Deloitte.

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

A Brief Overview

SPP RE Workshop
May 24, 2016

Agenda

- About Me
- Brief History: Why was the ES-C2M2 Developed?
- Overview of the Model
- Alignment with the NIST Framework
- Questions

About Me

Manager, Deloitte Advisory
Cyber Risk Services
Denver, CO

Prior:
NERC / ES-ISAC: Cybersecurity Specialist [CRISP Program Manager]
US Department of Energy: Infrastructure Analyst [ES-C2M2, RMP]

ES-C2M2 Experience:

- Member of the ES-C2M2 development team while at DOE
- Conducted over a dozen assessments using the ES-C2M2
- ES-C2M2 program manager prior to leaving DOE

Deloitte Advisory Experience:

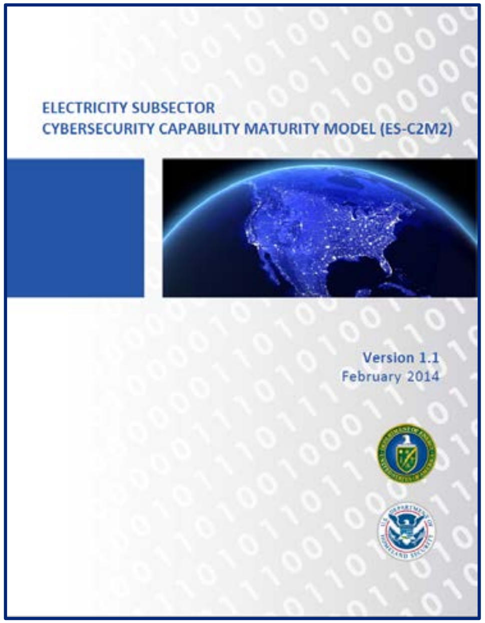
- Supported the NERC CIP v5 implementation at a large IOU
- Responsible for strengthening cybersecurity programs through governance, policies, procedures and implementation of cybersecurity technologies

Brief History

Why was the ES-C2M2 developed?

History:

- Developed by DOE in partnership with DHS and collaboration with industry experts
- Conducted over a dozen pilot evaluations with utilities during development
- Briefed to White House staff and released in May 2012



ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

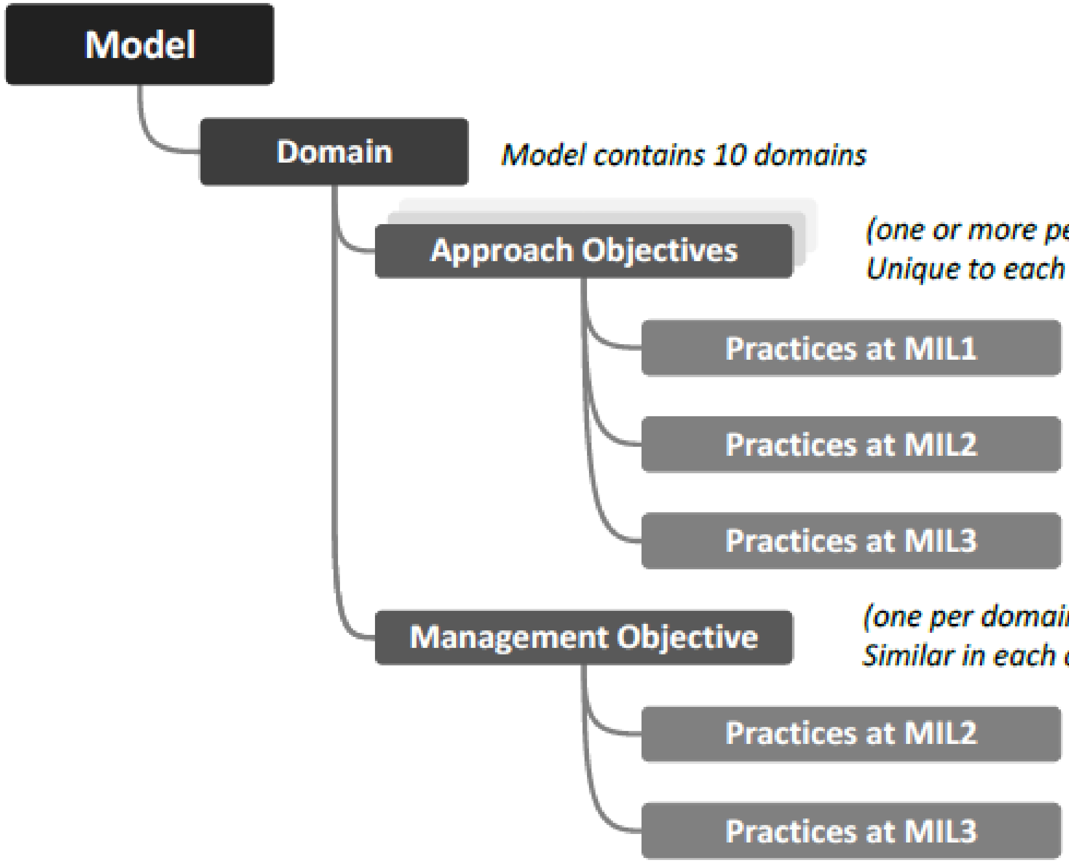
Version 1.1
February 2014

Purpose:

- Strengthen cybersecurity capabilities in the electricity subsector
- Enable utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities
- Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities
- Enable utilities to prioritize actions and investments to improve cybersecurity

Overview of the Model

Structure



Model contains 10 domains

(one or more per domain)
Unique to each domain

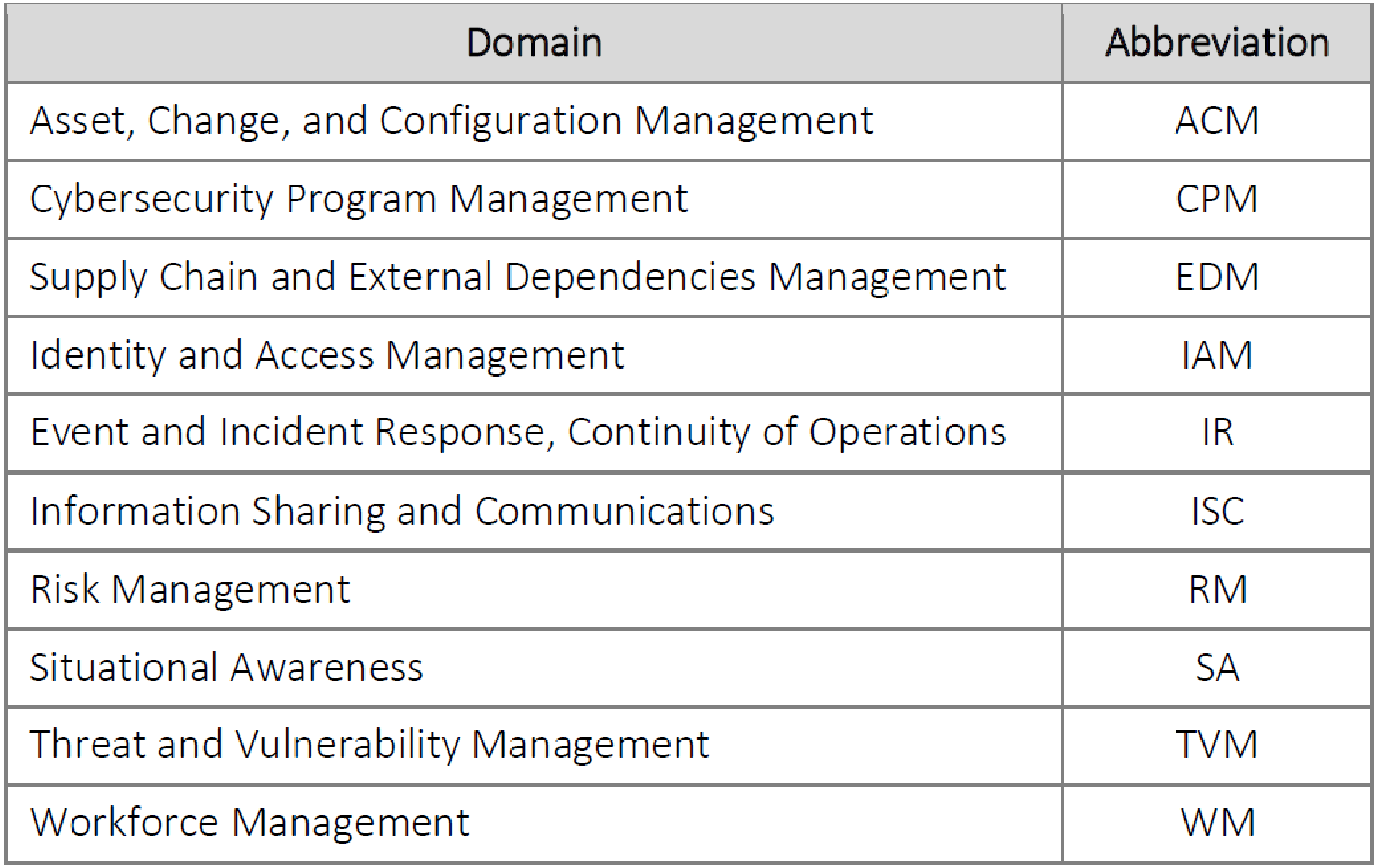
Approach objectives are supported by a progression of practices that are unique to the domain

(one per domain)
Similar in each domain

Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities

Overview of the Model

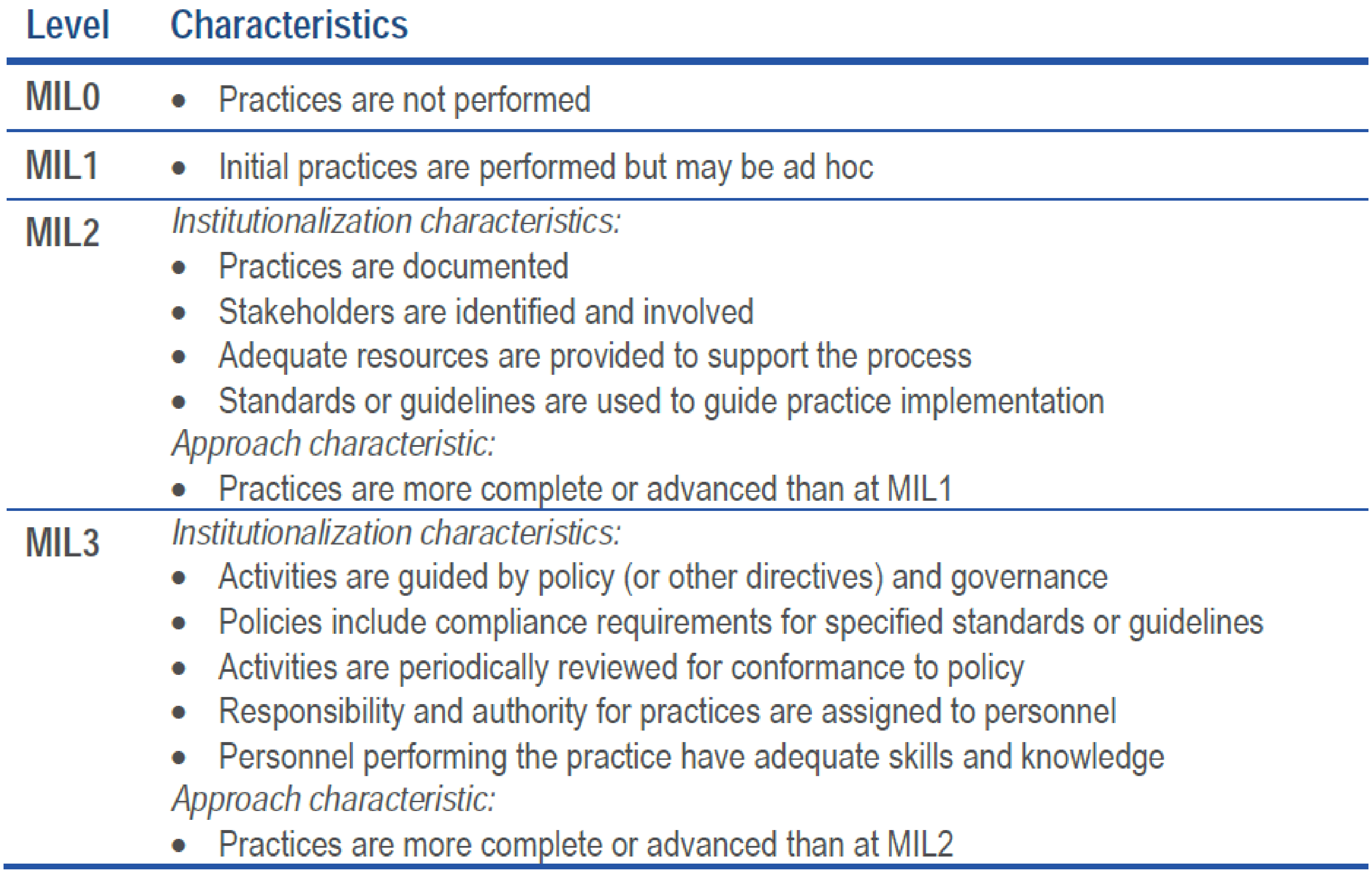
Domains



Domain	Abbreviation
Asset, Change, and Configuration Management	ACM
Cybersecurity Program Management	CPM
Supply Chain and External Dependencies Management	EDM
Identity and Access Management	IAM
Event and Incident Response, Continuity of Operations	IR
Information Sharing and Communications	ISC
Risk Management	RM
Situational Awareness	SA
Threat and Vulnerability Management	TVM
Workforce Management	WM

Overview of the Model

Maturity Indicator Level (MIL)



Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	*Institutionalization characteristics:* • Practices are documented • Stakeholders are identified and involved • Adequate resources are provided to support the process • Standards or guidelines are used to guide practice implementation *Approach characteristic:* • Practices are more complete or advanced than at MIL1
MIL3	*Institutionalization characteristics:* • Activities are guided by policy (or other directives) and governance • Policies include compliance requirements for specified standards or guidelines • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are assigned to personnel • Personnel performing the practice have adequate skills and knowledge *Approach characteristic:* • Practices are more complete or advanced than at MIL2

Overview of the Model

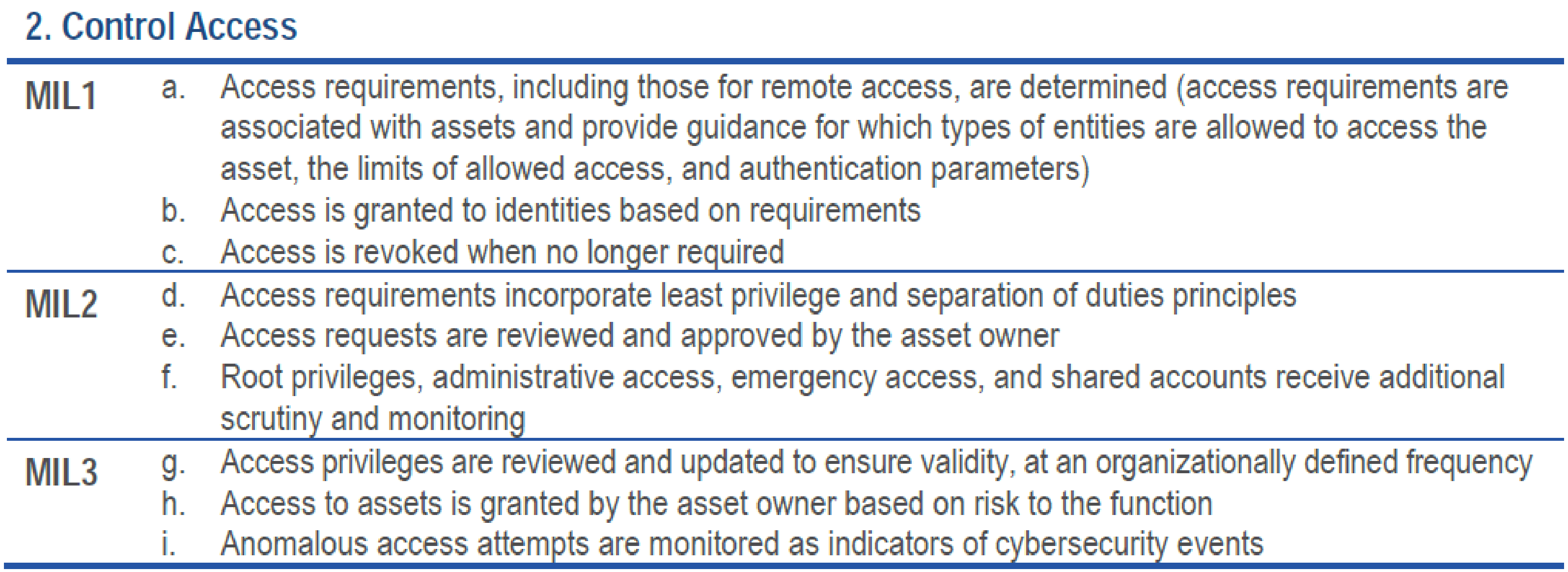
Putting it together

Domain: Identity and Access Management

Purpose: 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.

Objectives:

1. Establish and Maintain Identities
2. Control Access
3. Management Activities



2. Control Access

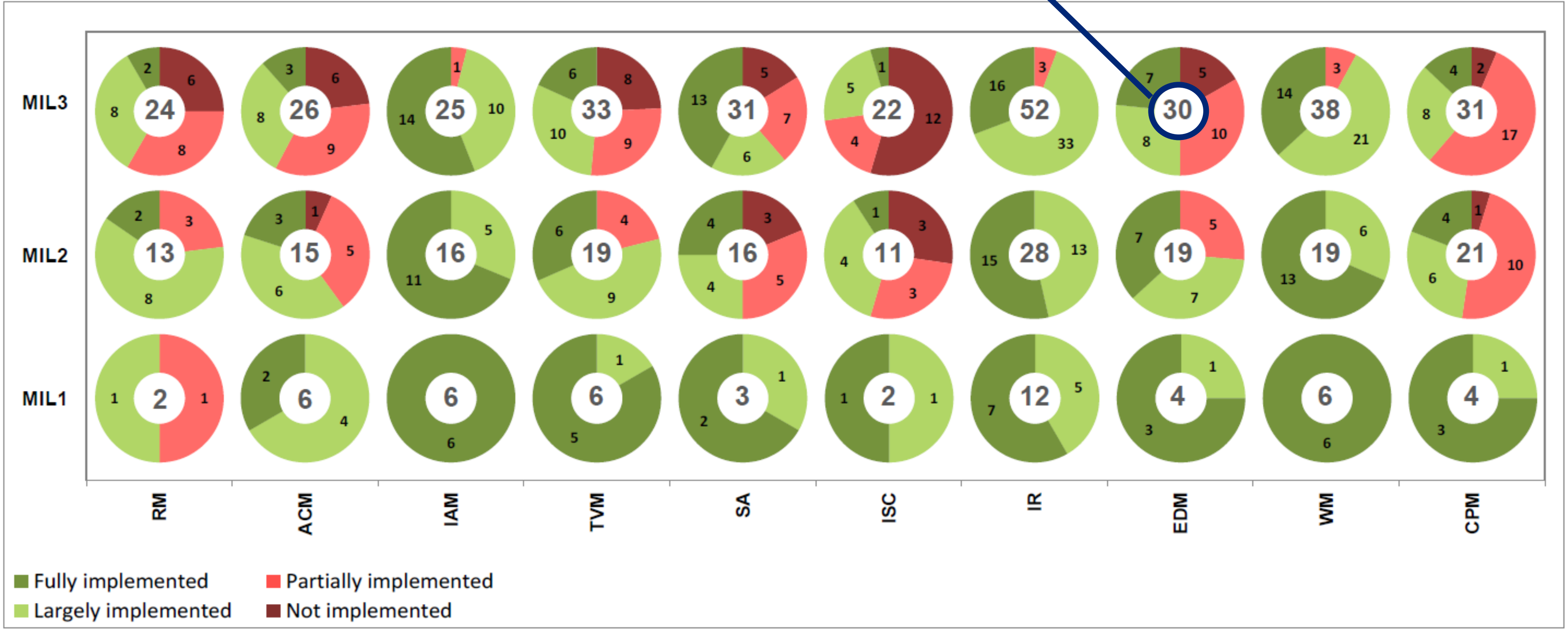
MIL1	a.	Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)
	b.	Access is granted to identities 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

Overview of the Model

Output

Scoring Report

Total Number of Practices for that Domain (cumulative)

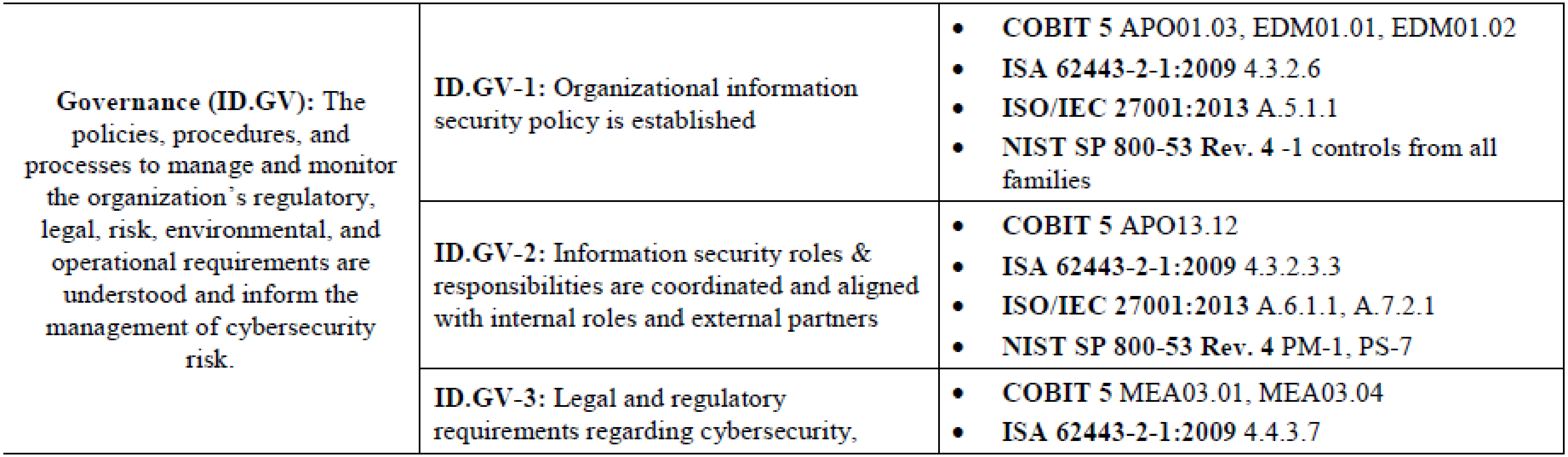


Alignment with the NIST Framework

Example

Function: Identify

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.



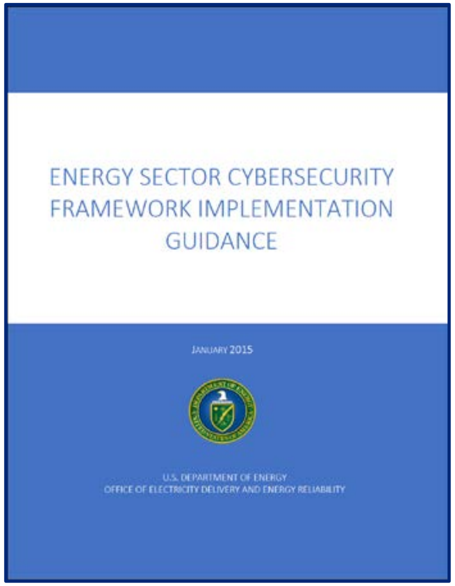
Category	Subcategory	Informative References
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity,	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7

Alignment with the NIST Framework

Mapping ES-C2M2 to the NIST Framework

Function: Protect

Framework Core		C2M2 Practices		
Category	**Subcategory**	MIL 1	MIL 2	MIL3
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



ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE

JANUARY 2015

U.S. DEPARTMENT OF ENERGY
OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY

Questions?

Contact Info:

Matt Light
Deloitte Advisory, Cyber Risk
Denver, CO
mlight@Deloitte.com
303-917-1413

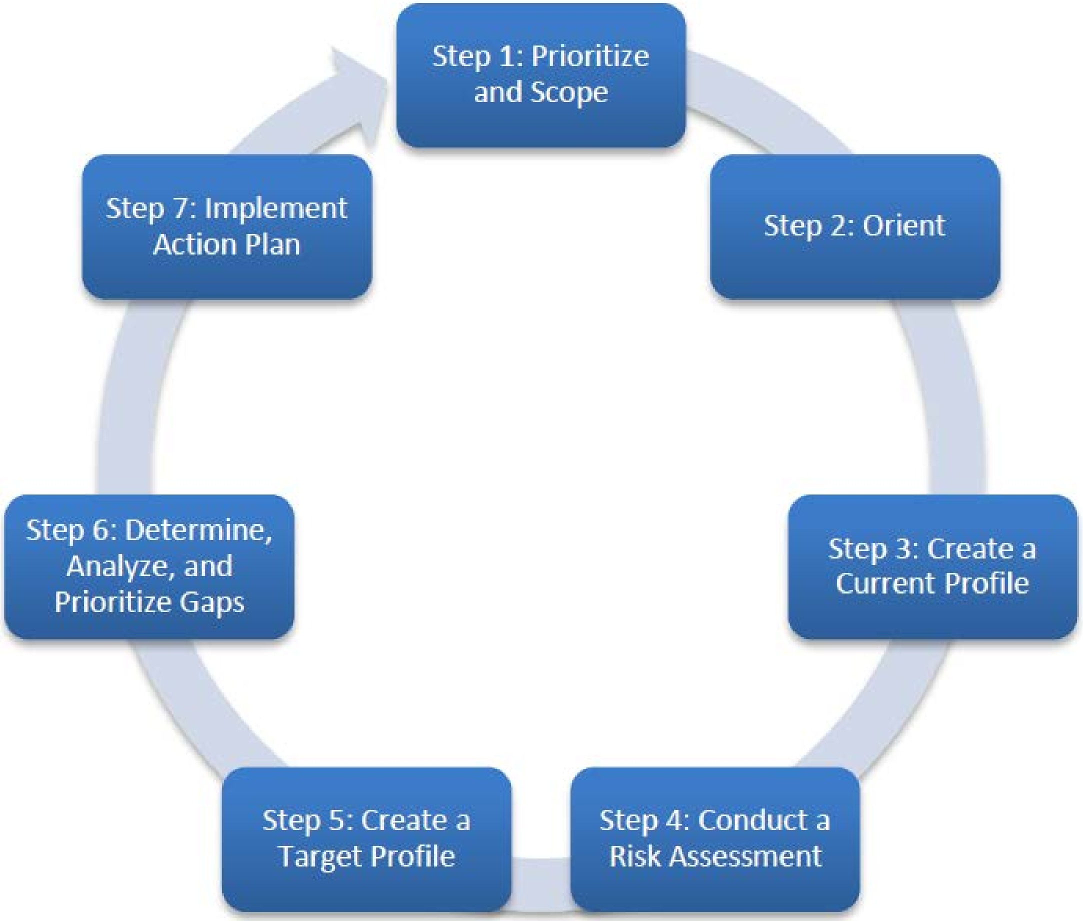
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Backup Slides

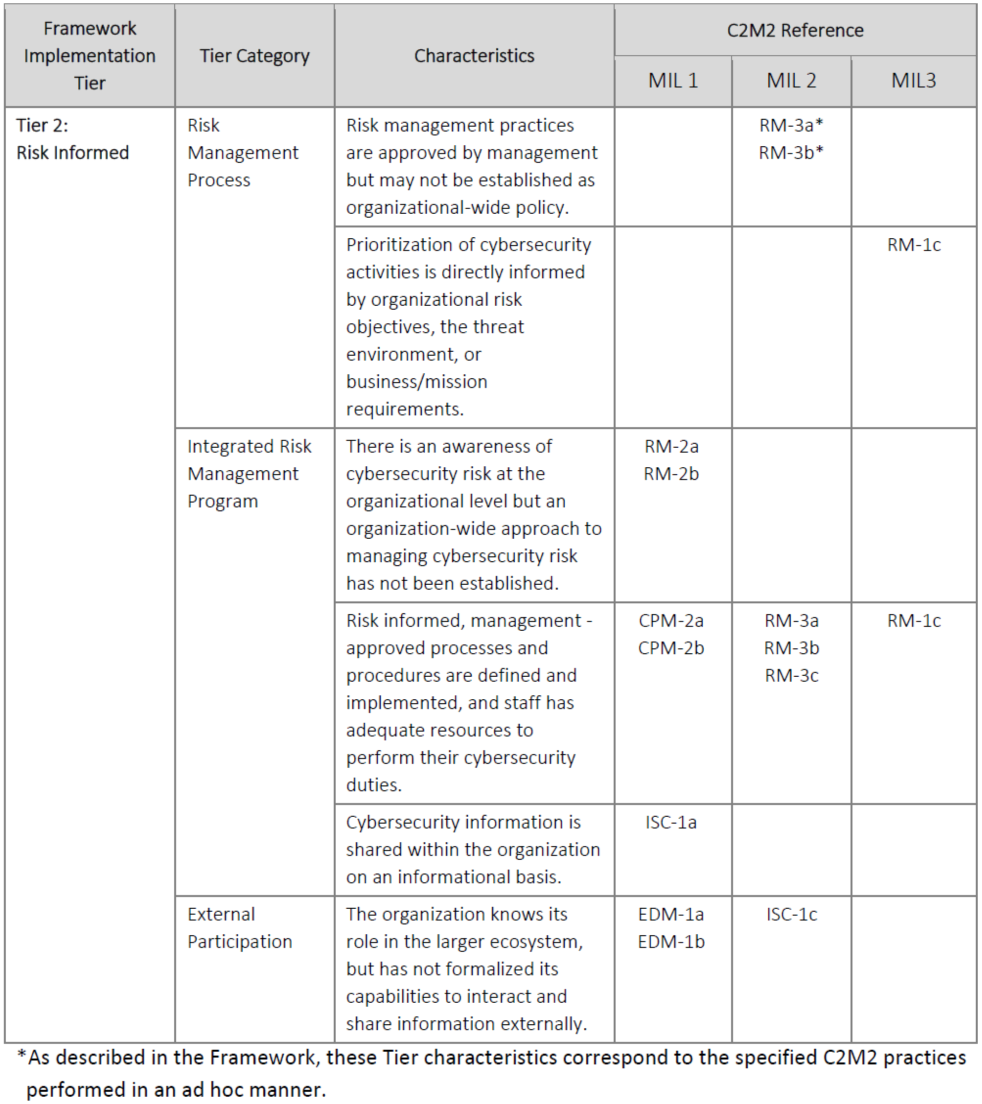
NIST Framework

Framework Implementation Approach


Step 1: Prioritize and Scope
Step 2: Orient
Step 3: Create a Current Profile
Step 4: Conduct a Risk Assessment
Step 5: Create a Target Profile
Step 6: Determine, Analyze, and Prioritize Gaps
Step 7: Implement Action Plan

NIST Framework

Tier vs. MIL



Framework Implementation Tier	Tier Category	Characteristics	C2M2 Reference		
			MIL 1	MIL 2	MIL3
Tier 2: Risk Informed	Risk Management Process	Risk management practices are approved by management but may not be established as organizational-wide policy.		RM-3a* RM-3b*	
		Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.			RM-1c
	Integrated Risk Management Program	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.	RM-2a RM-2b		
		Risk informed, management - approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties.	CPM-2a CPM-2b	RM-3a RM-3b RM-3c	RM-1c
		Cybersecurity information is shared within the organization on an informational basis.	ISC-1a		
	External Participation	The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.	EDM-1a EDM-1b	ISC-1c	

*As described in the Framework, these Tier characteristics correspond to the specified C2M2 practices performed in an ad hoc manner.

Integrated Security

Security at OGE - Agenda

POSITIVE ENERGY TOGETHER®

- ➢ Program Vision
- ➢ Integrated Security Capabilities
- ➢ Roadmap & Closing Gaps
- ➢ Measuring success
- ➢ Key Take Aways

Security Vision

OGE Security will be aware of its adversaries (threats) with an effective prevention, detection, defense and response strategy. Security will protect personnel and also those cyber and physical assets enabling OGE's business and operational capabilities.

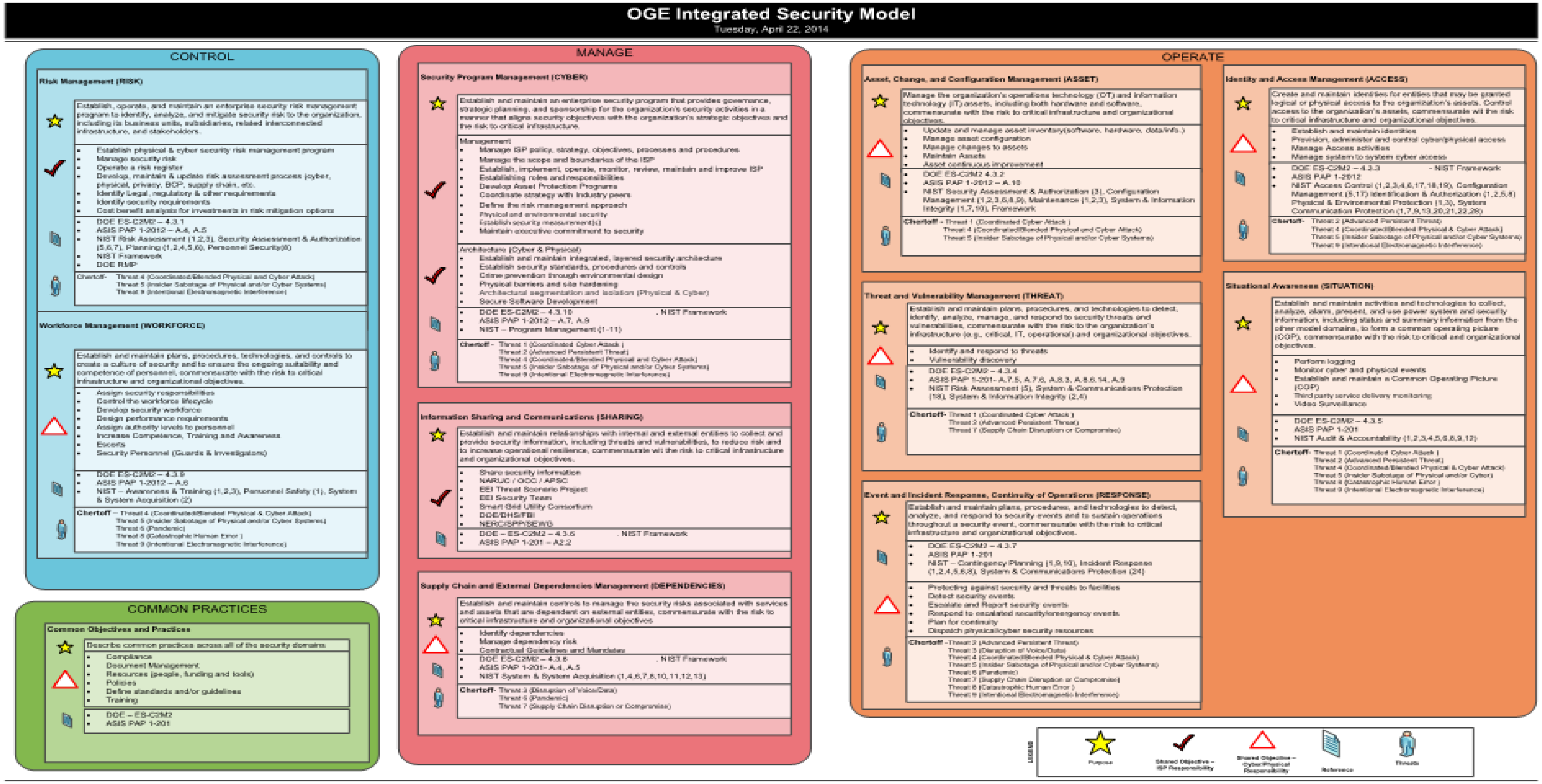
Advantages of C2M2

- Establish long-term investment strategy
- Measure success
- Communicate direction and strategy to Board of Directors and other senior leaders.

Integrated Security Capabilities

POSITIVE
ENERGY
TOGETHER®

The starting point was to identify the rudimentary capabilities of successful security programs



OGE Integrated Security Model

Tuesday, April 22, 2014

CONTROL

Risk Management (RISK)

★ Establish, operate, and maintain an enterprise security risk management program to identify, analyze, and mitigate security risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

✓
- Establish physical & cyber security risk management program
- Manage security risk
- Operate a risk register
- Develop, maintain & update risk assessment process (cyber, physical, privacy, BCP, supply chain, etc.
- Identify Legal, regulatory & other requirements
- Identify security requirements
- Cost benefit analysis for investments in risk mitigation options

📄
- DOE ES-C2M2 – 4.3.1
- ASIS PAP 1-2012 – A.4, A.5
- NIST Risk Assessment (1,2,3), Security Assessment & Authorization (5,6,7), Planning (1,2,4,5,6), Personnel Security(8)
- NIST Framework
- DOE RMP

👤 Chertoff- Threat 4 (Coordinated/Blended Physical and Cyber Attack)
Threat 5 (Insider Sabotage of Physical and/or Cyber Systems)
Threat 9 (Intentional Electromagnetic Interference)

Workforce Management (WORKFORCE)

★ Establish and maintain plans, procedures, technologies, and controls to create a culture of security and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

△
- Assign security responsibilities
- Control the workforce lifecycle
- Develop security workforce
- Design performance requirements
- Assign authority levels to personnel
- Increase Competence, Training and Awareness
- Escorts
- Security Personnel (Guards & Investigations)

📄
- DOE ES-C2M2 – 4.3.9
- ASIS PAP 1-2012 – A.6
- NIST – Awareness & Training (1,2,3), Personnel Safety (1), System & System Acquisition (2)

👤 **Chertoff** – Threat 4 (Coordinated/Blended Physical & Cyber Attack)
Threat 5 (Insider Sabotage of Physical and/or Cyber Systems)
Threat 6 (Pandemic)
Threat 8 (Catastrophic Human Error)
Threat 9 (Intentional Electromagnetic Interference)

COMMON PRACTICES

Common Objectives and Practices

★ Describe common practices across all of the security domains

△
- Compliance
- Document Management
- Resources (people, funding and tools)
- Policies
- Define standards and/or guidelines
- Training

📄
- DOE – ES-C2M2
- ASIS PAP 1-201

MANAGE

Security Program Management (CYBER)

★ Establish and maintain an enterprise security program that provides governance, strategic planning, and sponsorship for the organization's security activities in a manner that aligns security objectives with the organization's strategic objectives and the risk to critical infrastructure.

✓ Management
- Manage ISP policy, strategy, objectives, processes and procedures
- Manage the scope and boundaries of the ISP
- Establish, implement, operate, monitor, review, maintain and improve ISP
- Establishing roles and responsibilities
- Develop Asset Protection Programs
- Coordinate strategy with industry peers
- Define the risk management approach
- Physical and environmental security
- Establish security measurement(s)
- Maintain executive commitment to security

✓ Architecture (Cyber & Physical)
- Establish and maintain integrated, layered security architecture
- Establish security standards, procedures and controls
- Crime prevention through environmental design
- Physical barriers and site hardening
- Architectural segmentation and isolation (Physical & Cyber)
- Secure Software Development

📄
- DOE ES-C2M2 – 4.3.10 . NIST Framework
- ASIS PAP 1-2012 – A.7, A.9
- NIST – Program Management (1-11)

👤 Chertoff - Threat 1 (Coordinated Cyber Attack)
Threat 2 (Advanced Persistent Threat)
Threat 4 (Coordinated/Blended Physical and Cyber Attack)
Threat 5 (Insider Sabotage of Physical and/or Cyber Systems)
Threat 9 (Intentional Electromagnetic Interference)

Information Sharing and Communications (SHARING)

★ Establish and maintain relationships with internal and external entities to collect and provide security information, including threats and vulnerabilities, to reduce risk and to increase operational resilience, commensurate wi the risk to critical infrastructure and organizational objectives.

✓
- Share security information
- NARUC / OCC / APSC
- EEI Threat Scenario Project
- EEI Security Team
- Smart Grid Utility Consortium
- DOE/DHS/FBI
- NERC/SPP/SEWG

📄
- DOE – ES-C2M2 – 4.3.6 . NIST Framework
- ASIS PAP 1-201 – A2.2

Supply Chain and External Dependencies Management (DEPENDENCIES)

★ Establish and maintain controls to manage the security risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

△
- Identify dependencies
- Manage dependency risk
- Contractual Guidelines and Mandates

📄
- DOE ES-C2M2 – 4.3.8 . NIST Framework
- ASIS PAP 1-201- A.4, A.5
- NIST System & System Acquisition (1,4,6,7,8,10,11,12,13)

👤 **Chertoff**- Threat 3 (Disruption of Voice/Data)
Threat 6 (Pandemic)
Threat 7 (Supply Chain Disruption or Compromise)

OPERATE

Asset, Change, and Configuration Management (ASSET)

★ Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.

△
- Update and manage asset inventory(software, hardware, data/info.)
- Manage asset configuration
- Manage changes to assets
- Maintain Assets
- Asset continuous improvement

📄
- DOE ES-C2M2 4.3.2
- ASIS PAP 1-2012 – A.10
- NIST Security Assessment & Authorization (3), Configuration Management (1,2,3,6,8,9), Maintenance (1,2,3), System & Information Integrity (1,7,10), Framework

👤 **Chertoff** - Threat 1 (Coordinated Cyber Attack)
Threat 4 (Coordinated/Blended Physical and Cyber Attack)
Threat 5 (Insider Sabotage of Physical and/or Cyber Systems)

Identity and Access Management (ACCESS)

★ Create and maintain identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate wit the risk to critical infrastructure and organizational objectives.

△
- Establish and maintain identities
- Provision, administer and control cyber/physical access
- Manage Access activities
- Manage system to system cyber access

📄
- DOE ES-C2M2 – 4.3.3 - NIST Framework
- ASIS PAP 1-2012
- NIST Access Control (1,2,3,4,6,17,18,19), Configuration Management (5,17) Identification & Authorization (1,2,5,8) Physical & Environmental Protection (1,3), System Communication Protection (1,7,9,13,20,21,22,28)

👤 **Chertoff**- Threat 2 (Advanced Persistent Threat)
Threat 4 (Coordinated/Blended Physical & Cyber Attack)
Threat 5 (Insider Sabotage of Physical and/or Cyber Systems)
Threat 9 (Intentional Electromagnetic Interference)

Threat and Vulnerability Management (THREAT)

★ Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to security threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

△
- Identify and respond to threats
- Vulnerability discovery

📄
- DOE ES-C2M2 – 4.3.4
- ASIS PAP 1-201- A.7.5, A.7.6, A.8.3, A.8.6.14, A.9
- NIST Risk Assessment (5), System & Communications Protection (18), System & Information Integrity (2,4)

👤 **Chertoff**- Threat 1 (Coordinated Cyber Attack)
Threat 2 (Advanced Persistent Threat)
Threat 7 (Supply Chain Disruption or Compromise)

Situational Awareness (SITUATION)

★ Establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and security information, including status and summary information from the other model domains, to form a common operating picture (COP), commensurate with the risk to critical and organizational objectives.

△
- Perform logging
- Monitor cyber and physical events
- Establish and maintain a Common Operating Picture (COP)
- Third party service delivery monitoring
- Video Surveillance

📄
- DOE ES-C2M2 – 4.3.5
- ASIS PAP 1-201
- NIST Audit & Accountability (1,2,3,4,5,6,8,9,12)

👤 **Chertoff**- Threat 1 (Coordinated Cyber Attack)
Threat 2 (Advanced Persistent Threat)
Threat 4 (Coordinated/Blended Physical & Cyber Attack)
Threat 5 (Insider Sabotage of Physical and/or Cyber)
Threat 8 (Catastrophic Human Error)
Threat 9 (Intentional Electromagnetic Interference)

Event and Incident Response, Continuity of Operations (RESPONSE)

★ Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to security events and to sustain operations throughout a security event, commensurate with the risk to critical infrastructure and organizational objectives.

📄
- DOE ES-C2M2 – 4.3.7
- ASIS PAP 1-201
- NIST – Contingency Planning (1,9,10), Incident Response (1,2,4,5,6,8), System & Communications Protection (24)

△
- Protecting against security and threats to facilities
- Detect security events
- Escalate and Report security events
- Respond to escalated security/emergency events
- Plan for continuity
- Dispatch physical/cyber security resources

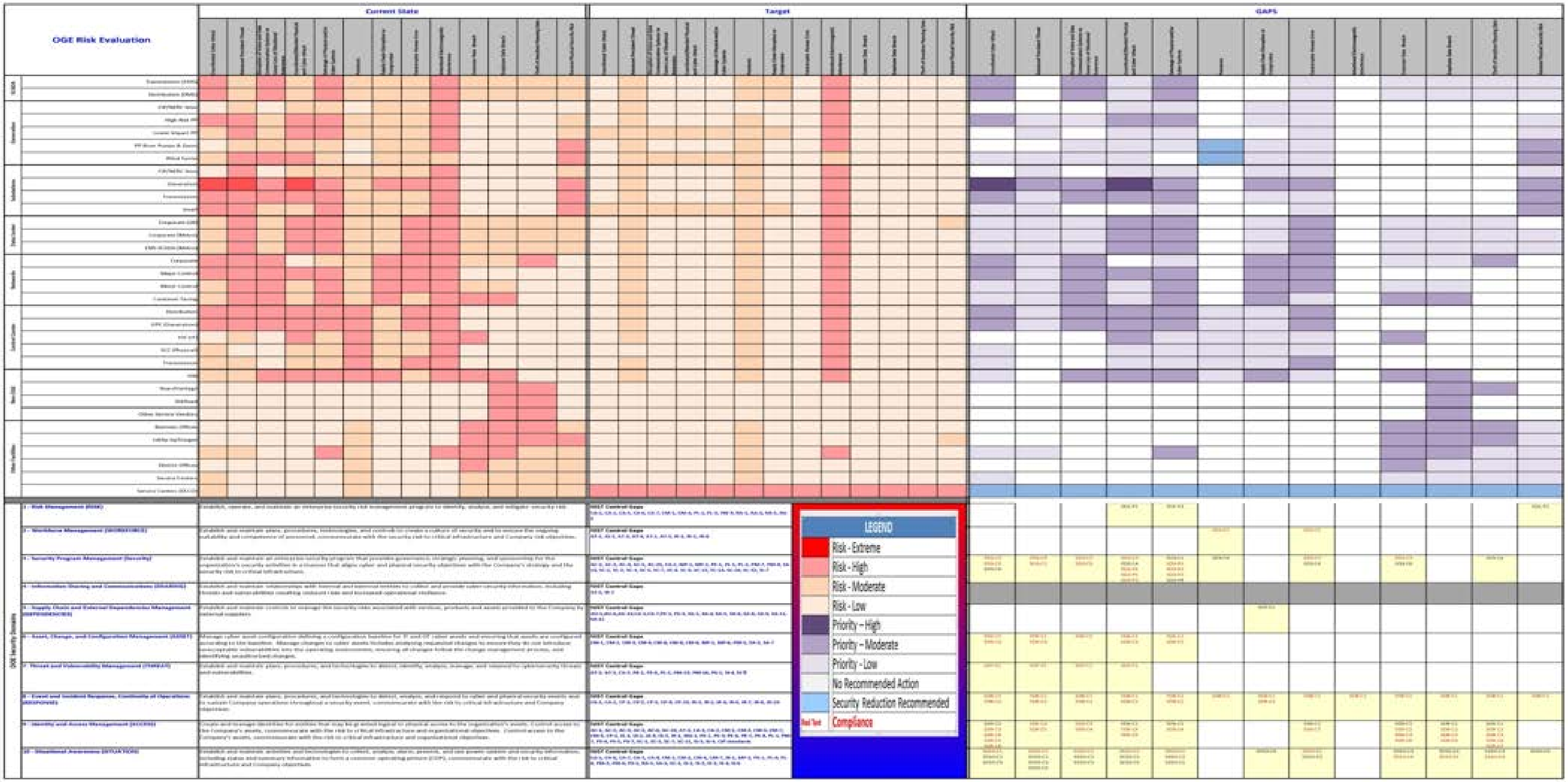
👤 **Chertoff** - Threat 2 (Advanced Persistent Threat)
Threat 3 (Disruption of Voice/Data)
Threat 4 (Coordinated/Blended Physical & Cyber Attack)
Threat 5 (Insider Sabotage of Physical and/or Cyber Systems)
Threat 6 (Pandemic)
Threat 7 (Supply Chain Disruption or Compromise)
Threat 8 (Catastrophic Human Error)
Threat 9 (Intentional Electromagnetic Interference)

LEGEND

★	✓	△	📄	👤
Purpose	Shared Objective – ISP Responsibility	Shared Objective – Cyber/Physical Responsibility	Reference	Threats

Current state/future state

POSITIVE ENERGY TOGETHER®



OGE Risk Evaluation

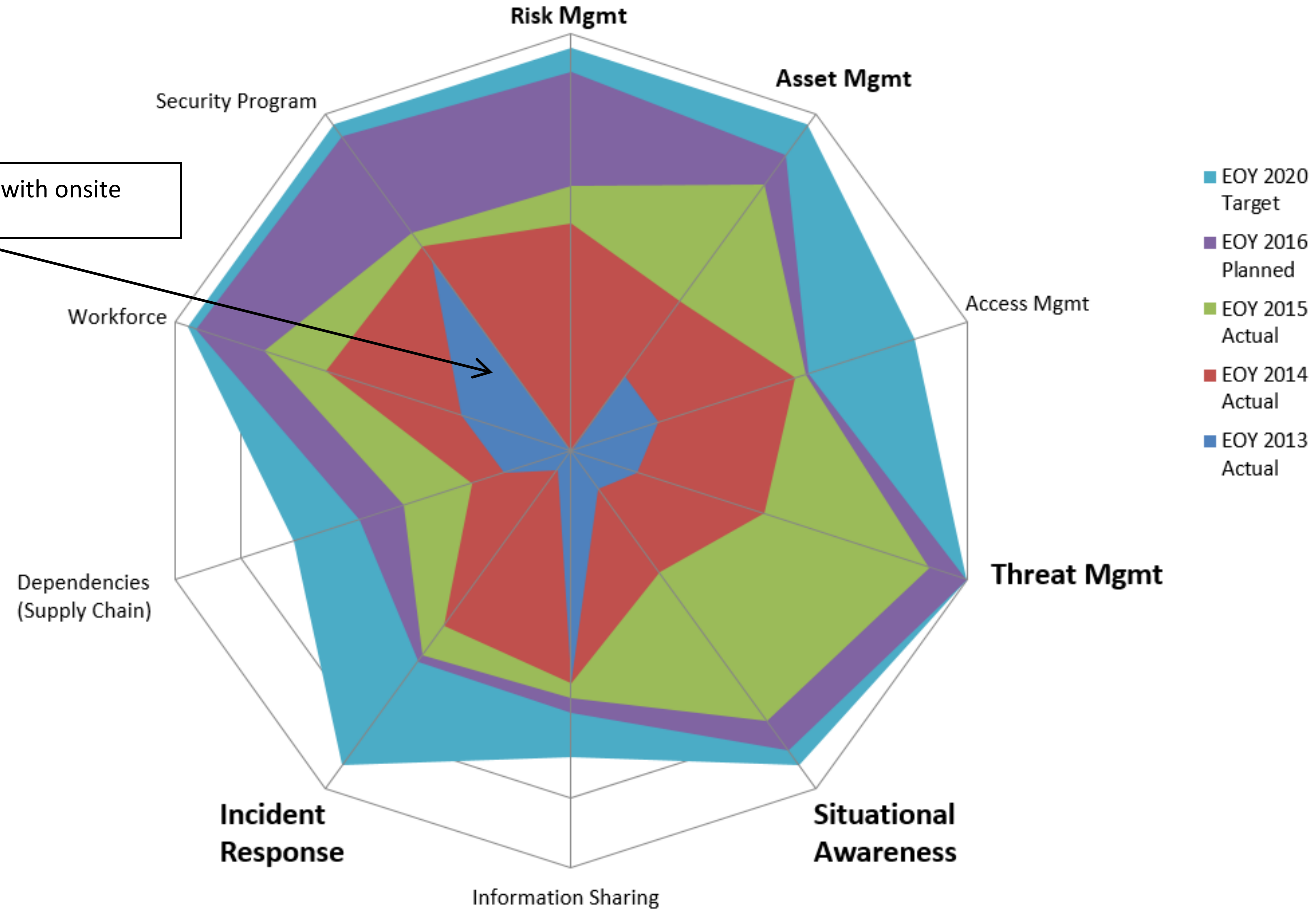
Current State	Target	GAPS
[illegible]	[illegible]	[illegible]

LEGEND

🟥	Risk - Extreme
🟥	Risk - High
🟧	Risk - Moderate
▫	Risk - Low
▨	Priority – High
▨	Priority – Moderate
▫	Priority - Low
▫	No Recommended Action
🟦	Security Reduction Recommended
Red Text	Compliance

OGE has matured its security capabilities using a prioritized approach since 2013

Based on security maturity dimensions established by the Department of Energy



2013 Model developed with onsite guidance from DOE.

Key Takeaways

- Extend C2M2 to allow for the integration of cyber and physical security.
- Develop a long-term strategy using a tool like C2M2 is key to a successful program.
- Using C2M2 for communicating to senior leaders has proven quite beneficial.
- Apply C2M2 to all initiatives, e.g. compliance, NERC Alerts, projects to counter threats & eliminate vulnerabilities, etc.
- Use of C2M2 requires a long-term commitment by security leaders.

Questions?