by connecting maturity moves (e.g., Level 1.5 → 2) to expected reductions in exposure, improved resilience, or reduced operational risk. When combined with quantitative or semi-quantitative methods (including FAIR where applicable), it supports defensible "why this, why now" prioritization.

6. **Assessment repeatability and assurance (reducing subjectivity and scoring drift)**
   OT CMJ can function as a standardized assessment backbone to reduce the known issues of subjectivity and inconsistency: sites can be assessed on a consistent scale, over time, with clearer evidence expectations. This increases defensibility for internal audit, external assurance, or regulator-facing reporting.

7. **OT lifecycle integration (project gates and operational acceptance criteria)**
   OT CMJ can be embedded into engineering and operational workflows as "maturity gates" (e.g., for new builds, upgrades, turnarounds): a system cannot transition to operations until minimum maturity expectations are met for access governance, inventory accuracy, backup/restore validation, and monitoring.

8. **Sector or consortium benchmarking programs (apples-to-apples measurement)**
   OT CMJ can serve as a neutral cross-sector benchmark layer to support industry groups or owner/operator

consortia. This aligns directly with the intent seen in C2M2 variants: consistent evaluation, shared references, and repeatable measurement of progress across participants.

9. **Strategic clarity: separating "Security Level (SL)" from "Maturity Level (ML)"**
   OT CMJ enables a clear two-dimensional framing that reduces persistent confusion in OT security discussions:

   - **Security Level (SL)** measures the *technical strength* of controls/safeguards (i.e., how robust the technical requirements are against classes of attackers).
   - **Maturity Level (ML)** measures *how well those controls are governed, implemented, repeated, measured, and improved* (i.e., the management system and institutionalization behind the controls).

   In practice, SL and ML are not interchangeable; they are separate dimensions. Framing OT CMJ explicitly as the **maturity dimension** helps avoid treating a maturity score as proof of technical hardening, and vice versa.

Referring back to section 3 'Known Issues with Existing Maturity Frameworks', many of the use-cases above are inhibited by insufficiently developed maturity frameworks.

7.2 Next Steps and Additional Research

With a harmonized maturity model, that has reduced subjectivity and increased consistency across different teams/regions/industries, attention can be drawn to higher order challenges.

1. **Control and Domain-specific Requirements**
   The requirements in Table 5 Harmonized Maturity Requirements can now be applied to NIST CSF Functions, Categories, or other cybersecurity control ontologies to develop specific requirements in each cybersecurity domain. What is generally lacking in industry is "what comes next" or "how do I advance this control to the next level". If incident response is assessed at level 2 Basic, what are specific requirements that are missing in the incident response domain that would allow the entity to advance to level 3 Defined maturity level? See figure below for proof of concept example.

Maturity Level	0 Don't Know / Not Started **Don't Know**	1 Adhoc / As Needed / No Plan **Adhoc**	1.5 Developing / Informal / Under Construction **Developing**	2 Basic / Managed / Complete **Basic**	3 Organized / Well-Defined / Company-wide **Defined**	4 Quantitatively Managed / Measured / Adaptive **Measured**	5 Optimizing / Continuous Improvement **Optimizing**	6 Autonomous **Auto**
Network Perimeter			Shared with IT	Isolated✓	DMZ✗	Dynamic rules✓	Reviewed regularly, KPI driven	
Malware Prevention		Classic antivirus, blacklisting,	Centrally Managed	Gen2 AV,✓ USB kiosk,✗	Device control,✗ AWL,✗	Malware indicators & metrics,✓	Malware KPIs,	
Logging & Auditing		Basic logging enabled	Advanced local logging	Log Forwarding,✓ SIEM✓	Regular SIEM/SOAR tuning,	Indicators & metrics✗	Logging KPIs	
Access Controls		Default passwords	Distributed Auth, Shared admins,	Site Active Dir, group policies,✓	Hardening standards✗	Hardening compliance	Hardening KPIs	
Remote Access		Free SRA tools		MFA from Internet,✓ Jump host,✓	MFA from Corp,✗			

2. **Negative Indicators**
   The concept of negative indicators is just starting to emerge and will compliment cybersecurity maturity frameworks very well. Negative indicators are observations or findings that undermine the efforts of the cybersecurity program, that when found provide strong indication of a particular maturity level. This idea has been in my mind [Donovan Tindill] for a decade. For example, if ICS/OT documentation is out of date, it is a strong negative indicator that change control & configuration management is low maturity. Recently emerging in the UK Cyber Assessment Framework are its 'Not Achieved' requirements and the Australia Energy Sector Cyber Security Framework (AESCSF) 'Anti-Patterns'. These compliment maturity level requirements, as negative indicators would downgrade or prove a lower level. Next steps in this area of research would involve expanding these negative indicators, and extending them into control-specific domains as well.

3. **Data-Driven Maturity Indicators and Metrics**
   Once control and domain-specific requirements are established, it helps reveal telemetry or other metrics as leading or lagging indicators that an entity is at a particular maturity level. Through cybersecurity assessments correlated with key metrics like 'annual OT cyber budget', 'Percent assessed for vulnerabilities', or 'patching interval' it will reveal how these metrics generally align with maturity indicator levels. Before this can happen, a more granular maturity model is needed (this document) as well as control-specific requirements. See figure below for proof of concept example.

Maturity Indicator	0	1	1.5	2	3	4	5	6
	Don't Know / Not Started	Adhoc / As Needed / No Plan	Developing / Informal / Under Construction	Basic / Managed / Complete	Organized / Well-Defined / Company-wide	Quantitatively Managed / Measured / Adaptive	Optimizing / Continuous Improvement	Autonomous
	Don't Know	**Adhoc**	**Developing**	**Basic**	**Defined**	**Measured**	**Optimizing**	**Auto**
Mean Days b/w Vuln discovery			<24mos	<12mos	<6mos	<1mos	<10d	
% Assessed for Vulnerabilities	0%		>40%	>60%	>80%	>95%	>97%	
Patching Interval		>14mos	<14mos	<7mos	<90d	<30d		
Mean Time to Remediate (site)				<24mos	<14mos	<6mos	<3mos	
Mean Time to Remediate (DMZ)			<14mos	<6mos	<2mos	<32d		
Last Tabletop DR Exercise		Never	<38mos	<26mos	<14mos	<7mos		
% Coverage for ...			>40%	>60%	>80%	>95%	>97%	

4. **Risk modeling via effectiveness coefficients by maturity level**
   OT CMJ levels can be treated as an input variable to quantitative or semi-quantitative risk models by assigning "effectiveness coefficients" to each maturity level (or to specific capability groups within a level). This supports estimating relative risk reduction from moving between levels and helps compare candidate investments on a common basis. If an organization uses quantitative methods, OT CMJ can be paired with a quantification approach such as FAIR or DeNexus DeRISK to express changes in risk in measurable terms (e.g., frequency/magnitude of loss events).

This document represents the first deliverable in a planned series of artifacts related to the OT Cybersecurity Maturity Journey. Some of the ideas above may be addressed in future deliverables.