Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (Case Study)

James Stevens
Senior Member, Technical Staff - CERT® Division

James Stevens is a senior member of the technical staff in the CERT Program at Carnegie Mellon University's Software Engineering Institute. James has been working in the information security field for over eighteen years and holds a BS degree in Electrical Engineering from the University of Notre Dame and an MBA from Carnegie Mellon University's Tepper School of Business. James currently performs information and infrastructure security and resilience research and develops methods, tools, and techniques that support the secure and resilient delivery of critical services.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
23 JAN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Electricity Subsector Cybersecurity Capability Maturity Model	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**38**	

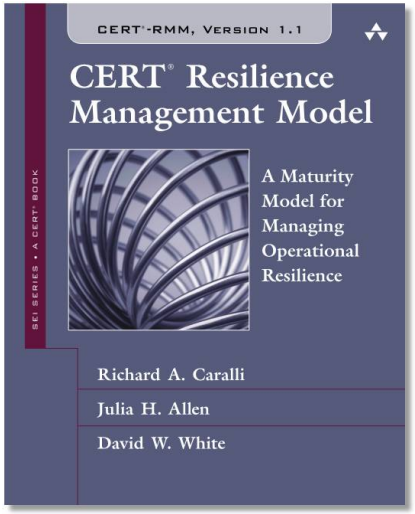
Notices

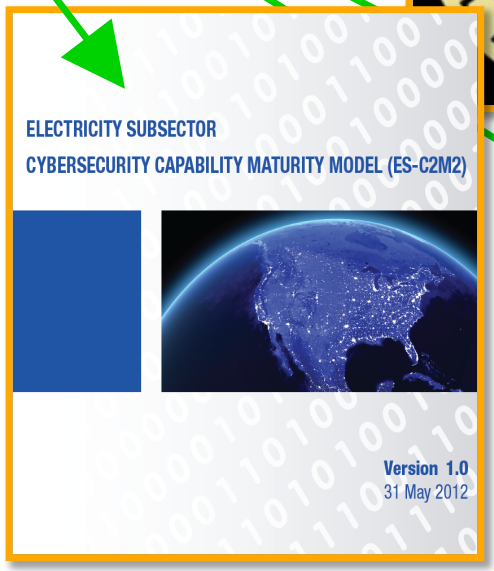
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

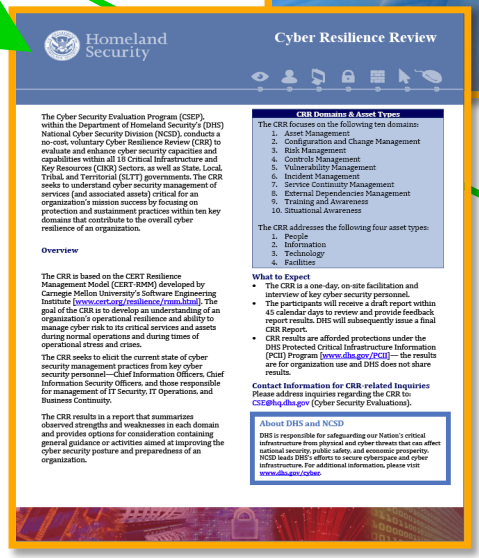
Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0000906

A Sampling of CERT-RMM Applications and Derivatives







Contents

ES-C2M2 History and Background

ES-C2M2 Genesis – January 2012

the WHITE HOUSE PRESIDENT BARACK OBAMA

THE WHITE HOUSE WASHINGTON

BLOG | PHOTOS & VIDEO | BRIEFING ROOM | ISSUES | the ADMINISTRATION

Home • The White House Blog

The White House Blog

Protecting the Nation's Electric Grid from Cyber Threats

Howard A. Schmidt

January 09, 2012

03:58 PM EDT

Share This Post

Protecting the electric system from cyber threats and ensuring its resilience are vital to our national security and economic well-being. This is exactly why cybersecurity is one of four key themes in the White House's Policy Framework for a 21st Century Grid. For obvious reasons, the private sector shares our interest in a safe and secure electric grid. The Administration has benefited from working closely with industry, including to develop the Roadmap to Achieve Energy Delivery Systems Cybersecurity, released by the Department of Energy last September.

To continue that close cooperation, last week Deputy Secretary of Energy Dan Poneman and I, along with senior officials from Department of Homeland Security, hosted industry leaders to discuss a new initiative to further protect the electric grid from cyber risks. This initiative – the Electric S[illegible]ybersecurity Risk Ma[illegible]ity [illegible]t – is a new White

ES-C2M2 Background

White House initiative

Led by Department of Energy

In partnership with Department of Homeland Security

In collaboration with representatives of electricity subsector asset owners and operators

ES-C2M2 Challenge and Objectives

Challenge:

Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid

Objectives:

- Strengthen cybersecurity capabilities
- Enable consistent evaluation and benchmarking of cybersecurity capabilities
- Share knowledge and best practices
- Enable prioritized actions and cybersecurity investments

ES-C2M2 Approach and Results

Approach:

- Create a maturity model and self-evaluation survey to develop and measure cybersecurity capabilities
- Encourage public–private collaboration effort
- Leverage existing guidance and knowledge

Results:

- A scalable, sector-specific model created in partnership with industry

ES-C2M2 Collaboration

Model Architect

Edison Electric Institute
Power by Association

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Software Engineering Institute
Carnegie Mellon University

National Rural Electric Cooperative Association
A Touchstone Energy® Cooperative

National Electric Sector Cybersecurity Organization

INL Idaho National Laboratory

APPA American Public Power Association
PublicPower.org

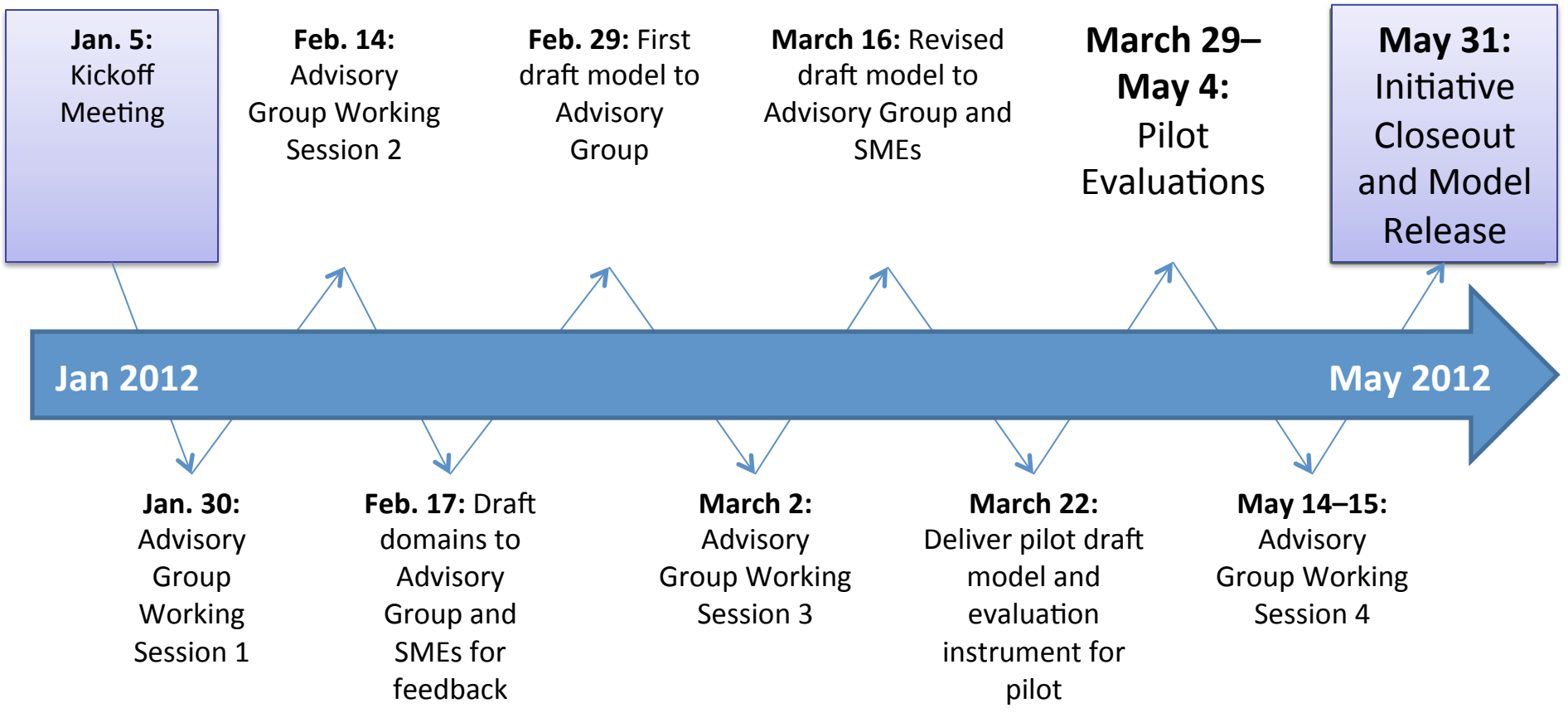
NIST National Institute of Standards and Technology
U.S. Department of Commerce

Pacific Northwest NATIONAL LABORATORY

And numerous utilities, including

Southern California Edison	Bonneville Power Administration	Pacific Gas & Electric
Electric Reliability Council of Texas	Dominion Resources	American Electric Power

Short Model-Development Time Frame



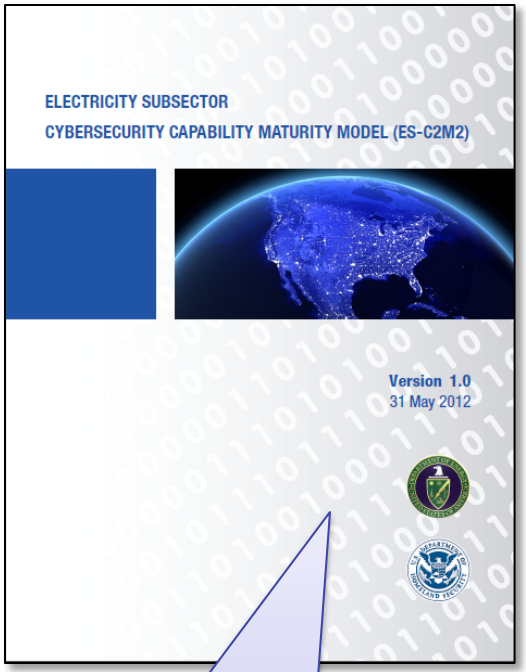
ES-C2M2 Resulting Artifacts

The Model

- http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012

Self-Evaluation Tool Requests,
Requests for Facilitation, & Questions

- ES-C2M2@doe.gov



- 94-page document
- The model itself is only 45 pages

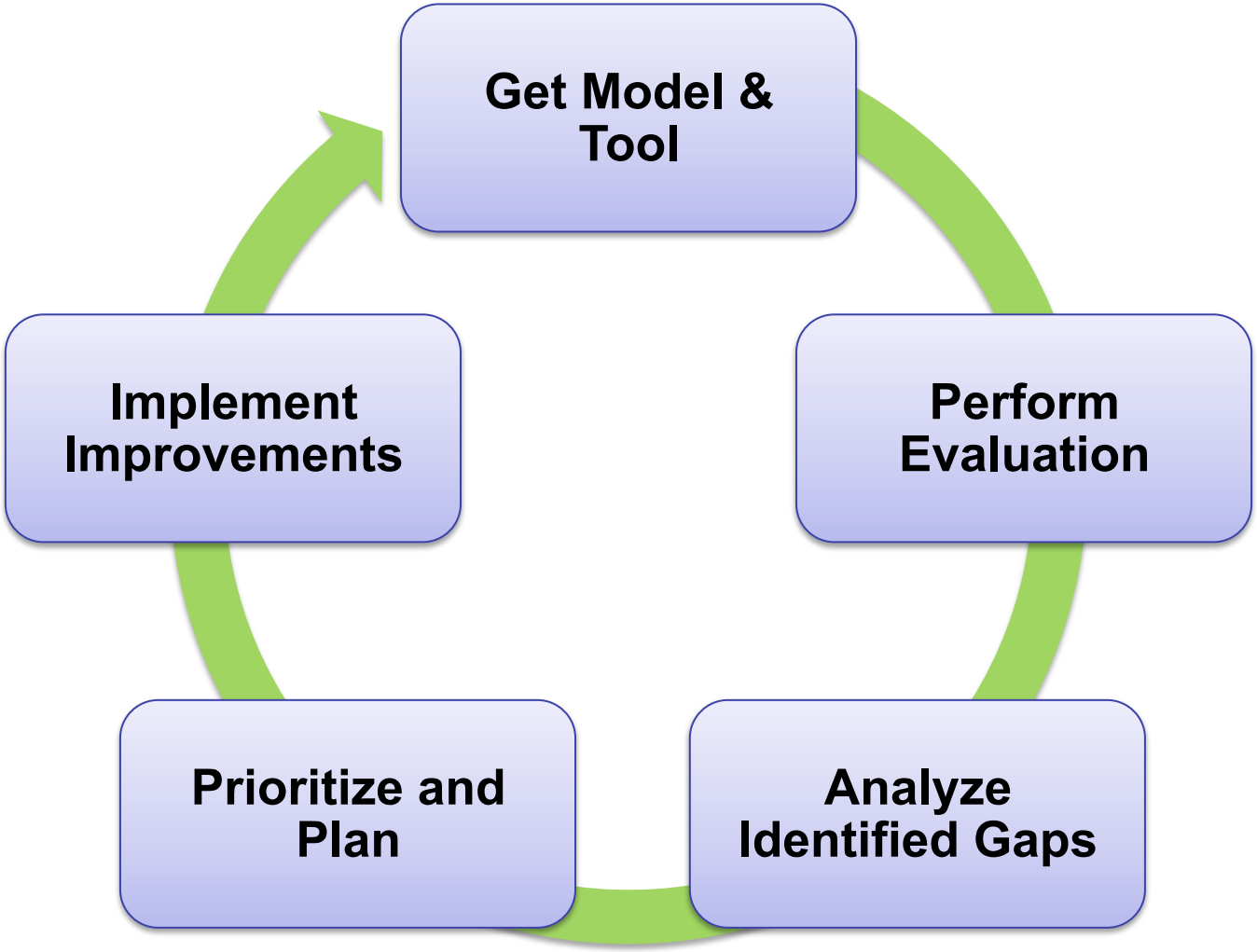
ES-C2M2: Industry Use and Adoption

Data as of 06/05/2013

Requesting entity type	Organizations[1]	Individuals[2]
Utilities		
Cooperative (COOP)	14	14
International	3	3
Investor-owned (IOU)	42	51
Public power (Muni)	37	47
Regional Transmission Organization (RTO)	3	3
Total Utilities	**99**	**118**
Non-utilities	**79**	**86**
International	**20**	**20**
TOTAL	**198**	**224**

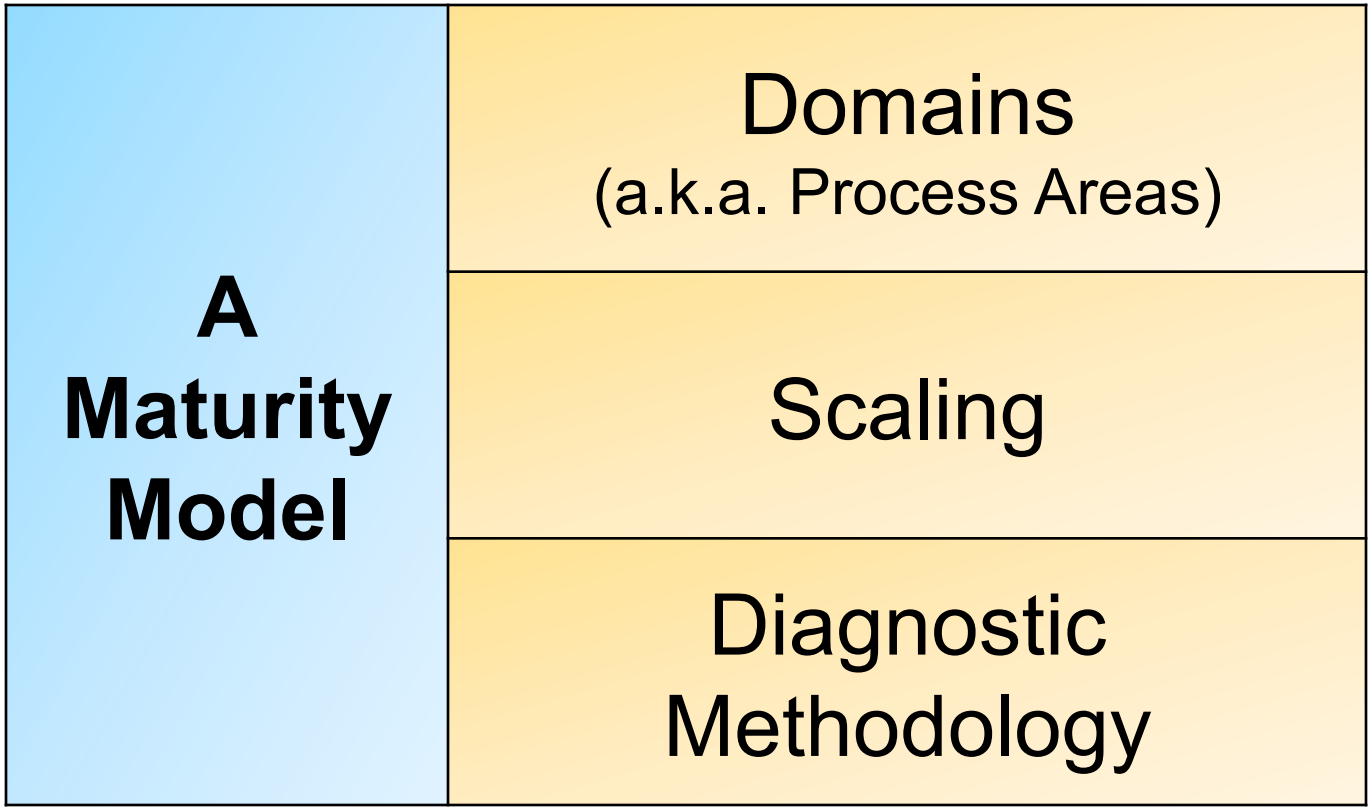
1. *Total number of unique organizations that have received the ES-C2M2 Self-Evaluation Toolkit.*
2. *Total number of unique individuals who have received the ES-C2M2 Self-Evaluation Toolkit.*

Using ES-C2M2



Overview of ES-C2M2 Model

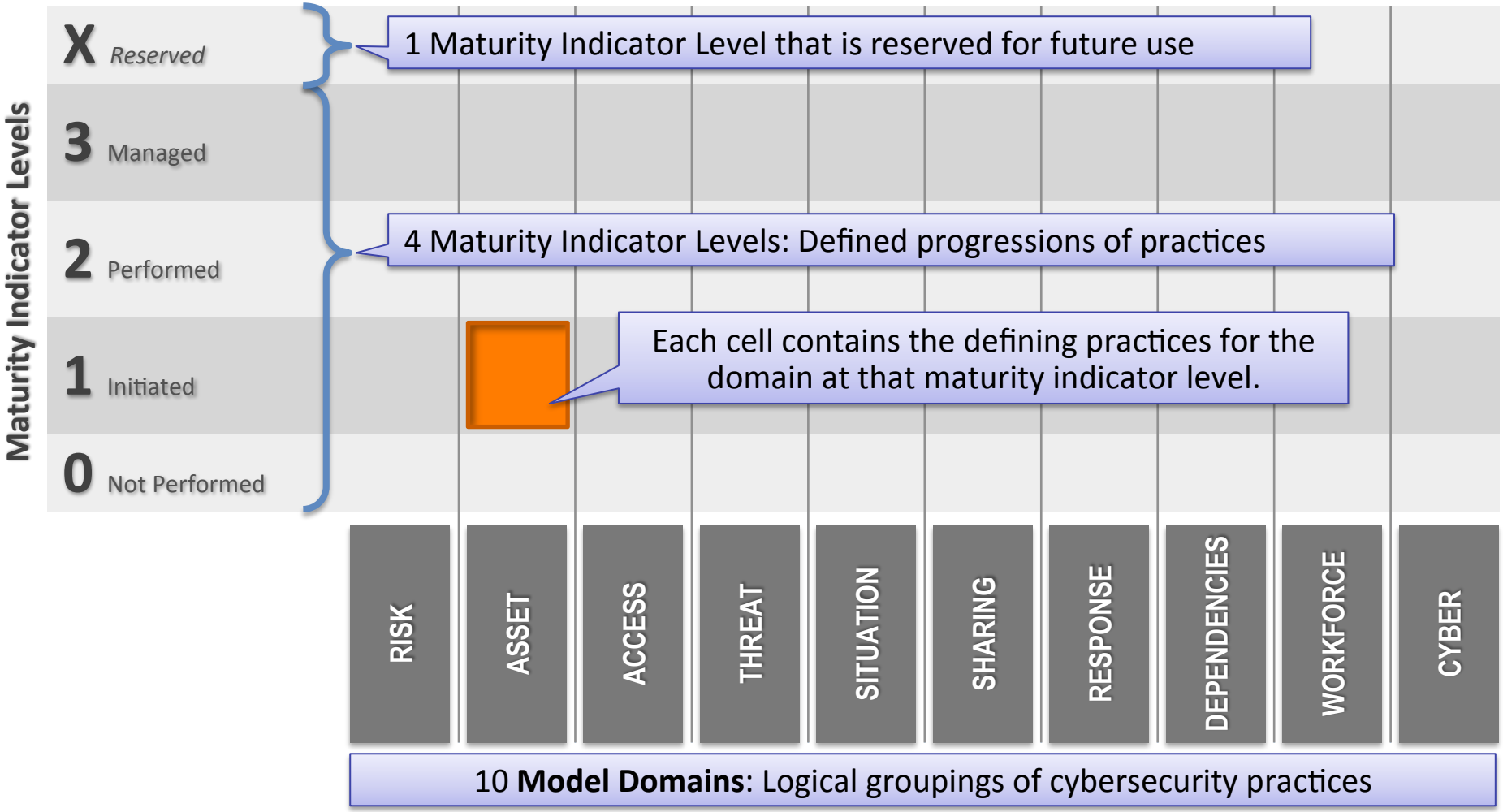
ES-C2M2



Domains that ES-C2M2 Examines

Domains are logical groupings of cybersecurity practices.

ES-C2M2 Structure



ES-C2M2 Maturity Indicator Levels Example

	Specific Characteristics for the ASSET Domain
MIL0	
MIL1	1. Asset inventory a. There is an inventory of OT (operational technology) and IT (information technology) assets that are important to the delivery of the function. …
MIL2	…
MIL3	1. Asset inventory a. The asset inventory is current and complete for assets of defined categories that are selected based on risk analysis. b. Asset prioritization is informed by risk analysis. …

Progress from one MIL to the next involves more complete or more advanced implementations of the core activities in the domain.

The organization is also expected to perform additional activities at higher levels consistent with its risk strategy.

ES-C2M2 Maturity Indicator Levels

Level	Name	Description
MIL0	Not Performed	• MIL1 has not been achieved in the domain.
MIL1	Initiated	• Initial practices are performed, but may be ad hoc.
MIL2	Performed	• Practices are documented. • Stakeholders are involved. • Adequate resources are provided for the practices. • Standards or guidelines are used to guide practice implementation. • Practices are more complete or advanced than at MIL1.
MIL3	Managed	• Domain activities are guided by policy (or other directives). • Activities are periodically reviewed for conformance to policy. • Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge. • Practices are more complete or advanced than at MIL2.

A Dual-Progression Model

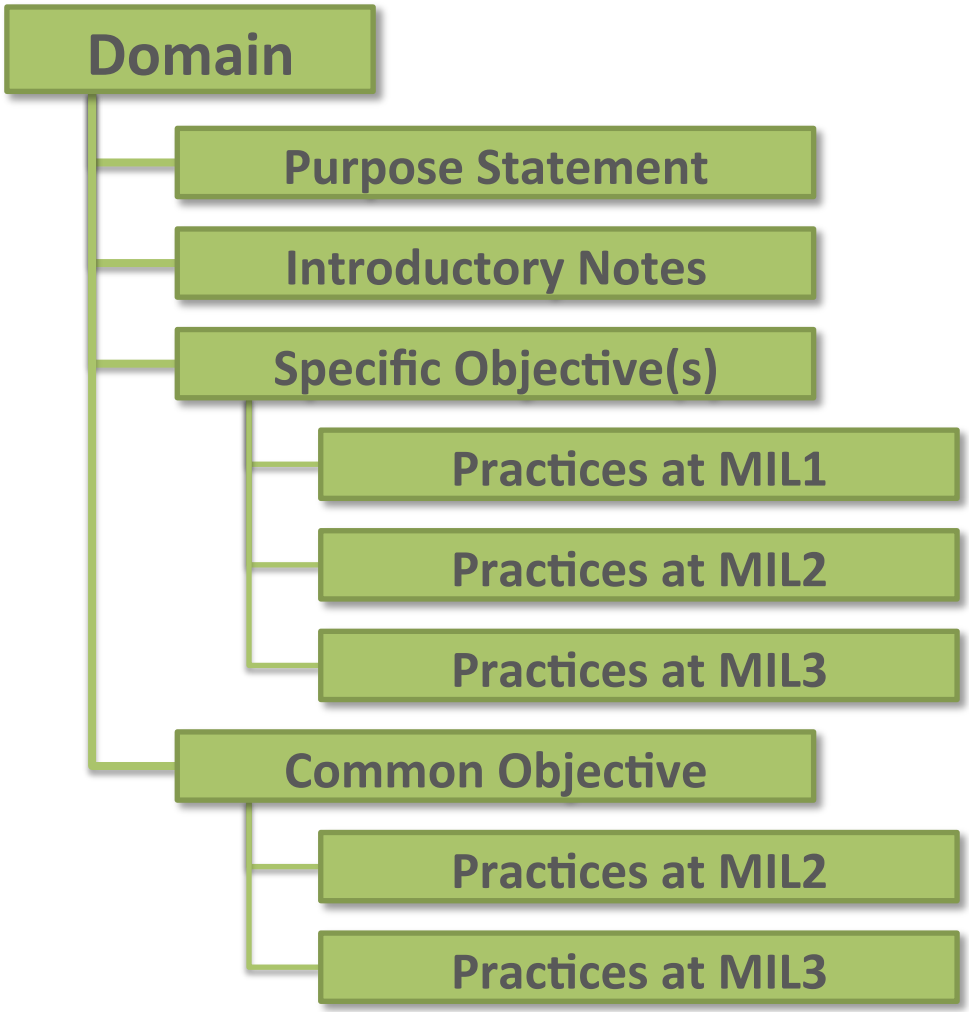
ES-C2M2 is a dual-progression model.

Two things progress across the maturity indicator levels:

1. **Institutionalization** – the extent to which the practices are ingrained in the organization's operations

2. **Approach** – the activity's completeness, thoroughness, or level of development/ sophistication

Domain Structure



Intent and overview

One or more progressions of practices that are unique to the domain

Progression of practices that describe institutionalization activities – same in each domain

Example Specific Objective: ASSET — approach progression

Electricity Subsector Cybersecurity Capability Maturity Model **Version 1.0** **ASSET DOMAIN**

3. Manage Changes to Assets

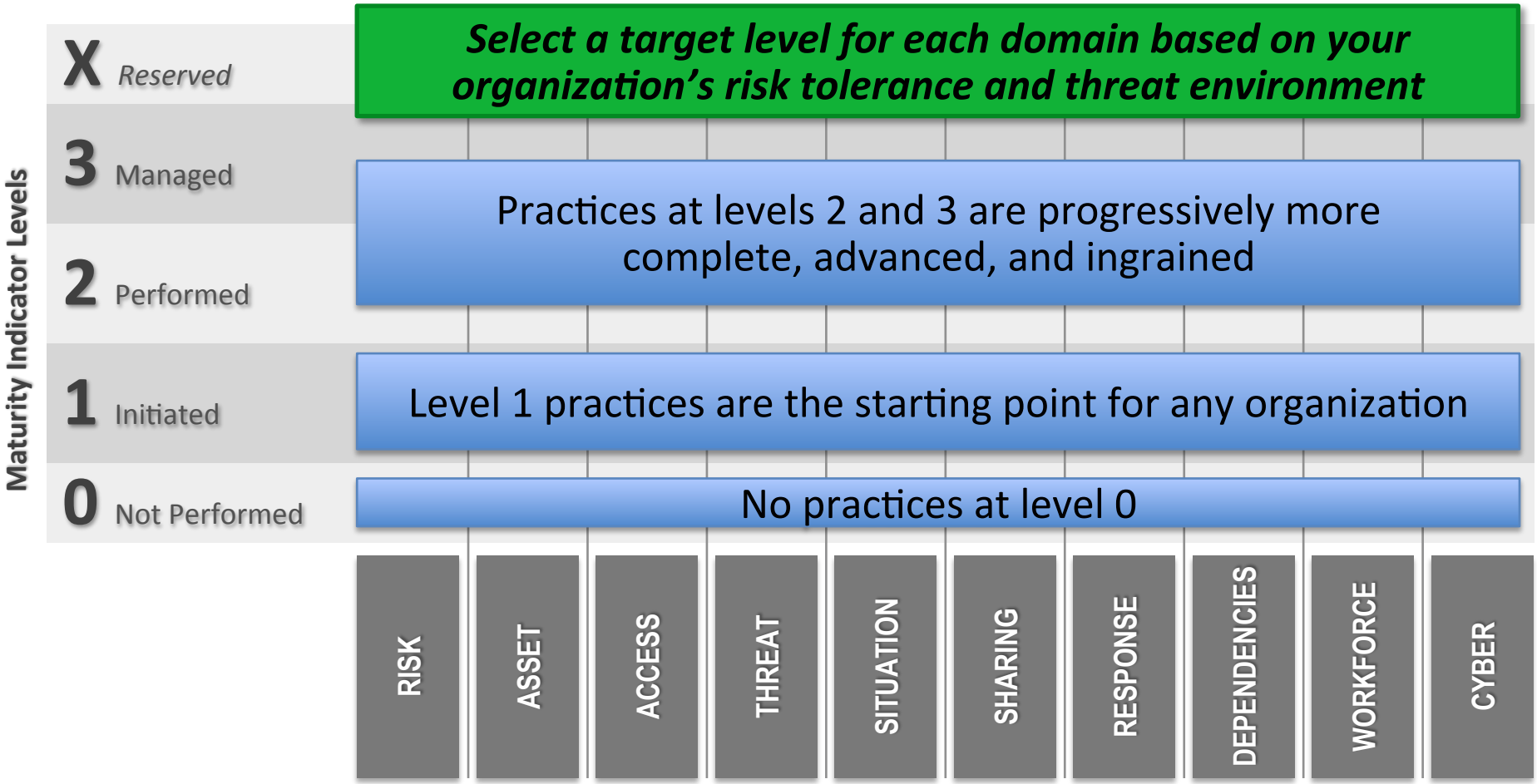
MIL1	a.	Changes to inventoried assets are evaluated before being implemented
	b.	Changes to inventoried assets are logged
MIL2	c.	Changes to assets are tested prior to being deployed, whenever possible
	d.	Change management practices address the full lifecycle of assets (i.e., acquisition, deployment, operation, retirement)
MIL3	e.	Changes to assets are tested for cybersecurity impact prior to being deployed
	f.	Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)

Notice that the practices progress from one MIL to the next within the objective (practices at higher MILs are more complete in their implementation, more sophisticated in their approach, or more thorough).

Example Common Objective: ASSET — institutionalization progression

4. Manage ASSET Activities		
MIL1		*No practice at MIL1*
MIL2	a.	Documented practices are followed for asset inventory, configuration, and change management activities
	b.	Stakeholders for asset inventory, configuration, and change management activities are identified and involved
	c.	Adequate resources (people, funding, and tools) are provided to support asset inventory, configuration, and change management activities
	d.	Standards and/or guidelines have been identified to inform asset inventory, configuration, and change management activities
MIL3	e.	Asset inventory, configuration, and change management activities are guided by documented policies or other organizational directives
	f.	Policies include compliance requirements for specified standards and/or guidelines
	g.	Asset inventory, configuration, and change management activities are periodically reviewed to ensure conformance with policy
	h.	Responsibility and authority for the performance of asset inventory, configuration, and change management activities is assigned to personnel
	i.	Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities

ES-C2M2: Maturity Indicator Levels



Model Domains (1–2 of 10)

Domain	Description
Asset, Change, and Configuration Management (ASSET)	Manage the organization's operational technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives, including activities to • identify, inventory, and prioritize assets • manage asset configurations • manage changes to assets and to the asset inventory
Workforce Management (WORKFORCE)	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives. • Responsibilities • Workforce controls • Knowledge, skills, and abilities • Awareness

Model Domains (3–4 of 10)

Domain	Description
Identity and Access Management (ACCESS)	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives. • Identity management • Access management
Risk Management (RISK)	Establish, operate, and maintain a cybersecurity risk management and mitigation program to identify and manage cybersecurity risk to the organization and its related interconnected infrastructure and stakeholders. • Strategy • Sponsorship • Program

Model Domains (5–6 of 10)

Domain	Description
Supply Chain and External Dependencies Management (DEPENDENCIES)	Establish and maintain controls to manage the cybersecurity risk associated with services and assets that are dependent on external entities, commensurate with the organization's business and security objectives. • Dependency identification • Risk management • Cybersecurity requirements
Threat and Vulnerability Management (THREAT)	Establish and maintain plans, procedures, and technologies to identify, analyze, and manage cybersecurity threats and vulnerabilities, commensurate with the risk to critical infrastructure and organizational objectives. • Threat management • Vulnerability management • Cybersecurity patch management • Assessments

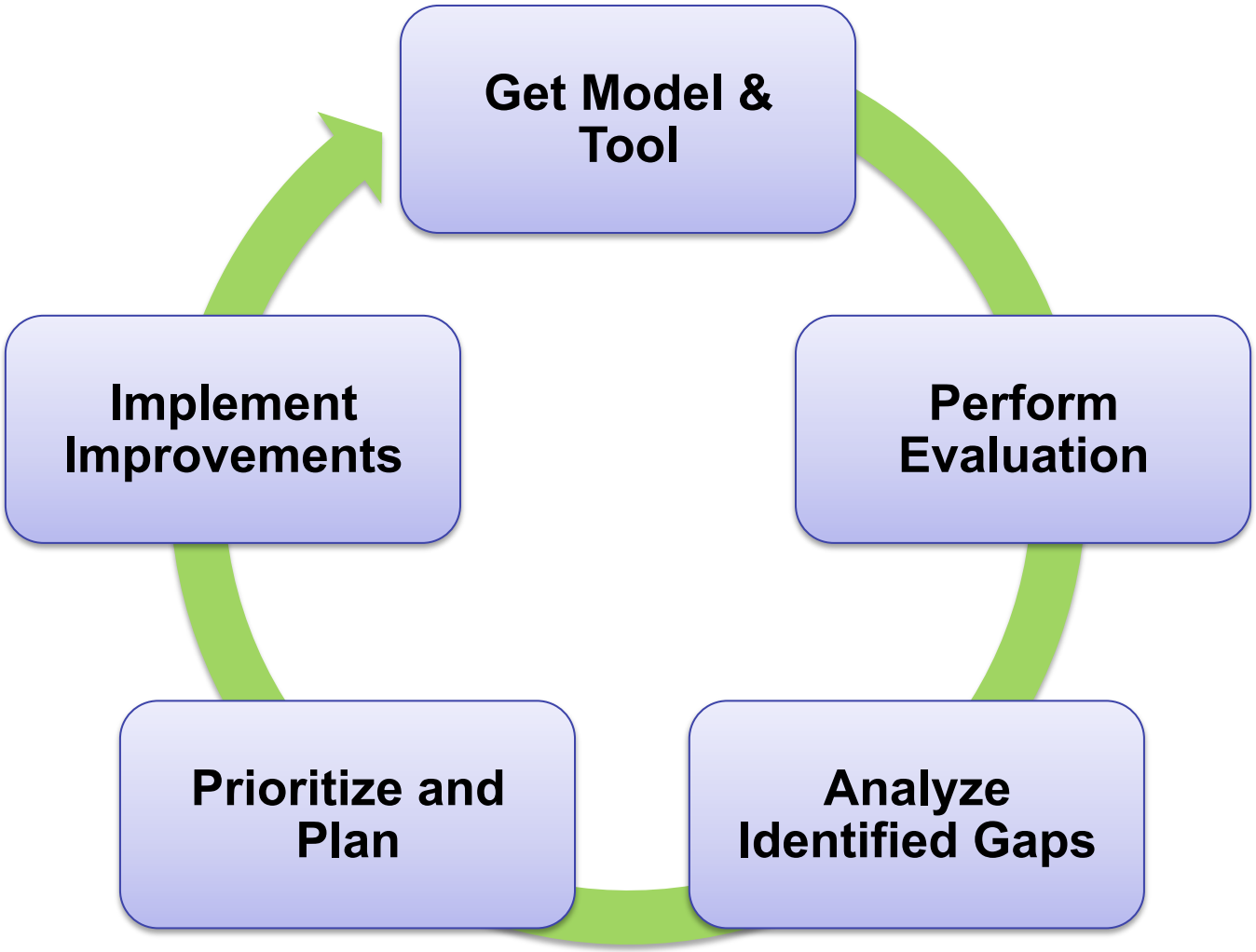
Model Domains (7–8 of 10)

Domain	Description
Event and Incident Response, Continuity of Operations (RESPONSE)	Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity incidents and to sustain critical functions throughout a cyber event, commensurate with the risk to critical infrastructure and organizational objectives. • Detect events • Declare incidents • Respond to incidents • Manage continuity
Situational Awareness (SITUATION)	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture, commensurate with the risk to critical infrastructure and organizational objectives. • Logging • Monitoring • Awareness

Model Domains (9–10 of 10)

Domain	Description
Information Sharing and Communications (SHARING)	Establish and maintain relationships with internal and external entities to share information, including threats and vulnerabilities, in order to reduce risks and increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives. • Communication • Analysis • Coordination
Cybersecurity Program Management (CYBER)	Establish and maintain a cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure. • Strategy • Sponsorship • Program • Architecture

Using ES-C2M2



ES-C2M2 Self-Evaluation

The ES-C2M2 model is supported by a survey-based self-evaluation.

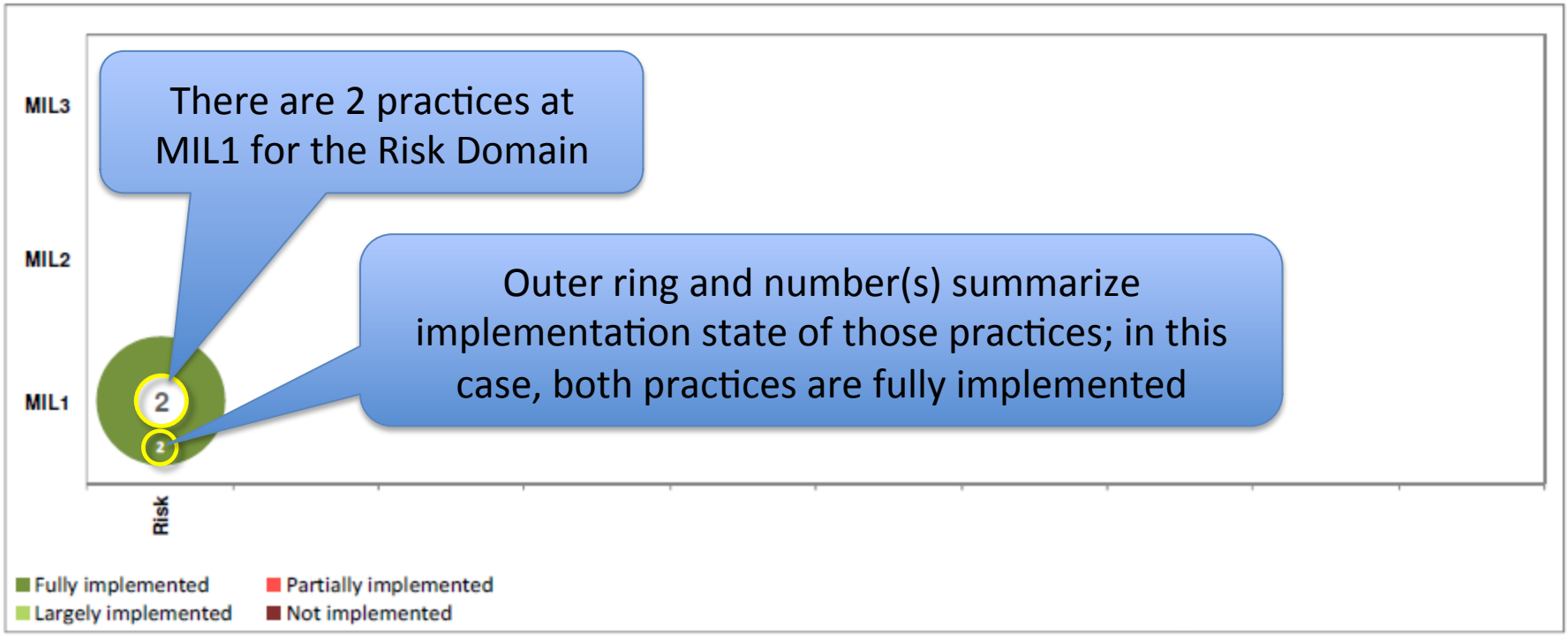
An organization can use the survey (and associated scoring tool) to evaluate its implementation of the model practices.

To complete the survey, an organization selects its level of implementation for the model practice from a 4-point answer scale.

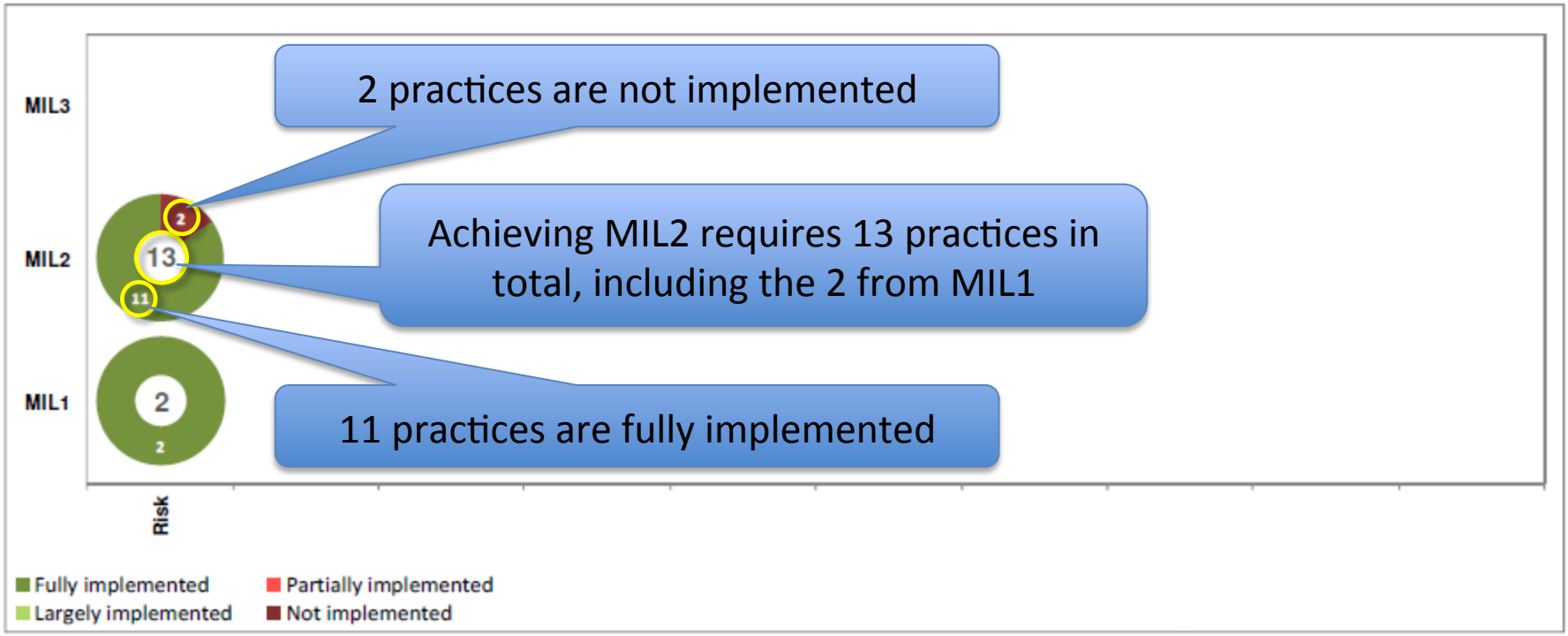
4-Point Answer Scale

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	Complete
Largely implemented	Complete, but with a recognized opportunity for improvement
Partially implemented	Incomplete; there are multiple opportunities for improvement
Not implemented	Absent; the practice is not performed in the organization

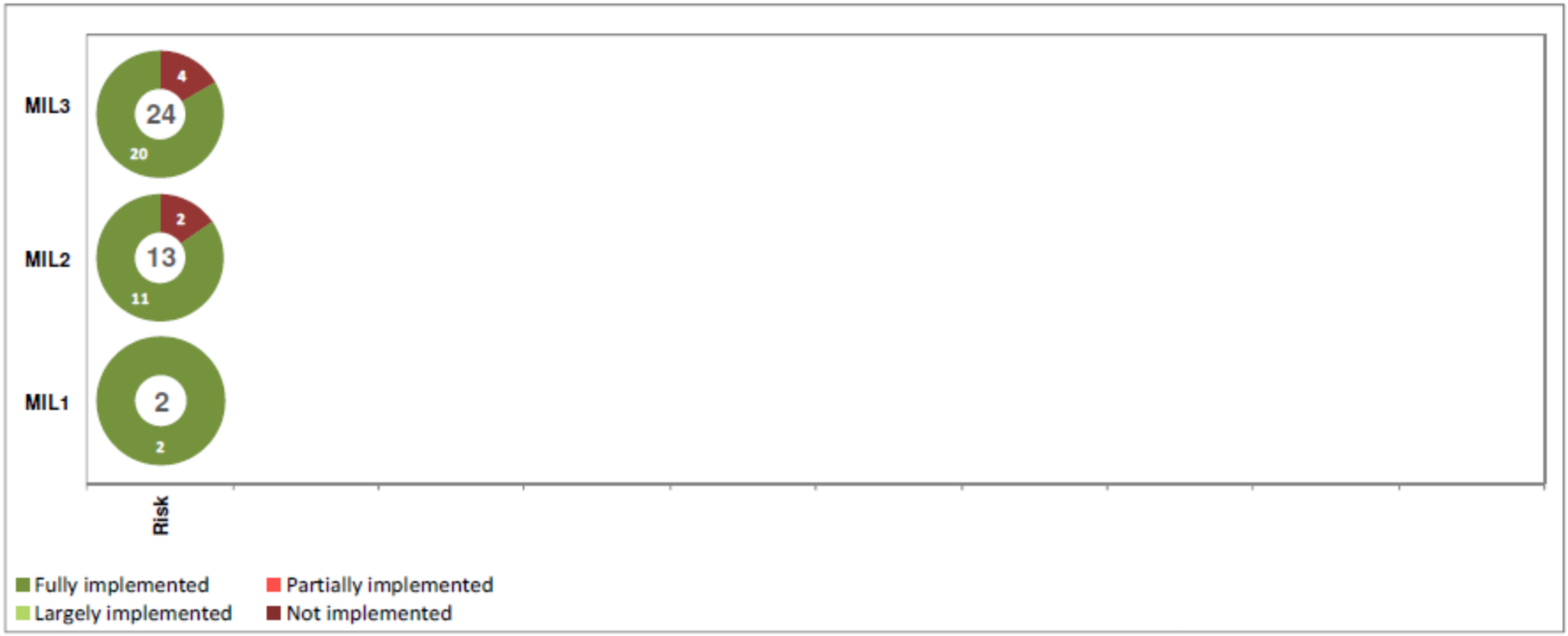
ES-C2M2 Sample Summary Score



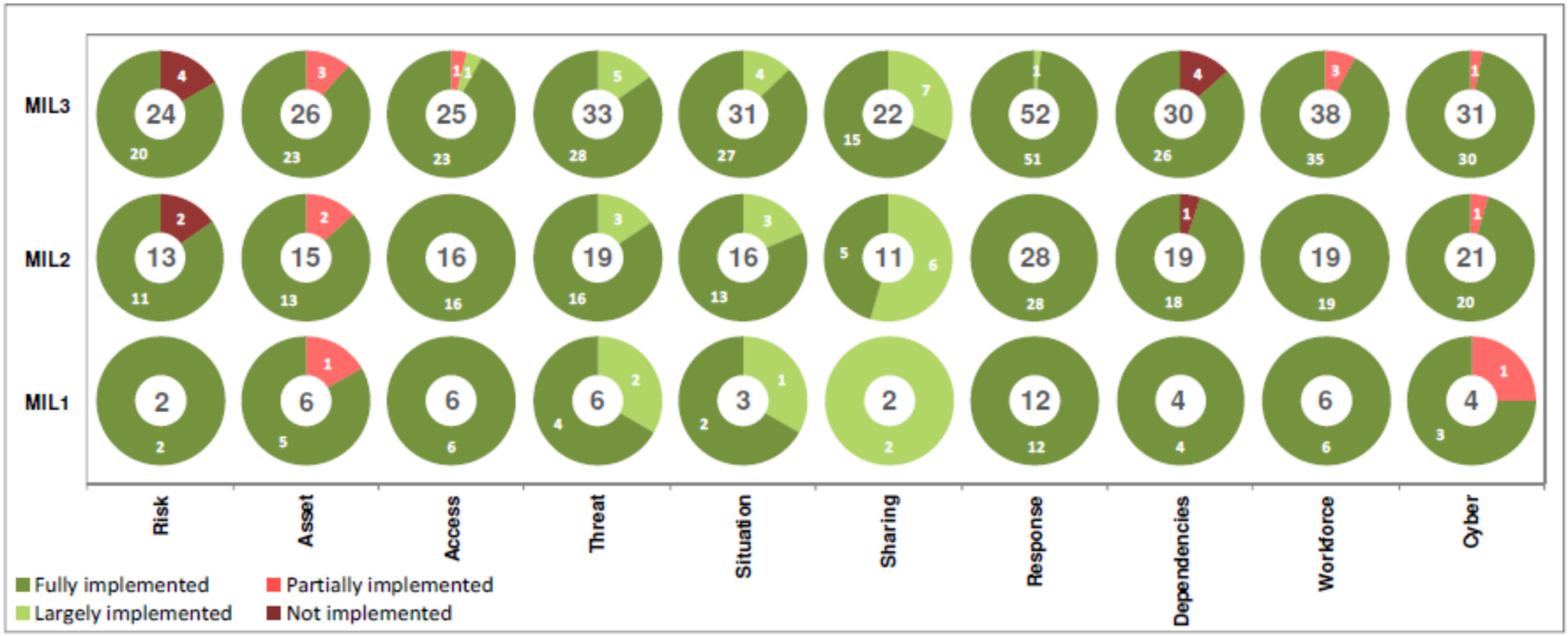
ES-C2M2 Sample Summary Score



ES-C2M2 Sample Summary Score



ES-C2M2 Sample Summary Score



SEI Training

Introduction to the CERT Resilience Management Model

February 18 - 20, 2014 (SEI, Arlington, VA)

June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document