

Evaluating and Improving **Cyber Resilience Capabilities** of the Electricity and Oil & Natural Gas Critical Infrastructure Components

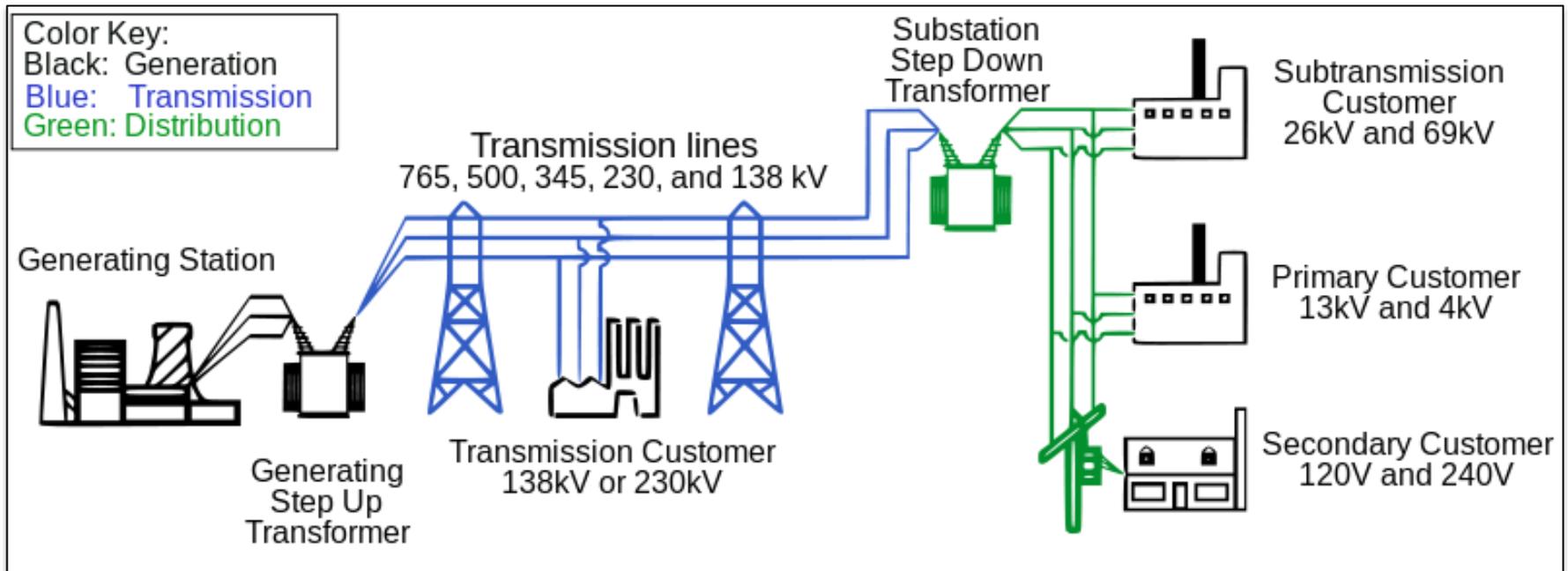
Dr. Nader Mehravari
James Stevens

*Cyber Risk & Resilience Management Team
Software Engineering Institute
Carnegie Mellon University*

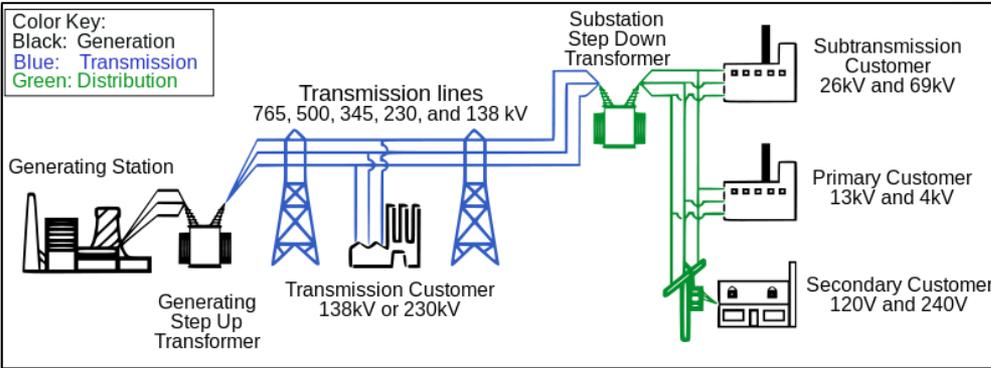


Software Engineering Institute
Carnegie Mellon University.

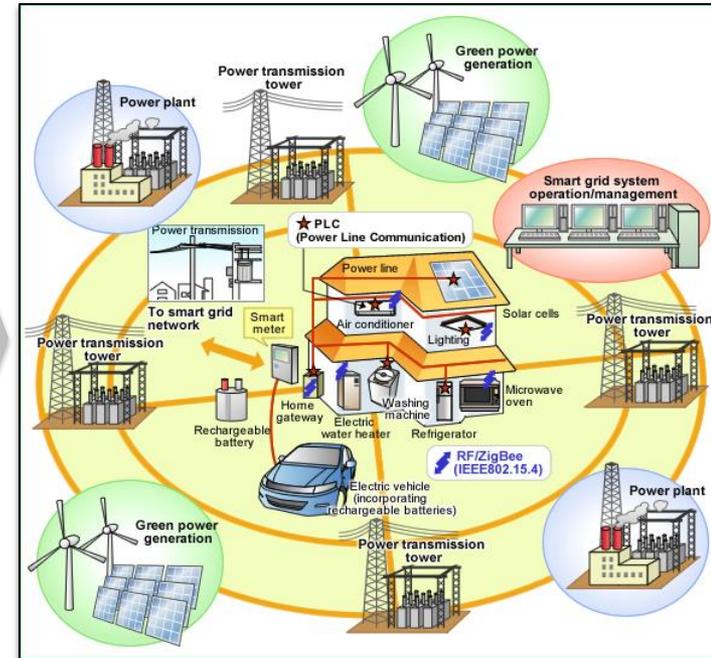
YESTERDAY: Legacy Electrical Grid



TODAY: Smart Grid



Legacy Electrical Grid



Modern Smart Grid

FUNCTIONALITY & EFFICIENCY

OPERATIONAL RISK

Challenge from the White House



Challenge:

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

Strong Sponsorship & Collaboration

- White House initiative
- Led by Department of Energy
- In partnership with DHS
- In collaboration with energy sector asset owners and operators
- SEI model architect



Software Engineering Institute
Carnegie Mellon.

The Approach: Maturity Model

- An organized way to convey a path of experience, wisdom, perfection, or acculturation.



A Maturity Progression for Authentication

Three-factor authentication

Two-factor authentication

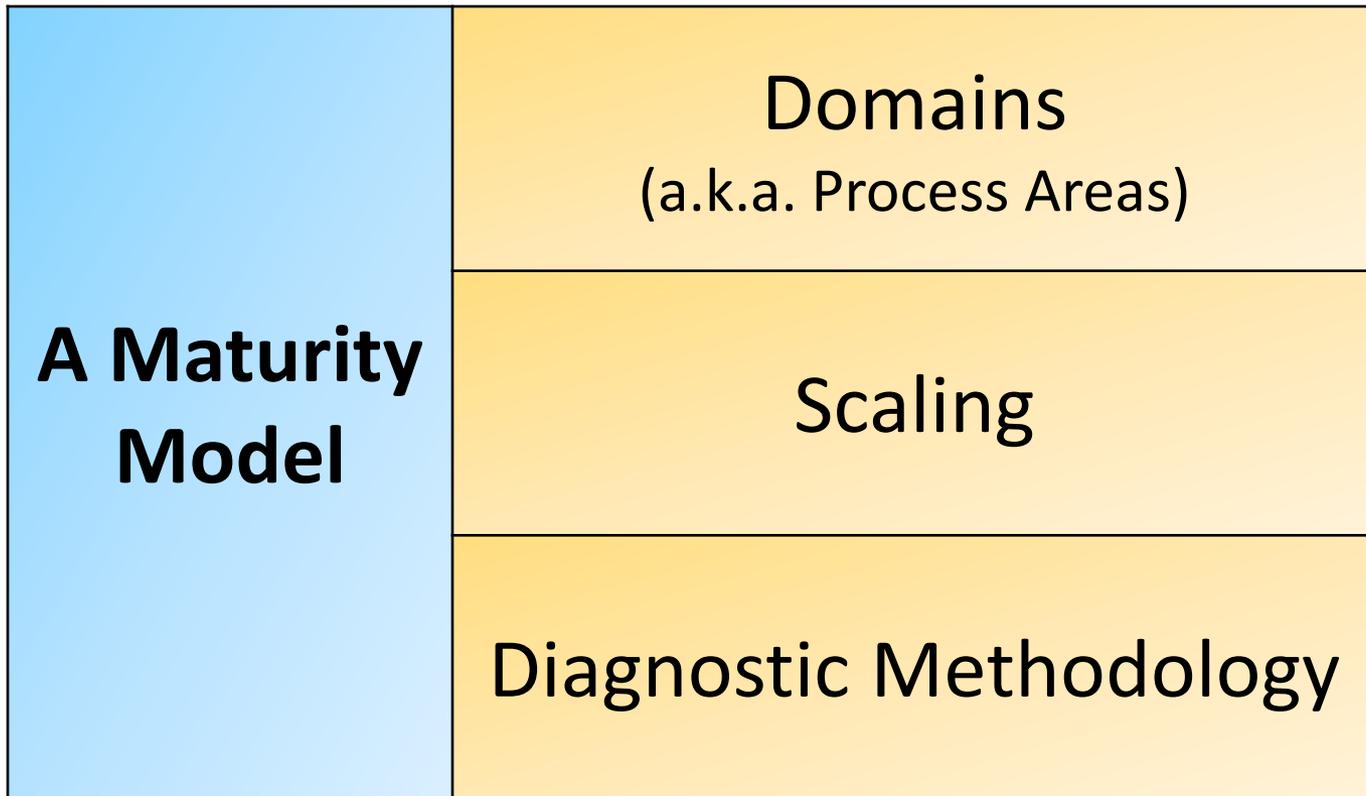
Addition of changing every 60 days

Use of strong passwords

6 Use of simple passwords`



Cybersecurity Capability Maturity Model (C2M2) Architecture

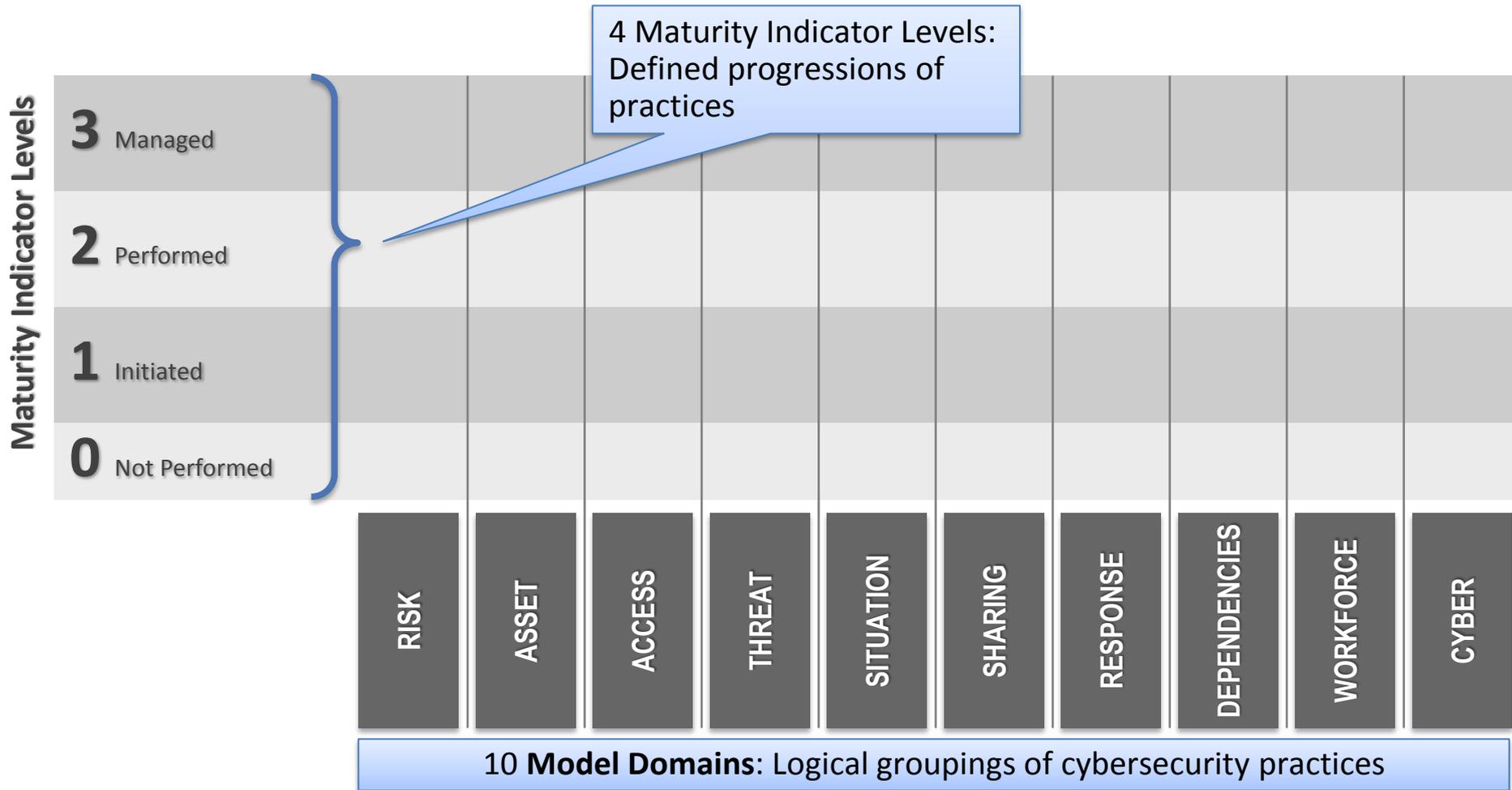


Domains that C2M2 Examines

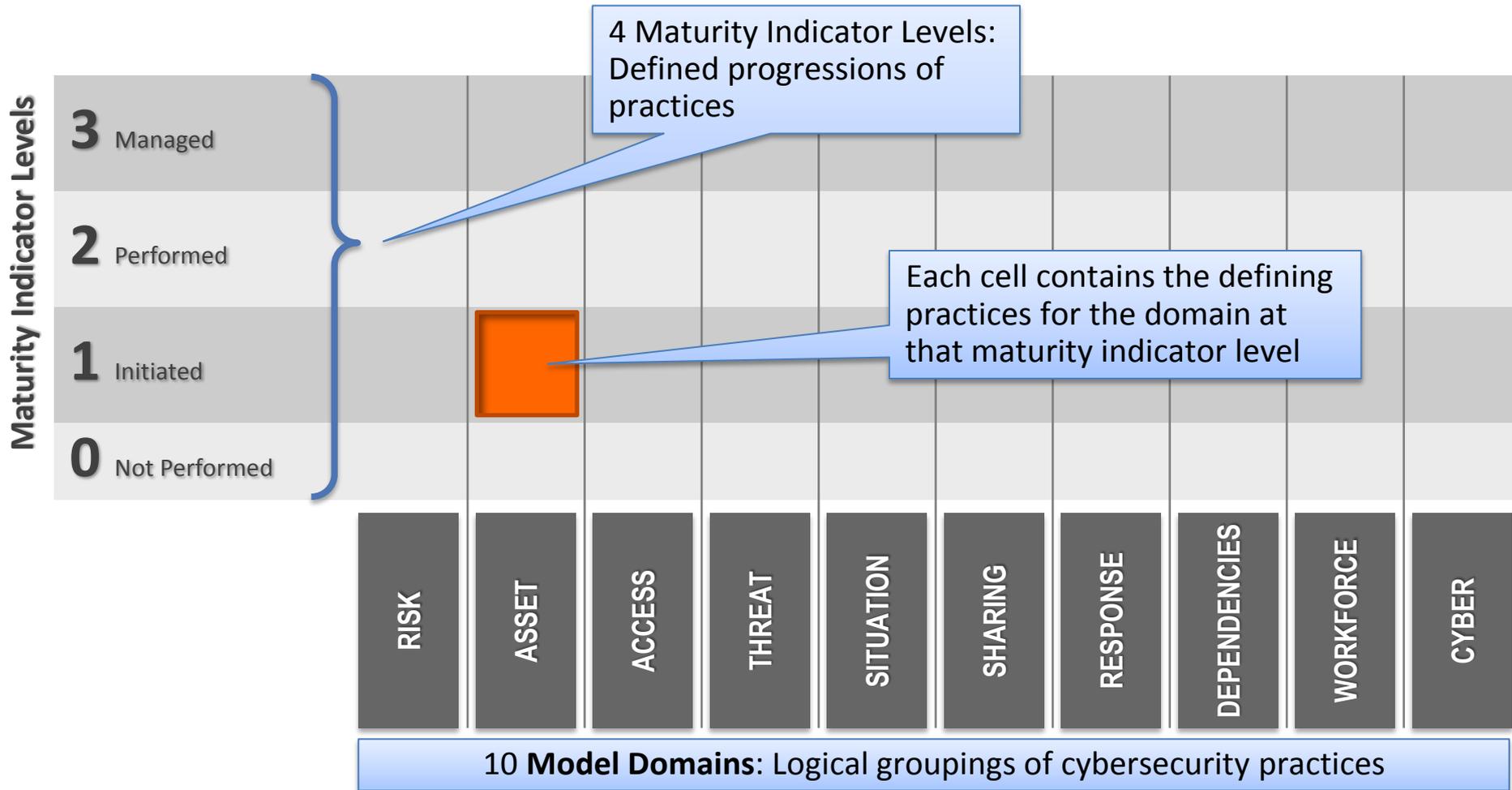


Domains are logical groupings of cybersecurity practices

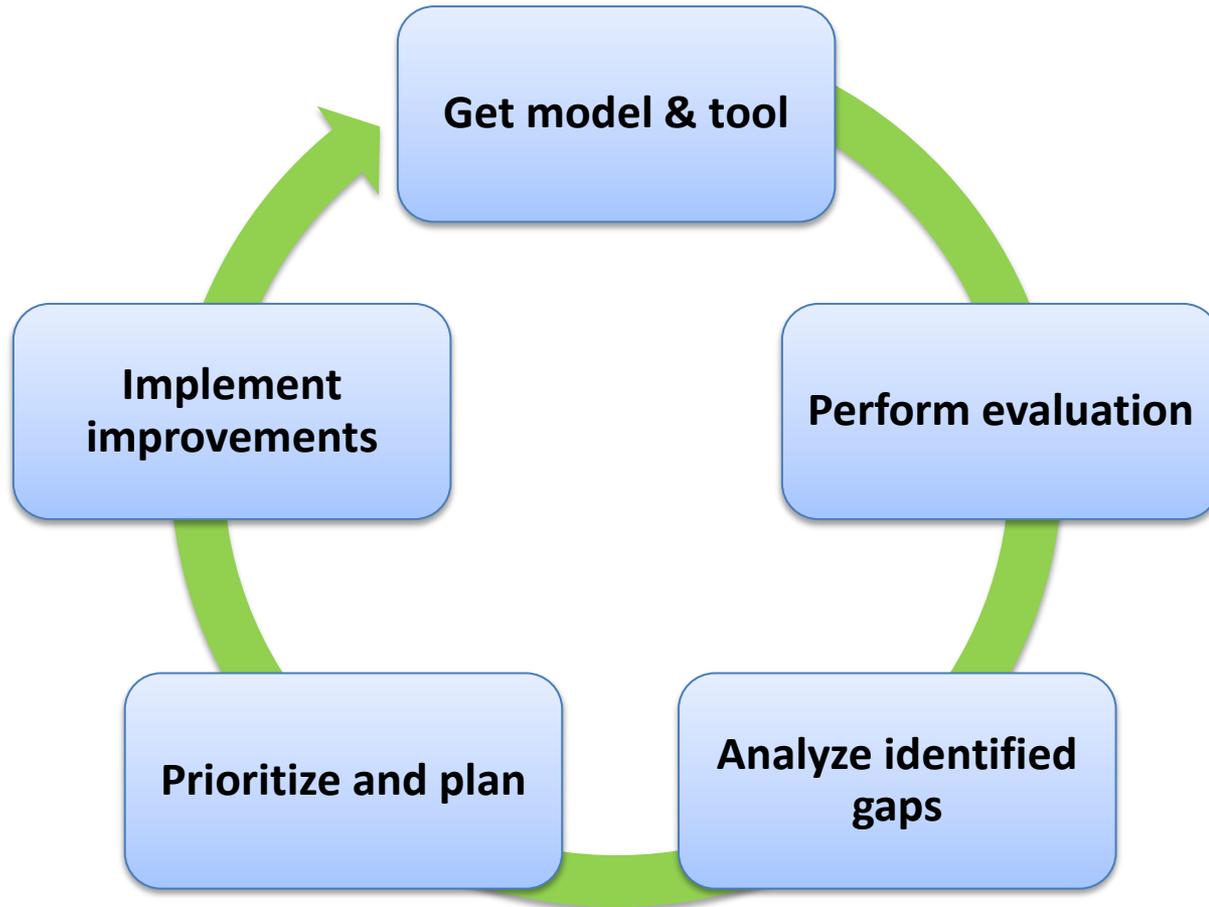
C2M2 Structure



C2M2 Structure



Using C2M2

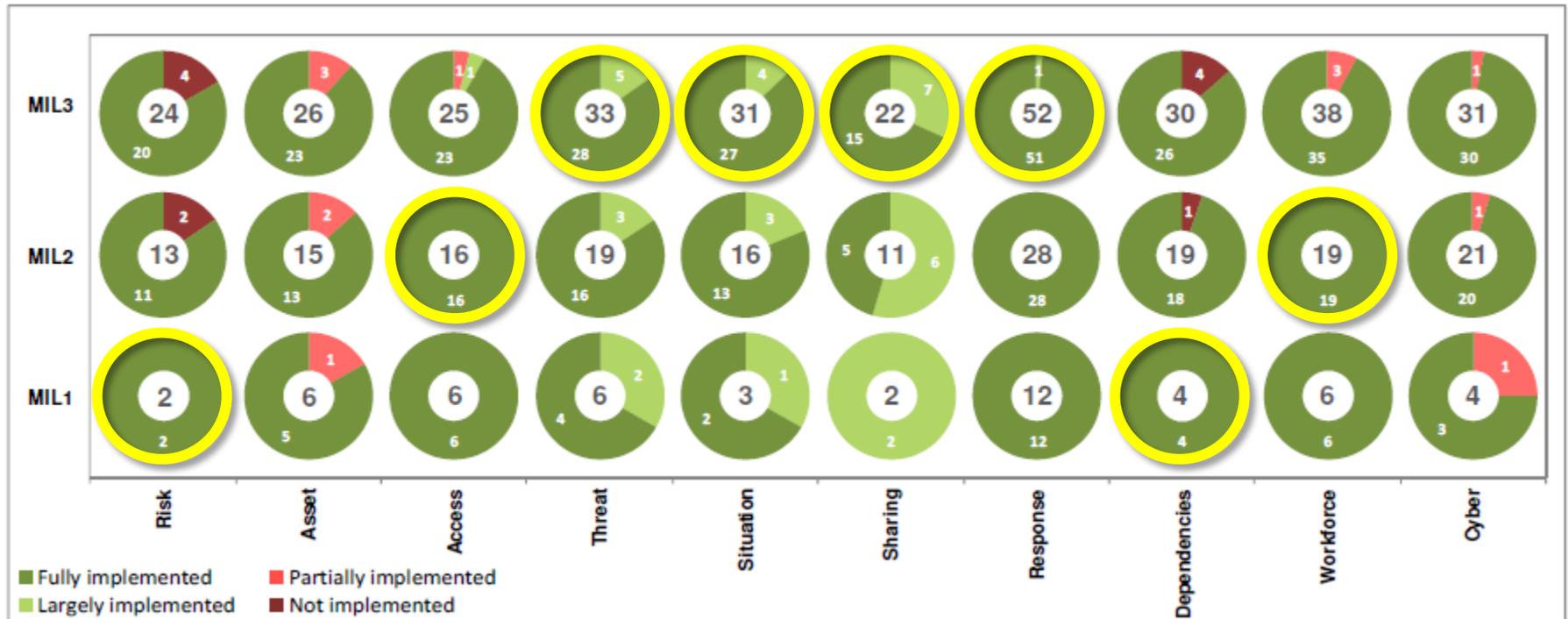


C2M2 Self-Evaluation

- The C2M2 models are supported by a survey-based self-evaluation

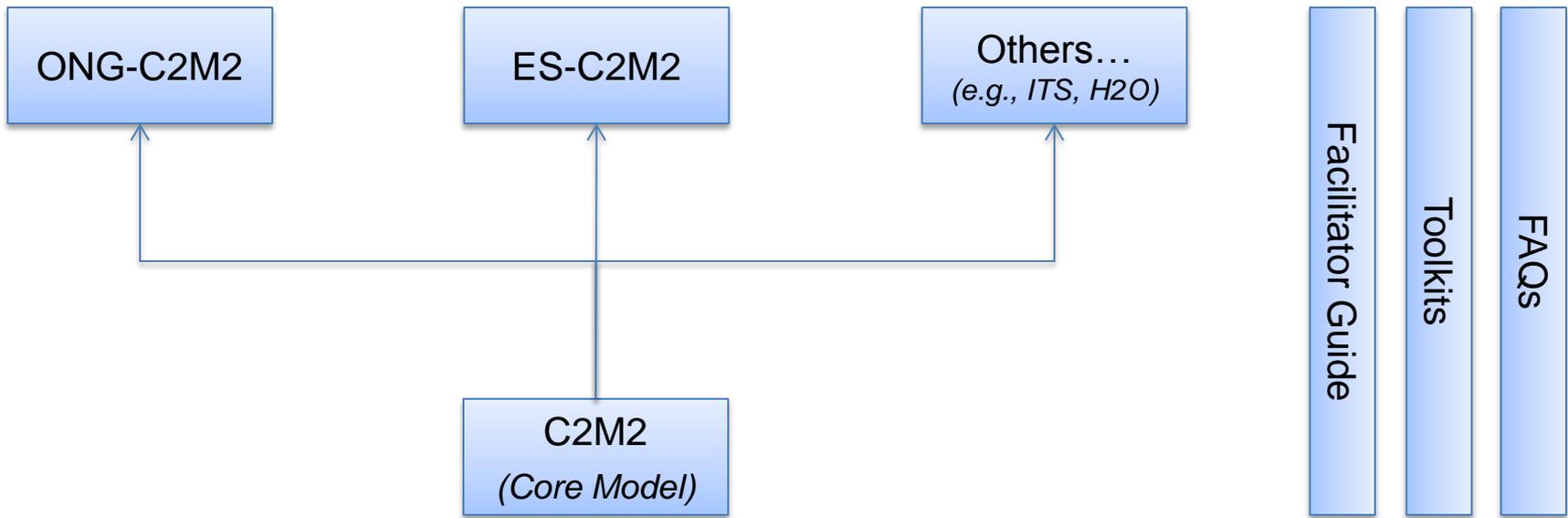


C2M2 Sample Summary Score



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

A Family of Cybersecurity Maturity Models



Enabling Consistent Applicability to Complex Organizations

Home » Services » Cybersecurity » Cybersecurity Capability Maturity Model (C2M2) Program

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) PROGRAM

- [Electricity Advisory Committee](#)
- [Technology Development](#)
- [Electricity Policy Coordination and Implementation](#)
- [DOE Grid Tech Team](#)
- [Energy Assurance](#)
- [Cybersecurity](#)
 - [NIST Framework](#)
 - [C2M2 Program](#)
 - [Cybersecurity Capability Maturity Model](#)
 - [ES-C2M2](#)
 - [ONG-C2M2](#)
 - [Cybersecurity Risk Management Process](#)
 - [Energy Delivery Systems Cybersecurity](#)



The Cybersecurity Capability Maturity Model (C2M2) program is a public-private partnership effort that was established as a result of the Administration’s efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the grid. The C2M2 helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity

- RELATED LINKS
- [Executive Order \(EO\) 13636 “Improving Critical Infrastructure Cybersecurity”](#)
 - [NIST Framework](#)
 - [Use of the NIST Cybersecurity Framework & DOE C2M2](#)
 - [Cybersecurity Capability Maturity Model \(C2M2\) Program](#)
 - [C2M2 Model](#)
 - [Electricity Subsector C2M2 Model](#)
 - [Podcast - Electricity Subsector C2M2 Model](#)
 - [Oil and Natural Gas Subsector C2M2 Model](#)