USEA-USAID Digitalization and Cyber Security Webinar Series

C2M2 Overview

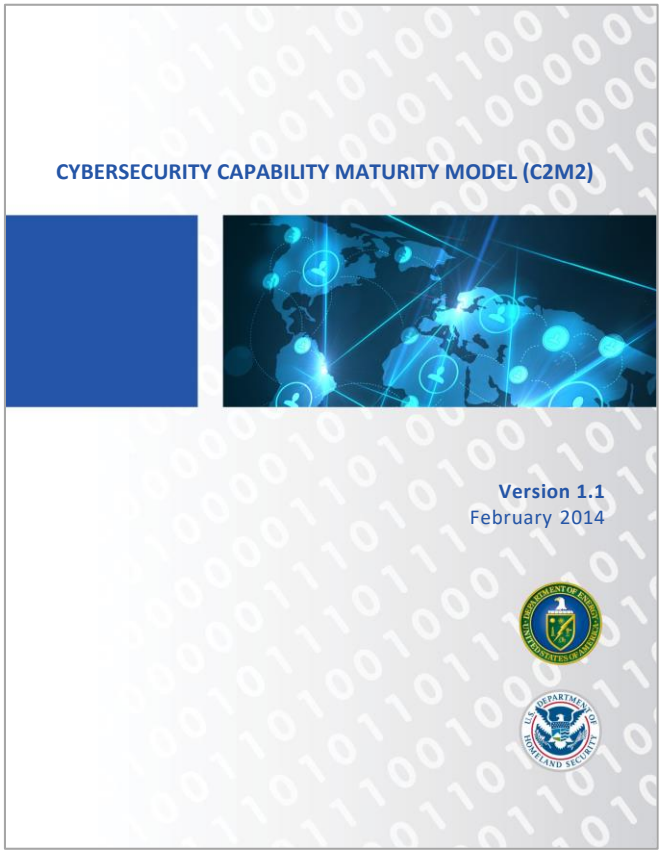
Christopher S. Taylor
September 2020

Cybersecurity Capability Maturity Model (C2M2)

Southern Company

Cybersecurity Capability Maturity Model (C2M2)

- Voluntary practices for building, maintaining, and maturing a cybersecurity program
- C2M2 is a model and assessment for both IT and OT
- Objectives
  - Strengthen cybersecurity capabilities
  - Consistent assessment and benchmarking
  - Share knowledge and best practices
  - Enable prioritized actions and investments
- Developed by utilities and for utilities in 2012 under the US Department of Energy, updated in 2014 (v1.1)
- New version (v2.0) to be released in 2021



The Approach: Maturity Model

Maturity Model Definition:

- An organized way to identify competencies and areas of improvement.
- The C2M2 is used to evaluate a business unit's practices, processes, and procedures
- Focuses more on organizational practices and maturity instead of technical controls

C2M2 Architecture

4 Maturity Indicator Levels

MIL3 (advanced)

MIL2 (intermediate)

MIL1 (beginning)

MIL0

Progression of 312 practices from MIL1 to MIL3

MIL3 practices

MIL2 practices

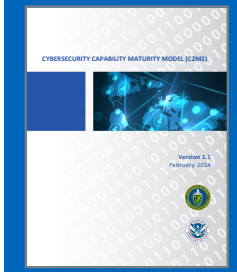
MIL1 practices

No practices

261 MIL2 & MIL3 practices are progressively more complete, advanced, and ingrained; target levels should be set for each domain based on risk tolerance and threat environment

51 MIL1 practices are *basic activities that any organization should perform*; these are the starting blocks

C2M2 Model Architecture



RM Risk Management

ACM Asset, Change, and Configuration Management

IAM Identity and Access Management

TVM Threat and Vulnerability Management

SA Situational Awareness

ISC Information Sharing and Communications

IR Event & Incident Response, Continuity of Operations

EDM Supply Chain & External Dependencies Management

WM Workforce Management

CPM Cybersecurity Program Management

10 Model Domains: logical groupings of cyber security practices — activities that protect operations from cyber-related disruptions

Assessment 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

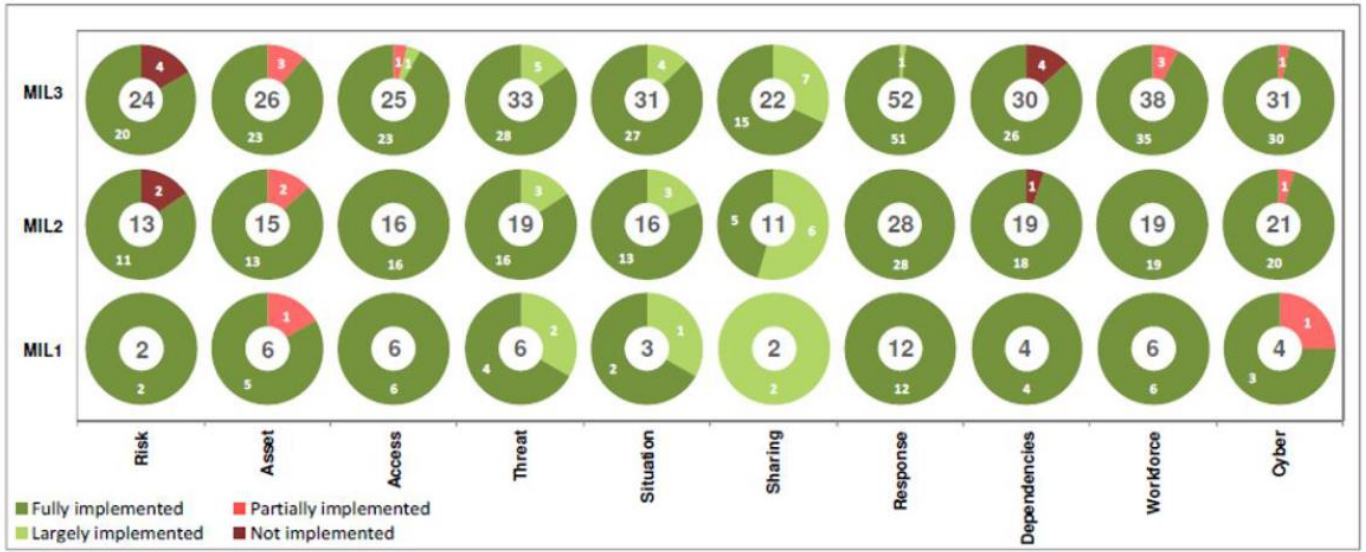
C2M2 Example Practices from Identity and Access Mgmt

2. Control Access

MIL1	a.	Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)
	b.	Access is granted to identities based on requirements
	c.	Access is revoked when no longer required
MIL2	d.	Access requirements incorporate least privilege and separation of duties principles
	e.	Access requests are reviewed and approved by the asset owner
	f.	Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
MIL3	g.	Access privileges are reviewed and updated to ensure validity, at an organizationally defined frequency
	h.	Access to assets is granted by the asset owner based on risk to the function
	i.	Anomalous access attempts are monitored as indicators of cybersecurity events

Note that C2M2 practices have an addressing scheme to ease implementation tracking. The first practice shown is IAM-2a.

C2M2 Sample Summary Score

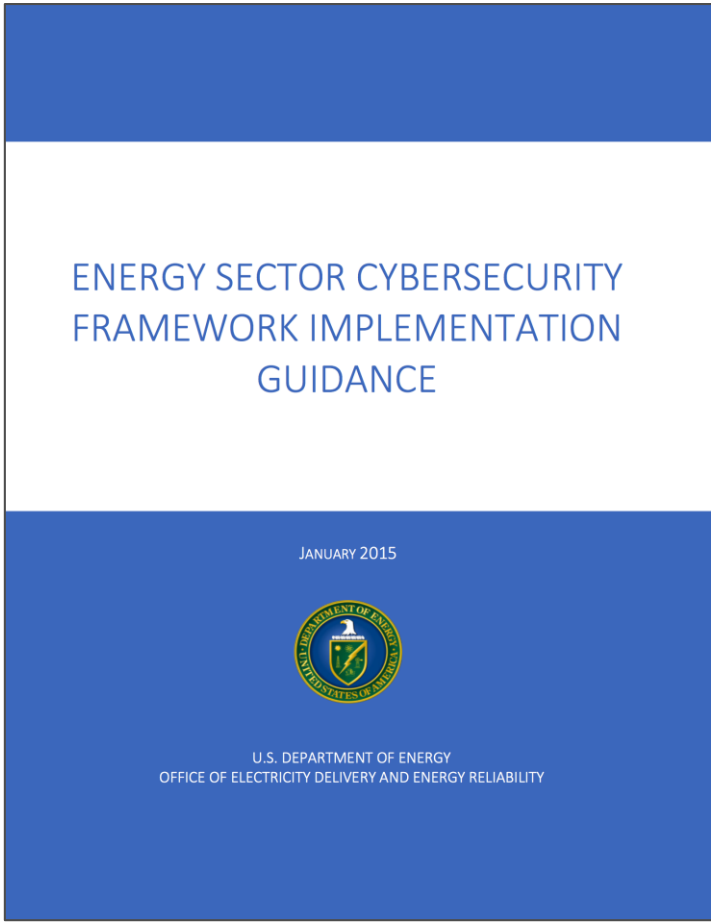


MIL Rating	1	0	2	3	3	3	3	1	2	0

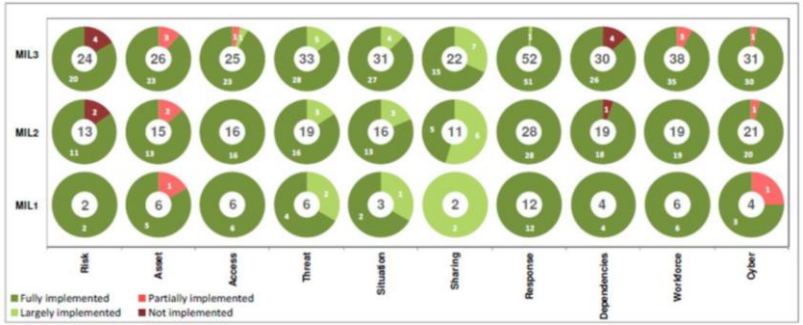
Using C2M2 to Implement the NIST CSF

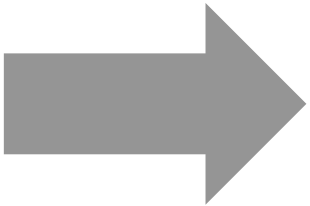
Sector-led Guidance

- EO 13636 stated
  - *"Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments."*
- US Department of Energy worked with Sector-Coordinating Councils (ES and ONG) to draft implementation
- Provides two use-cases:
  - Generic
  - C2M2-based



Implementing NIST CSF with C2M2





C2M2 Provides:

- Detailed technical/maturity considerations
- Assessment methodology and guidance
- Detailed scoring for measuring progress

C2M2 Does Not Provide

- Easy communication to non-cyber personnel or executives

NIST CSF Provides:

- Broad enterprise considerations (5 Functions)
- Minimal or no technical jargon
- Common lexicon to enable action across diverse stakeholders

NIST CSF Does Not Provide

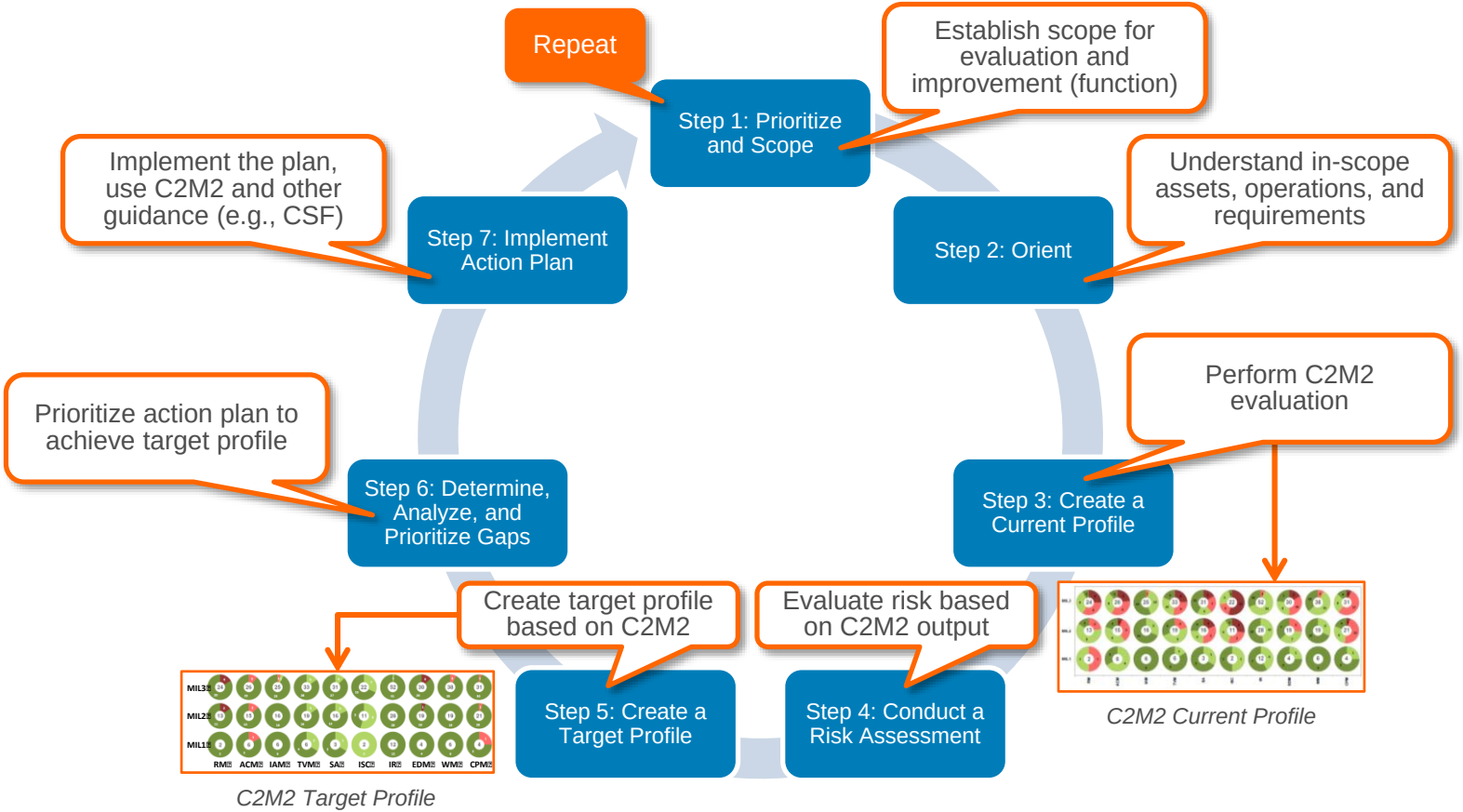
- Assessment methodology
- Scoring guidance

C2M2-CSF Mapping

Framework Core			C2M2 Practices		
Function	**Category**	**Subcategory**	MIL 1	MIL 2	MIL3
PROTECT (PR)	Access Control (AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	IAM-1a IAM-1b IAM-1c	IAM-1d IAM-1e IAM-1f	RM-1c IAM-1g
		PR.AC-2: Physical access to assets is managed and protected	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g
		PR.AC-3: Remote access is managed	IAM-2a IAM-2b IAM-2c	IAM-2d IAM-2e IAM-2f	IAM-2g
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties		IAM-2d	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	CPM-3a	CPM-3b CPM-3c	CPM-3d

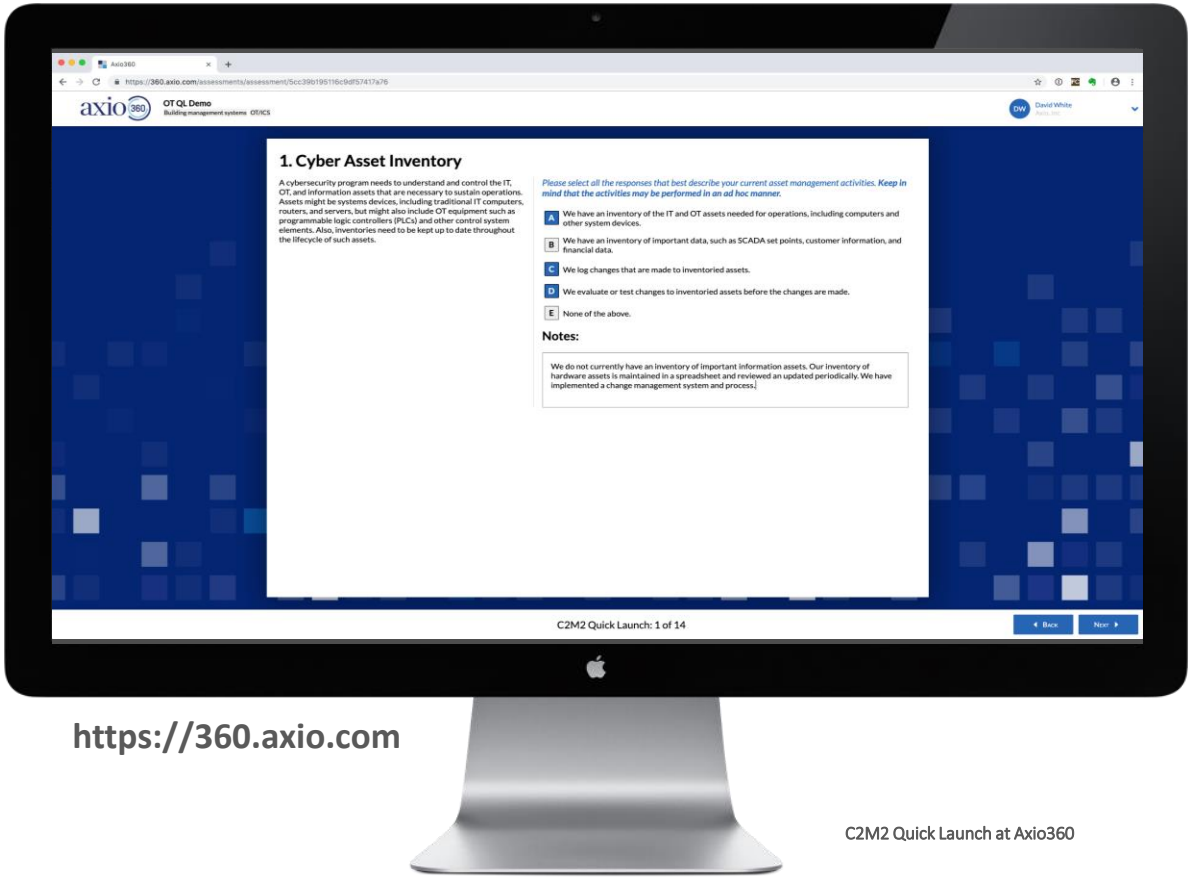
- Subcategory granularity varies across the CSF
- One subcategory may map to multiple C2M2 practices
- Per the guidance, performing the C2M2 maps to the entire CSF
  - Cybersecurity architecture is a notable sticky area
- Overlap of C2M2 practices across both the Framework Core and Implementation Tiers

Sector-led Guidance



Where to start? MIL 1 Controls

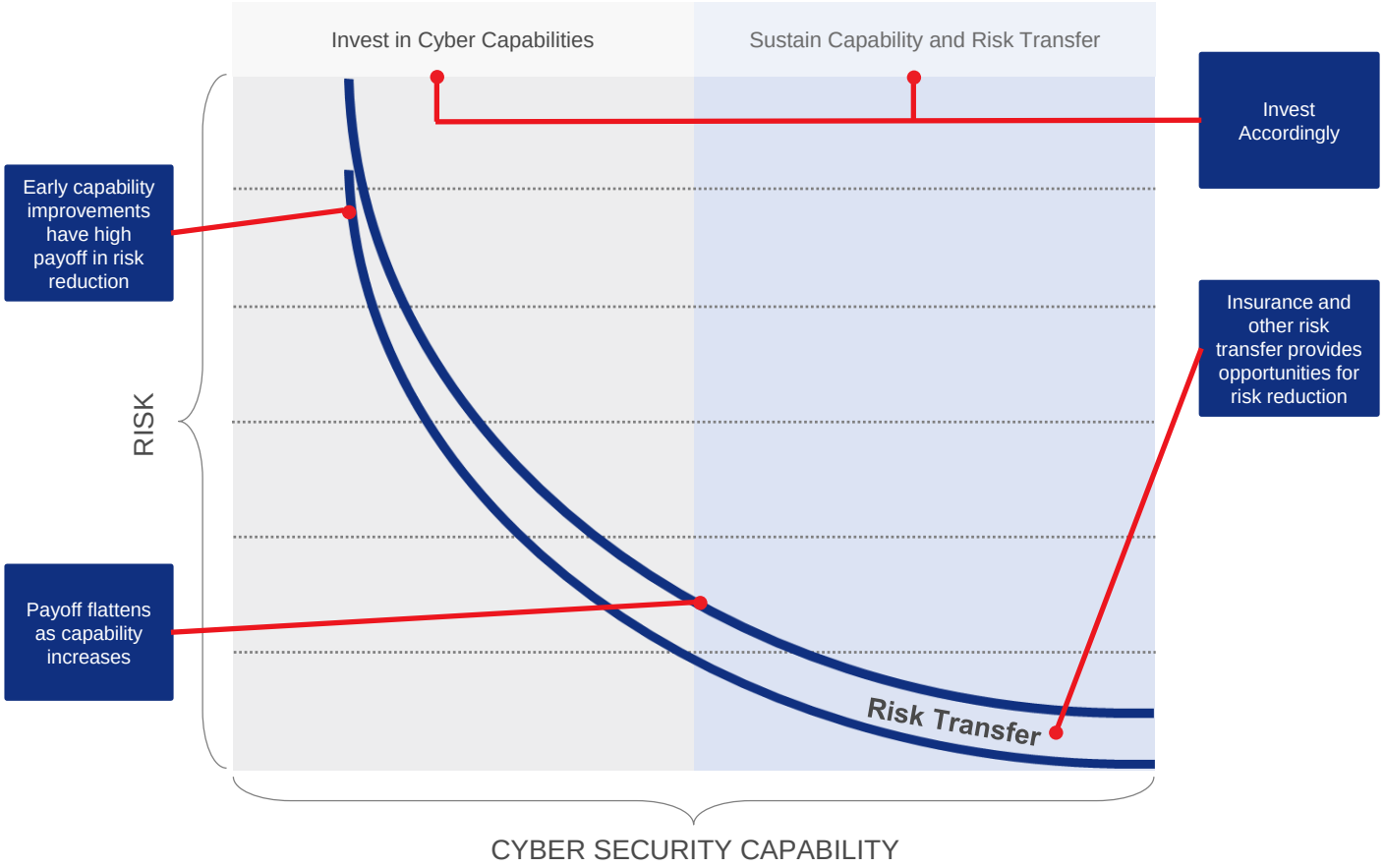
- Begin with C2M2 MIL1 practices (the basics)
- There are 51 C2M2 MIL1 practices
- Ensure you record notes to capture ideas and rationale
- Axio offers a free Rapid Start MIL 1 assessment



https://360.axio.com

C2M2 Quick Launch at Axio360

Target Profile Considerations

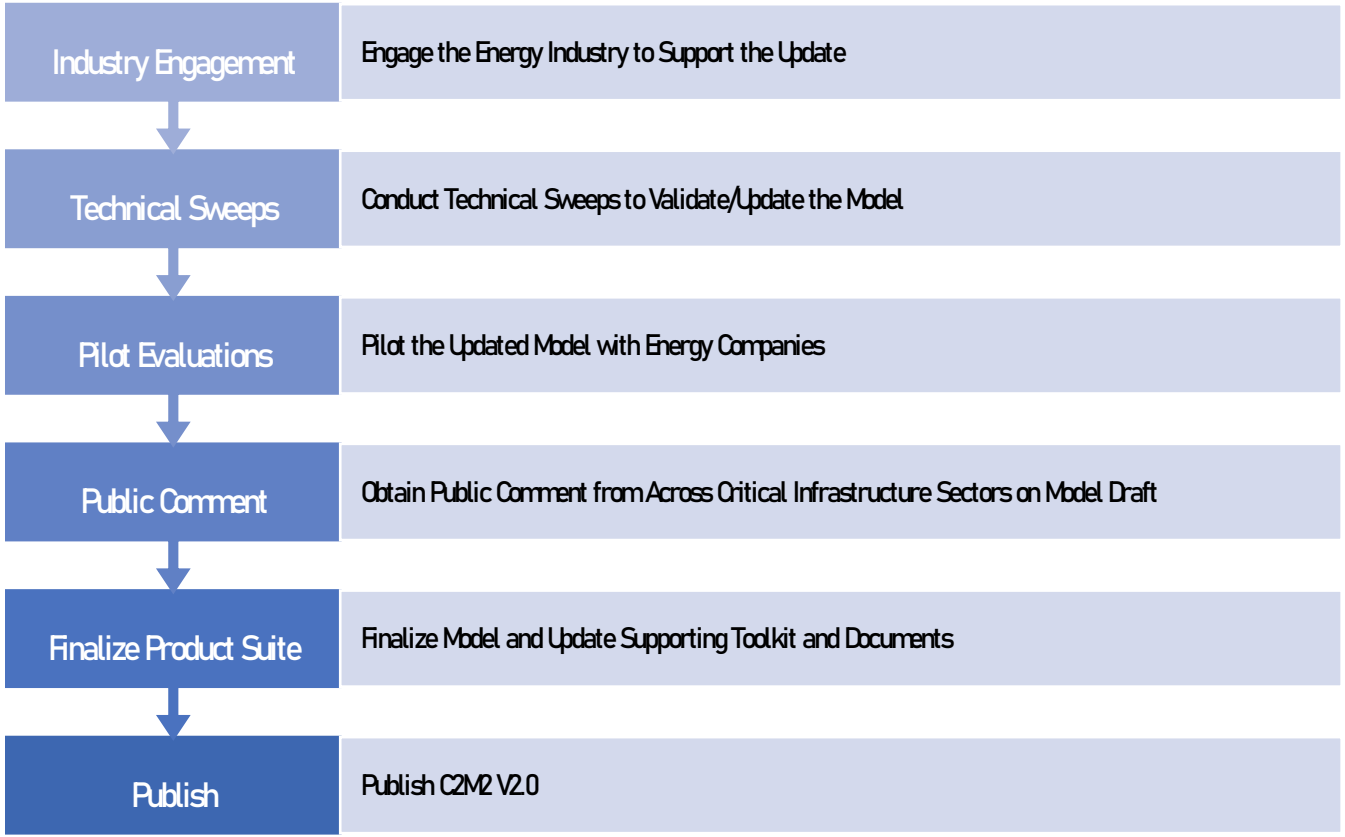


C2M2 Resources & Version 2

Southern Company

C2M2v2

C2M2 - v2.0 UPDATE



C2M2 Resources

- Department of Energy
  - https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0
- National Institute of Standards and Technology
  - https://www.nist.gov/cyberframework
- Axio
  - https://axio.com/
  - https://360.axio.com/
- Facility Cybersecurity F-C2M2 Lite Assessment
  - https://facilitycyber.labworks.org/

Southern Company