Electricity Subsector
Cybersecurity Capability Maturity Model (ES-C2M2)

Overview

ES-C2M2 Background

- **Administration initiative:** Led by DOE in collaboration with other public and private sector partners
- **Challenge:** Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid
- **Approach:** Develop a maturity model and self-evaluation survey to develop and measure cybersecurity capabilities
- **Results:** A scalable, sector-specific model created in partnership with industry

Future Objectives

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

ES-C2M2 Model Includes 10 Domains

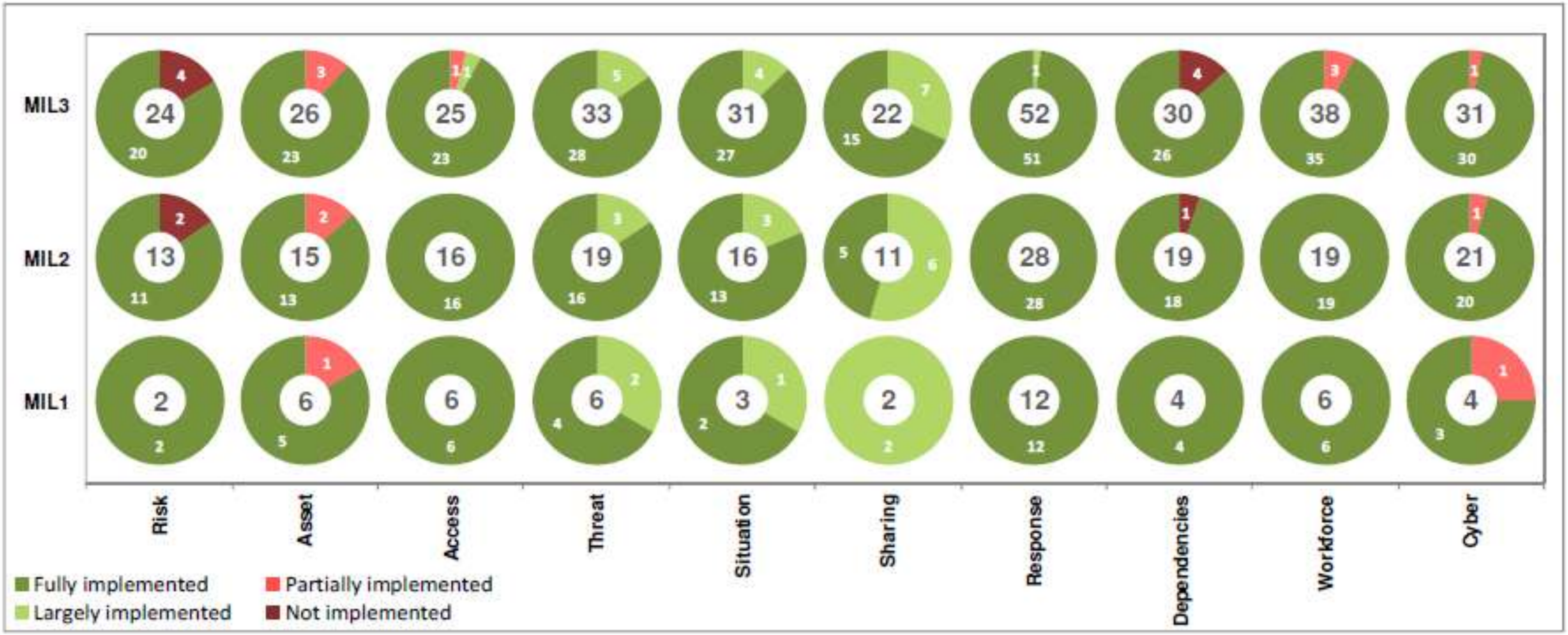
RISK	Risk Management
ASSET	Asset, Change, and Configuration Management
ACCESS	Identity and Access Management
THREAT	Threat and Vulnerability Management
SITUATION	Situational Awareness
SHARING	Information Sharing and Communications
RESPONSE	Event and Incident Response, Continuity of Operations
DEPENDENCIES	Supply Chain and External Dependencies Management
WORKFORCE	Workforce Management
CYBER	Cybersecurity Program Management

- Domains are logical groupings of cybersecurity practices
- Each domain has a short name for easy reference

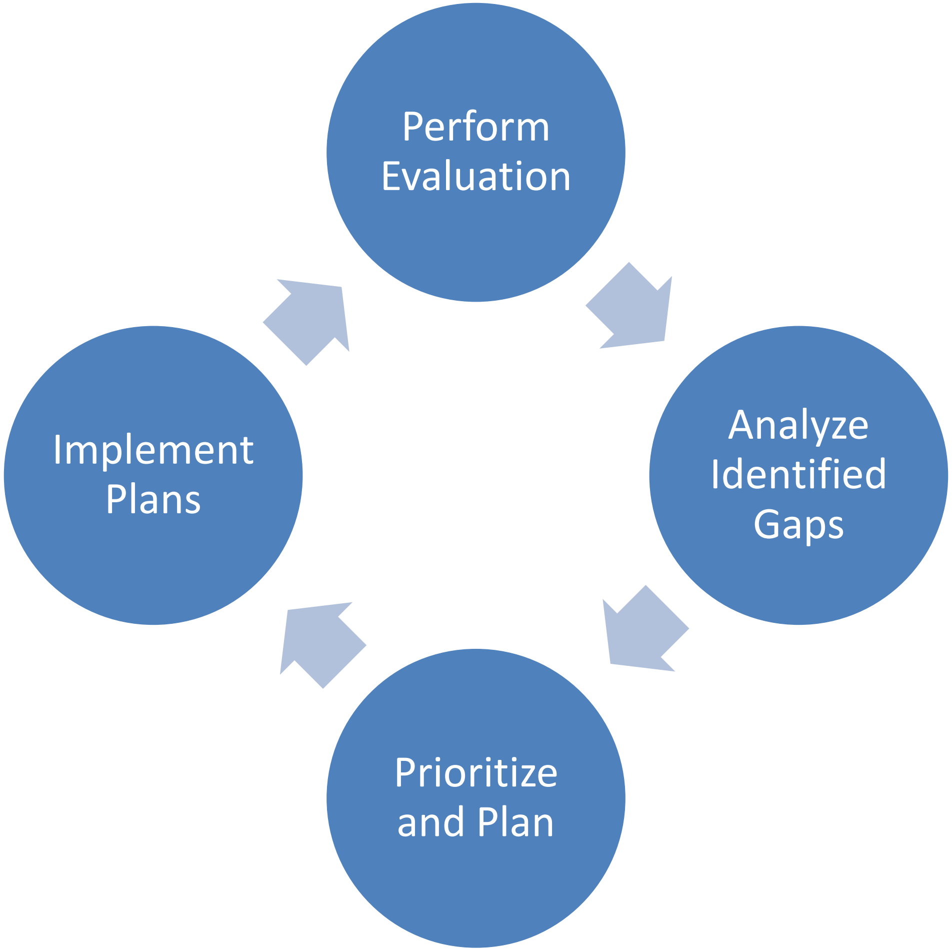
Maturity Indicator Level Descriptions

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

Sample Summary Score



Capability Development



Capability Development Illustration

- Example – *Night Dragon, a coordinated attack by Advanced Persistent Threat using multiple attack vectors with the goal of data theft*

Attack Vector	ES-C2M2 Practice	ES-C2M2 Domain
Social Engineering	Cybersecurity awareness content is based on the organization’s threat profile	WORKFORCE
Default Hardware Configuration	The design of configuration baselines includes cybersecurity objectives	ASSET
Known Vulnerability Exploits	Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organization-defined frequency	THREAT
Lack of awareness	Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings)	THREAT

ES-C2M2 Links

ES-C2M2 Model

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

ES-C2M2 Self-Evaluation Tool Requests, Questions, or Requests for Facilitation

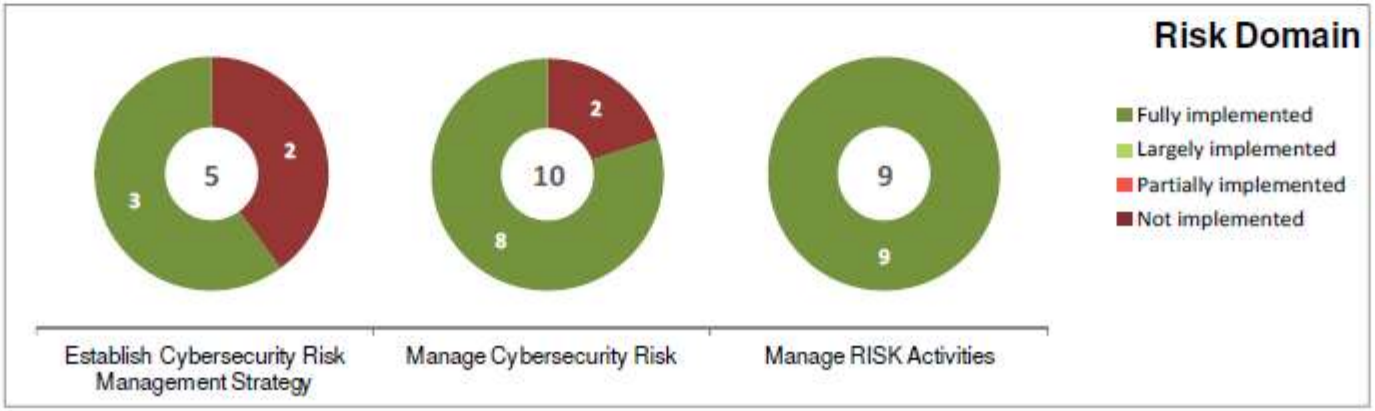
ES-C2M2@doe.gov

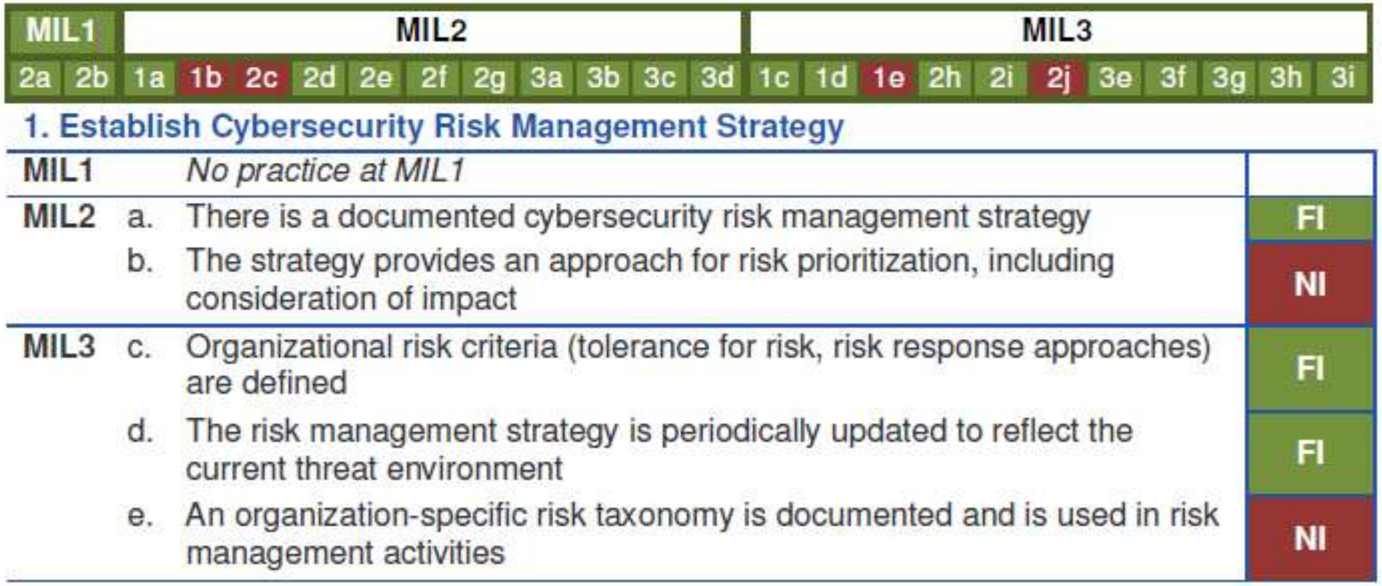
BACKUP MATERIALS

Evaluation by Function

- Function means which part of the organization is being evaluated
- Typically
  - Generation,
  - Transmission,
  - Distribution, or
  - Markets
- But may be a subset of one of these
  - The Facilitation Team used the ES-C2M2 to evaluate gas distribution of an entity. The tool covered most aspects of the ‘function’ with the exception of physical security.

Sample Domain Data





MIL1		MIL2											MIL3										
2a 🟩	2b 🟩	1a 🟩	1b 🟥	2c 🟥	2d 🟩	2e 🟩	2f 🟩	2g 🟩	3a 🟩	3b 🟩	3c 🟩	3d 🟩	1c 🟩	1d 🟩	1e 🟥	2h 🟩	2i 🟩	2j 🟥	3e 🟩	3f 🟩	3g 🟩	3h 🟩	3i 🟩

1. Establish Cybersecurity Risk Management Strategy

MIL1		*No practice at MIL1*	
MIL2	a.	There is a documented cybersecurity risk management strategy	FI
	b.	The strategy provides an approach for risk prioritization, including consideration of impact	NI
MIL3	c.	Organizational risk criteria (tolerance for risk, risk response approaches) are defined	FI
	d.	The risk management strategy is periodically updated to reflect the current threat environment	FI
	e.	An organization-specific risk taxonomy is documented and is used in risk management activities	NI

Maturity Indicator Level Guidelines

- Levels apply independently to each domain
- MILs are cumulative – to achieve MIL3, the organization must implement the MIL1, MIL2, and MIL3 practices
- Organizations should select MIL targets for each domain to align with cybersecurity strategies and objectives

Recommended Process for Using Results

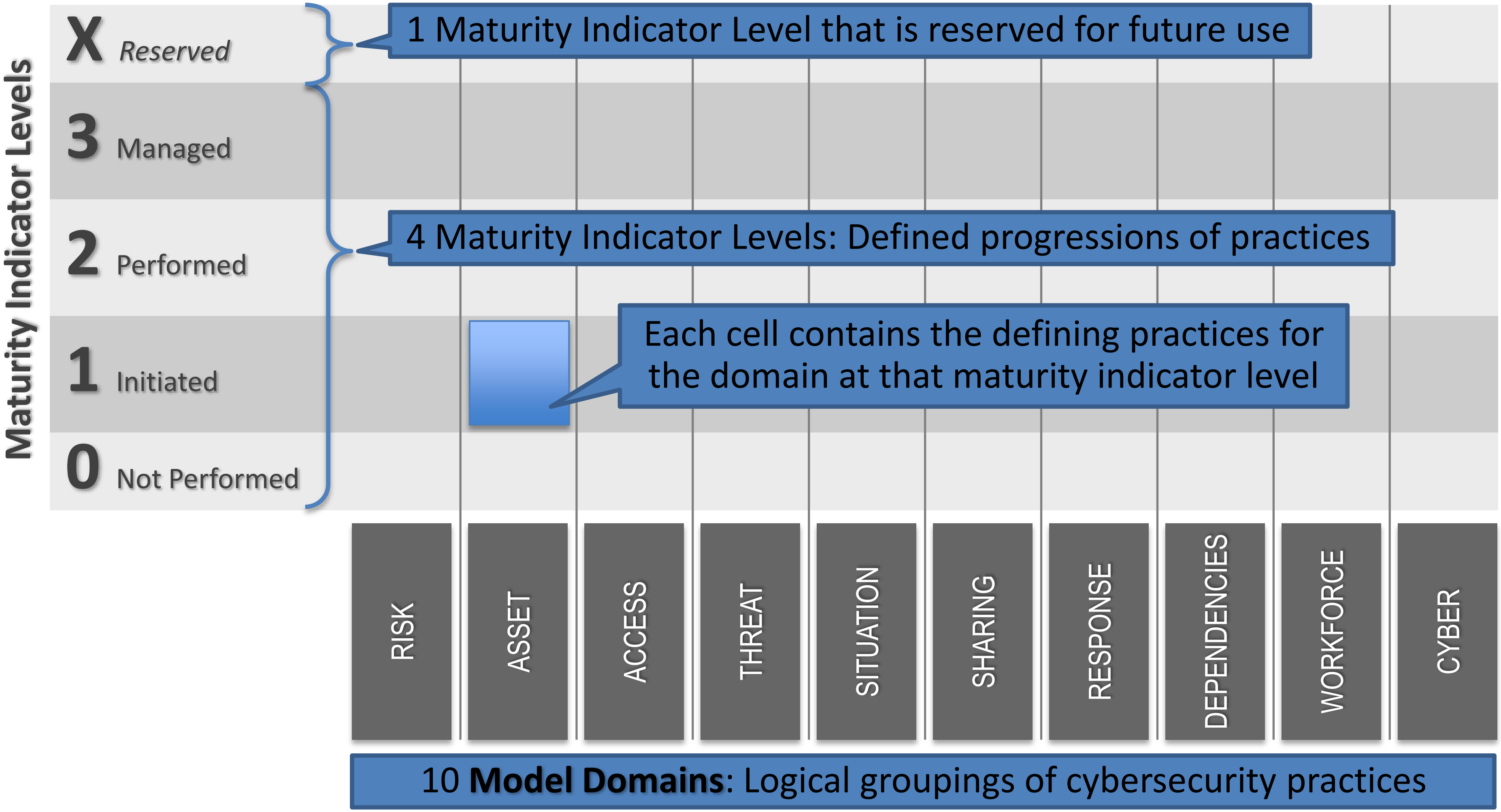
	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self-Evaluation Workshop with appropriate attendees	ES-C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	Prioritized implementation plan	1. Track progress to plan 2. Re-evaluate periodically or in response to major change	Project tracking data

Leveraged Resources and Inputs

1. CSET (tool)
2. CERT®-Resilience Management Model (CERT-RMM)
3. Capability Maturity Model Integrated (CMMI®)
4. Smart Grid Maturity Model (SGMM)
5. NESCO Security Logging CMM (model)
6. DHS Cyber Resilience Review (source)
7. International Society for Automation (ISA) 99
8. NERC Cyber Readiness Posture Assessment (tool)
9. Cross Sector Roadmap (source)
10. NISTIR 7628 (source)
11. NESCOR Failure Scenarios and Analyses (source)
12. EEI Threat Scenario Project Document (source)
13. Systems Security Engineering Capability Maturity Model (SSE-CMM)

…and there are many additional resources already referenced in the draft model

The Model at a Glance



Maturity Indicator Levels

X *Reserved*

3 Managed

2 Performed

1 Initiated

0 Not Performed

1 Maturity Indicator Level that is reserved for future use

4 Maturity Indicator Levels: Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level

RISK

ASSET

ACCESS

THREAT

SITUATION

SHARING

RESPONSE

DEPENDENCIES

WORKFORCE

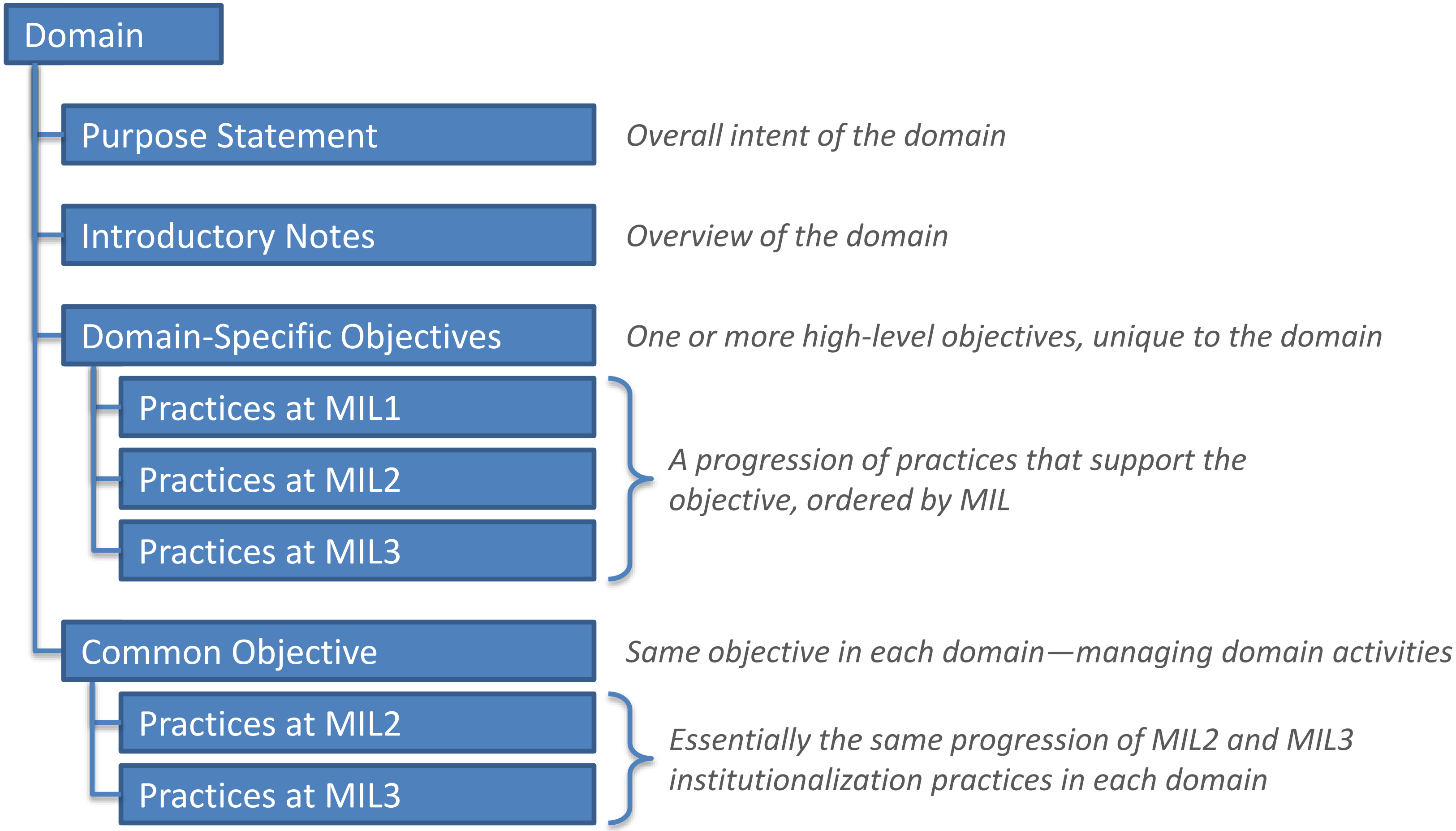
CYBER

10 **Model Domains**: Logical groupings of cybersecurity practices

Special Note about MIL1 Practices

- By design, MIL1 practices may be implemented in an ad hoc manner and still be considered “Fully Implemented”
- Ad hoc means
  - Practice performance may depend on initiative and experience of an individual or team, without much organizational guidance (policy and/or procedures)
  - Methods, tools, techniques, priority, and quality may vary significantly depending on who is performing the practice or when it is performed
  - Lessons learned may not be captured and outcomes may be difficult to repeat
- Even if ad hoc, the practice needs to meet business and critical infrastructure objectives to be “Fully Implemented”

Organization of a Domain



- Domain
  - Purpose Statement — *Overall intent of the domain*
  - Introductory Notes — *Overview of the domain*
  - Domain-Specific Objectives — *One or more high-level objectives, unique to the domain*
    - Practices at MIL1
    - Practices at MIL2
    - Practices at MIL3

    A progression of practices that support the objective, ordered by MIL
  - Common Objective — *Same objective in each domain—managing domain activities*
    - Practices at MIL2
    - Practices at MIL3

    Essentially the same progression of MIL2 and MIL3 institutionalization practices in each domain