Cyber Resilience Tools and Models

Brian Benestelli

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0189

Agenda

Introduction

Core Concepts

CERT Models and Assessments

C2M2

Questions

About Me

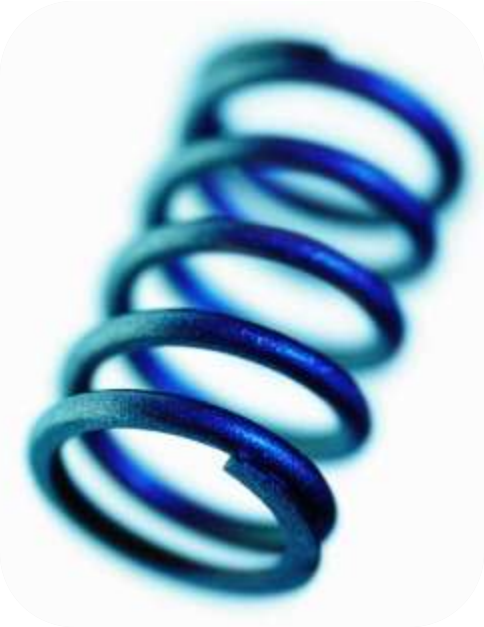
Brian Benestelli
Cybersecurity Engineer

Cybersecurity Assurance Team
CERT Division
Software Engineering Institute

bdbenestelli@cert.org

Core Concepts

What is Resilience?



"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

– Presidential Policy Directive – PPD 21
Critical Infrastructure Security and Resilience
February 12, 2013

This definition explicitly includes ***attacks, accidents, or naturally occurring threats or incidents,*** intentionally expanding resilience beyond a cyber definition.

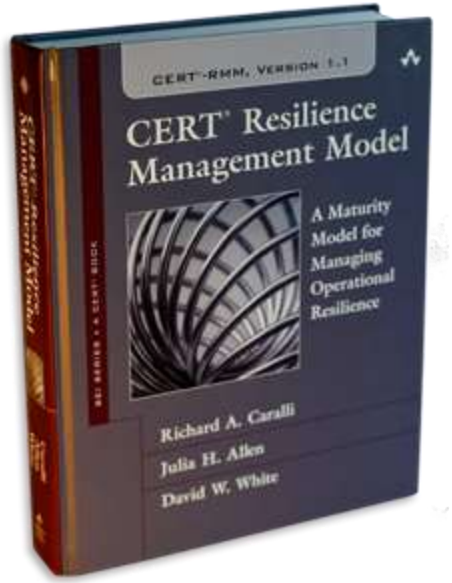
What Do We Mean by *Operational Resilience*?

***"Operational resilience:** the organization's ability to adapt to risk that affects its core operational capacities; the **emergent** property of an organization that can **continue to carry out its mission** after disruption that does not exceed its operational limit"*

– CERT-RMM

Operational resilience expands on the PPD 21 definition of resilience, which emphasizes the need to define operational limits while stressing the emergent nature of resilience.

What is the CERT-RMM?



The CERT Resilience Management Model (CERT-RMM) is a process improvement model for managing operational resilience.

It provides guidelines and practices for

- converging security, business continuity, disaster recovery, and IT ops
- implementing, managing, and sustaining operational resilience activities
- managing operational risk through process
- measuring and institutionalizing the resilience process

CERT-RMM provides a common vernacular and basis for planning, communicating, and evaluating improvements.

It is organized into 26 process areas.

Maturity Models

"A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline." – C2M2 V2.0

Attributes define levels in a maturity model

- Capability progression: crawl, walk, run
- Process maturity: institutionalization (a.k.a., what makes it "stick")

Having measurable transitions between the levels enables an organization to use the scaling to

- define its current state
- define its future, more "mature" state
- identify the attributes it must attain to reach that future state

Assessments and Models

CRR, EDM, and CRA

CISA (link)

- Cyber Resilience Review
- External Dependency Management Assessment

DC3 DCISE

- Cyber Resilience Analysis

CYBER RESILIENCE ANALYSIS

Goal 2 - A process for identifying and analyzing vulnerabilities is established and maintained.		Yes	Incomplete	No
1. Have sources of vulnerability information been identified? [VAR:SG2.SP1]				
	Information	☐	☐	☐
	Technology	☐	☐	☐
	Facilities	☐	☐	☐
2. Is the information from these sources kept current? [VAR:SG2.SP1]				
	Information	☐	☐	☐
	Technology	☐	☐	☐
	Facilities	☐	☐	☐
3. Are vulnerabilities being actively discovered? [VAR:SG2.SP2]				
	Information	☐	☐	☐
	Technology	☐	☐	☐
	Facilities	☐	☐	☐

Process Institutionalization

Maturity indicator levels (MILs) are used to measure process institutionalization.

Higher degrees of institutionalization translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

Cybersecurity Maturity Model Certification (CMMC)

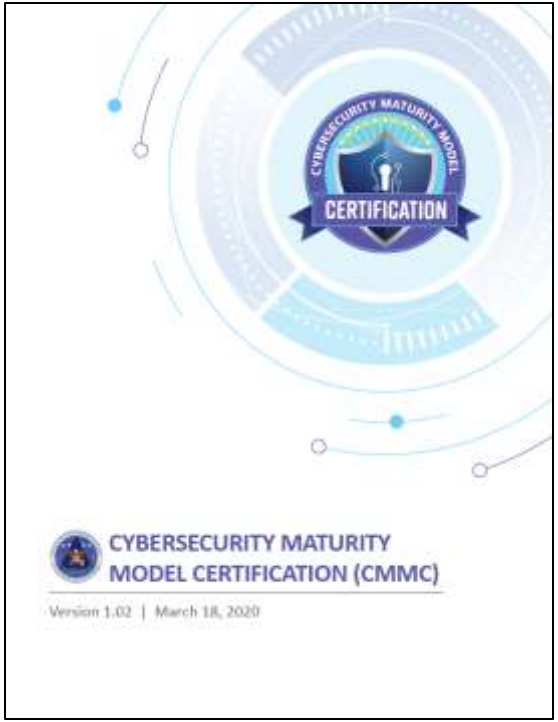
Measures implementation of NIST SP 800-171 Rev 2 security requirements to protect controlled unclassified information (CUI)

Practices originate from FAR Clause 52.204-21 and DFARS Clause 252.204-7012

Version 2.0 released in Dec ’21 was significantly changed from V1.02

- Elimination of maturity processes
- 5 Levels -> 3 Levels
- Elimination of 20 “delta” practices
- Self-assessments and POA&Ms

Once rulemaking is complete, this will become a contract requirement for all defense contractors



OUSD A&S website

Cybersecurity Capability Maturity Model (C2M2)

Cybersecurity Capability Maturity Model (C2M2)

C2M2 is a scalable, sector-specific mechanism that energy sector organizations use to evaluate, prioritize, and improve their cybersecurity capabilities

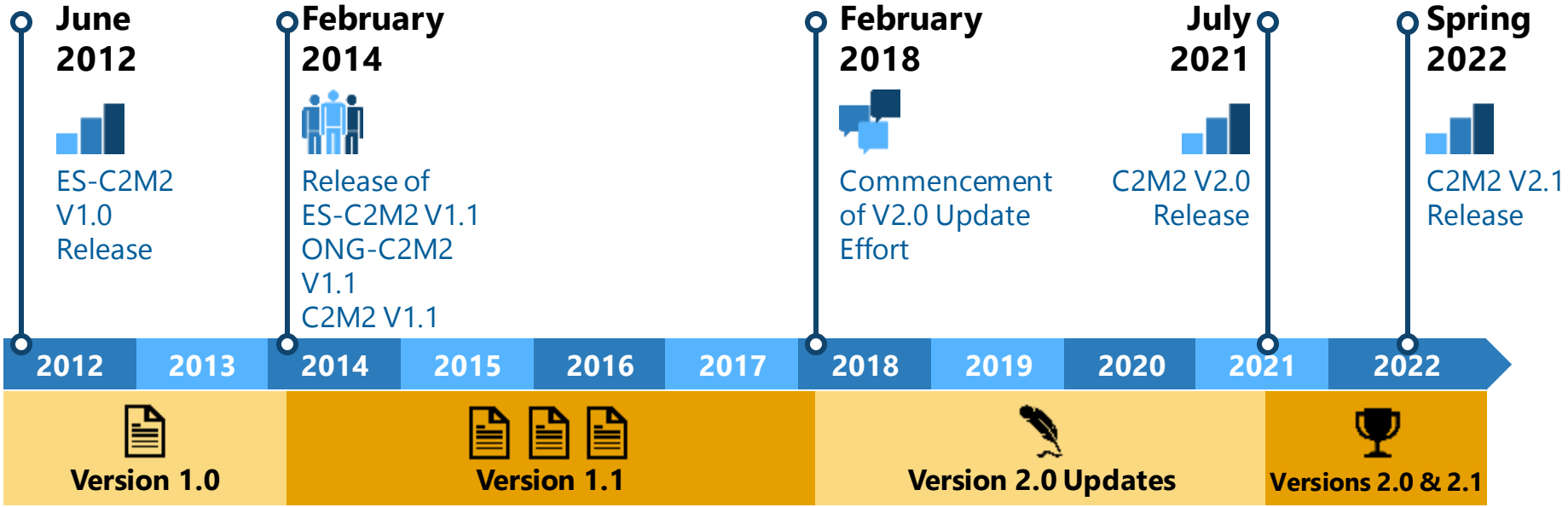
Designed for the energy sector

Developed through a public-private partnership with U.S. electricity, natural gas, and oil companies

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

[DOE C2M2 Program Page]

C2M2 Model Evolution

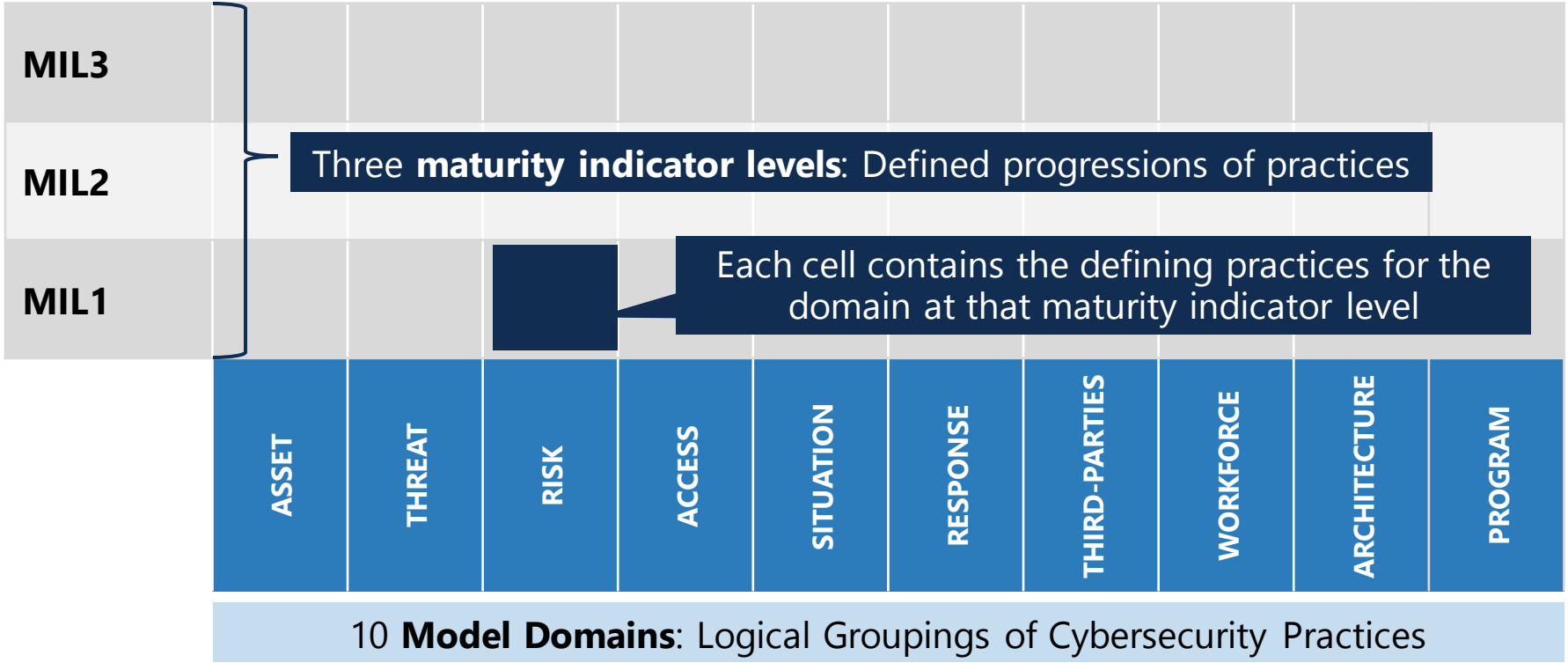


Model Domains

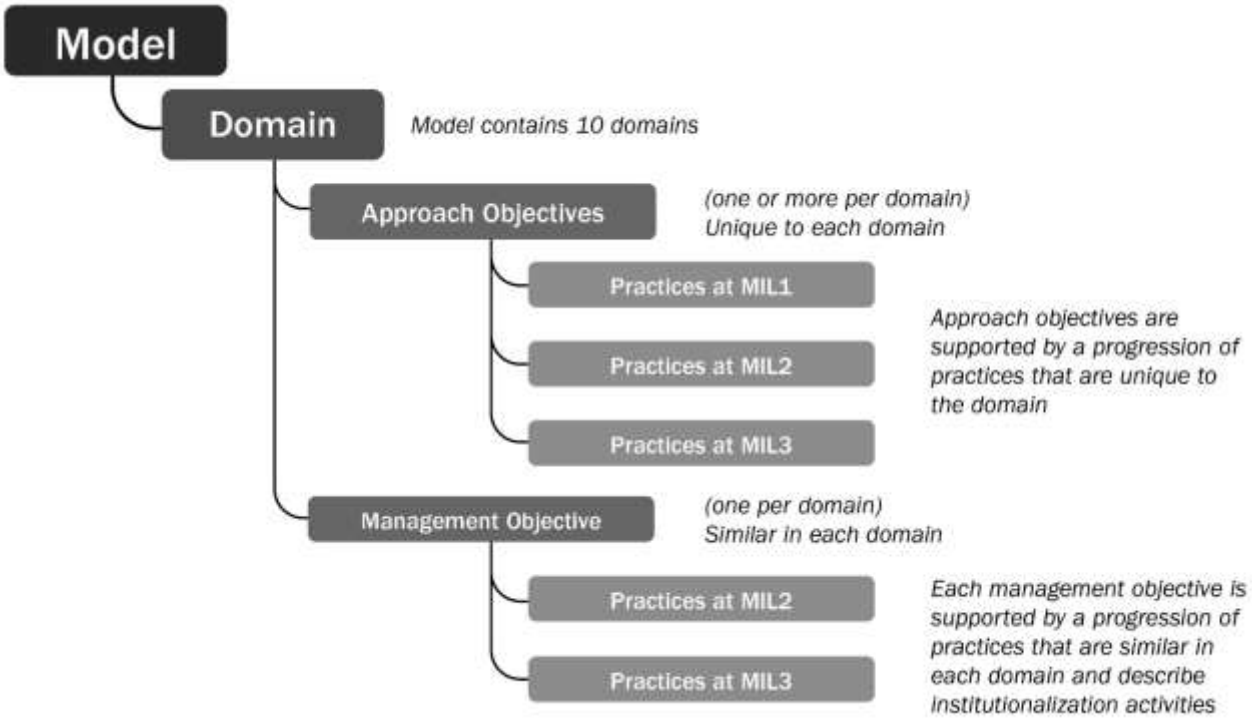
ASSET	Asset, Change, and Configuration Management
THREAT	Threat and Vulnerability Management
RISK	Risk Management
ACCESS	Identity and Access Management
SITUATION	Situational Awareness
THIRD-PARTIES	Third-Party Risk Management
RESPONSE	Event and Incident Response, Continuity of Operations
ARCHITECTURE	Cybersecurity Architecture
WORKFORCE	Workforce Management
PROGRAM	Cybersecurity Program Management

- Domains are logical groupings of cybersecurity practices
- Each domain has a short name that cross-references with the self-evaluation tool

Model at a Glance



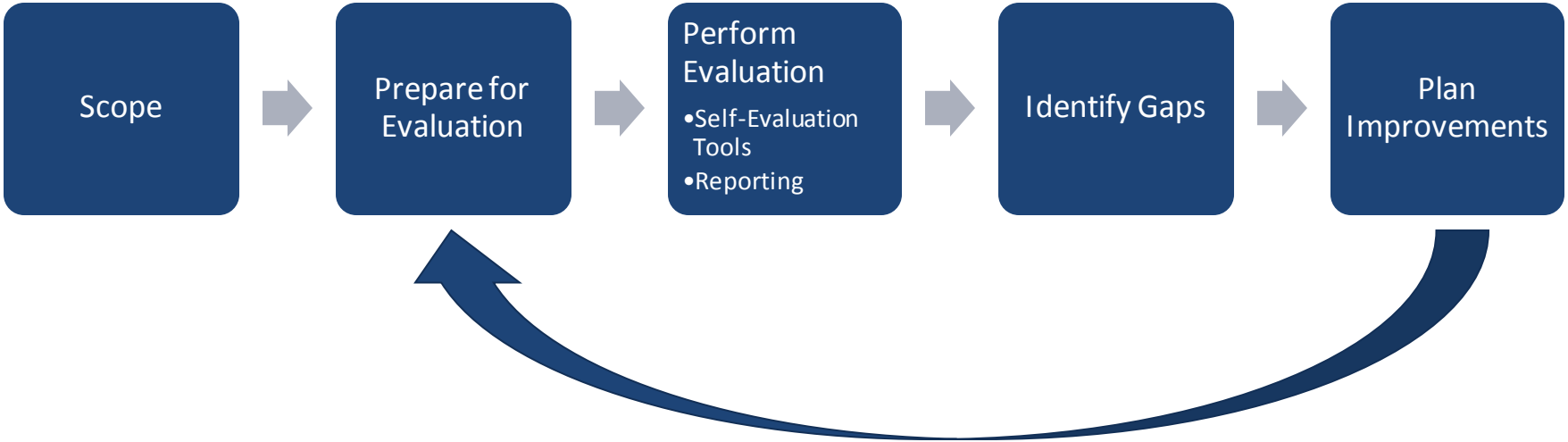
Organization of a Domain



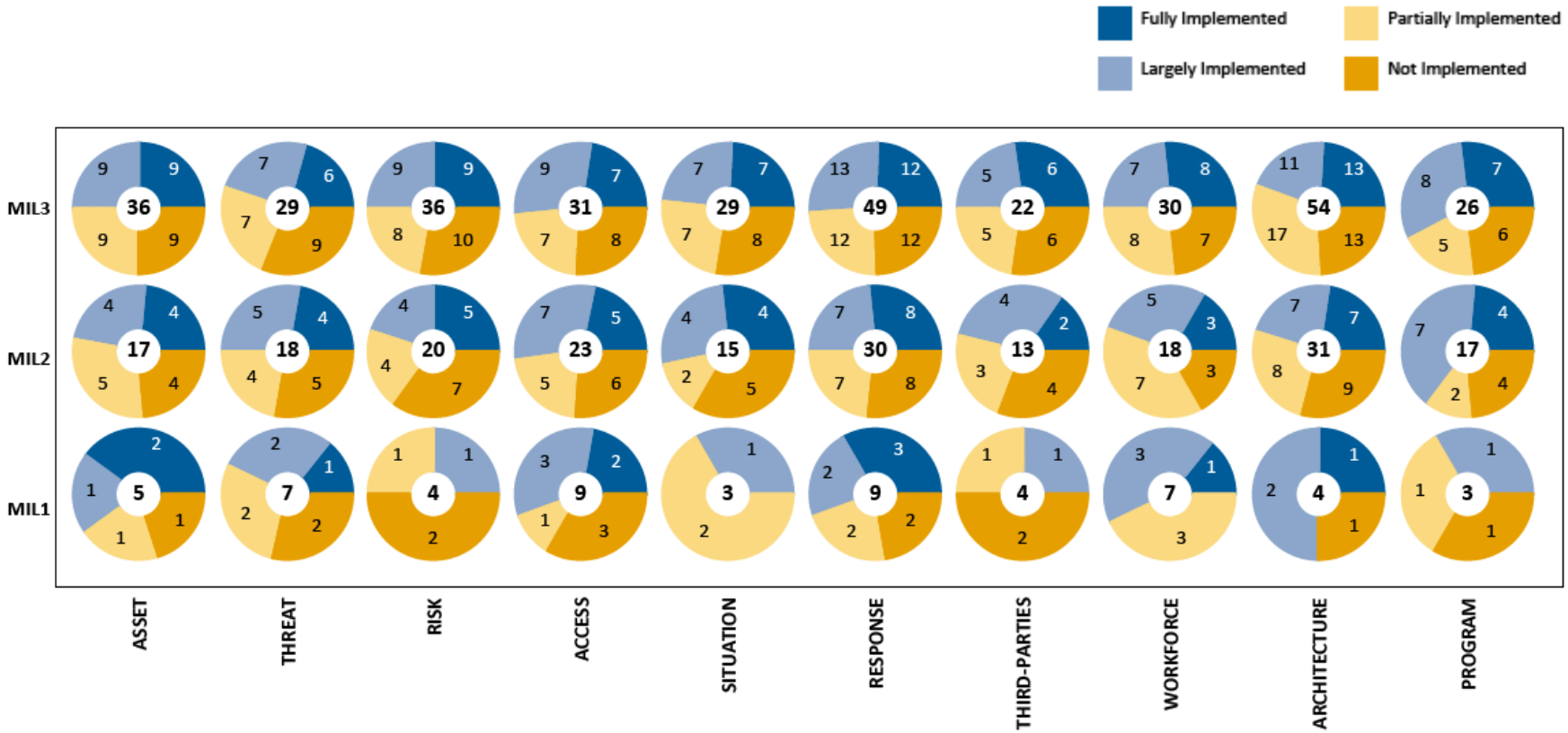
Maturity Indicator Levels

Level	Description
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 at MIL1
MIL3	**Management Characteristics** ▪ Activities are guided by policies or other organizational directives ▪ Personnel performing the practices have adequate skills and knowledge ▪ Responsibility, accountability, and authority for performing the practices are assigned ▪ The effectiveness of activities in the domain is evaluated and tracked **Approach Characteristic** ▪ Practices are more complete or advanced than at MIL2

How does it work?



C2M2 Reporting



[C2M2 Online Tool]

[PDF tool can be requested from DOE]

Thank you!

Questions?