

CYBER SECURITY WORKING GROUP

MARIANNE SWANSON
CSWG CHAIR

DECEMBER 4, 2012
8:30 – 10:00 AM CST

WINTER 2012 FACE-TO-FACE
IRVING, TEXAS • DEC. 3-6, 2012



SGiP SMART GRID
INTEROPERABILITY PANEL

Agenda

2

December 4, 2012

- 8:30 – 8:40 AM Welcome (Marianne Swanson)
- 8:40 – 9:00 AM Department of Energy (DOE) Update (Matthew Light)
- 9:00 – 9:20 AM Privacy Subgroup Update (Rebecca Herold)
- 9:20 – 10:00 AM SGIP 2.0 Briefing and Q&A (Mike Coop/George Bjelovuk)



Welcome

Marianne Swanson

CSWG Chair

marianne.swanson@nist.gov

Grid-Interop

WINTER 2012 FACE-TO-FACE
IRVING, TEXAS

SGiP

Sponsored by:



Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Program

Participating Organizations:



WINTER 2012 FACE-TO-FACE
IRVING, TEXAS



ES-C2M2 Development and Pilot

5

- Public-Private collaborative effort
- Leveraged existing guidance and knowledge
 - CMU Software Engineering Institute
 - Appendix A References
- Short timeframe for development
 - Initiated Jan 2012, Ver 1 released May 2012
 - 17 pilot assessments
 - Feedback resulted in significant changes to the model

ES-C2M2 Background & Overview

6

- **Challenge:** Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid

ES-C2M2 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: Industry Use and Adoption

7

Requesting entity type	Organizations ¹	Individuals ²
Utilities		
Cooperative	12	12
International	3	3
Investor-owned	27	33
Public power	32	36
Regional Transmission Organization	2	2
Total Utilities	77	87
Non-utilities	63	69
International	13	13
TOTAL	153	169

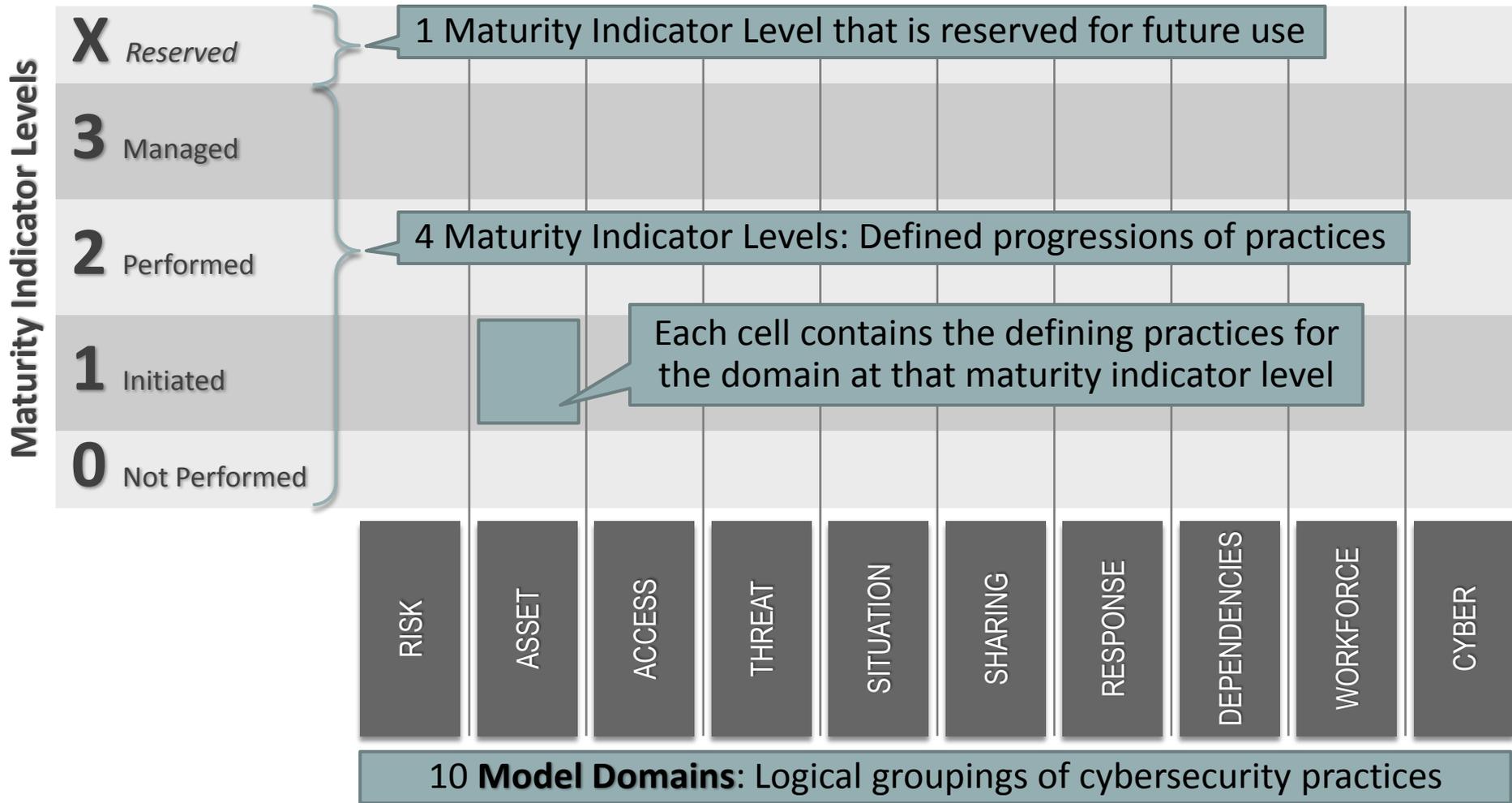
1. Total number of unique organizations that have received the ES-C2M2 Self Evaluation Toolkit.
2. total number of unique individuals that have received the ES-C2M2 Self Evaluation Toolkit.



ES-C2M2 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	<ul style="list-style-type: none">• Domains are logical groupings of cybersecurity practices• Each domain has a short name for easy reference	

The Model at a Glance



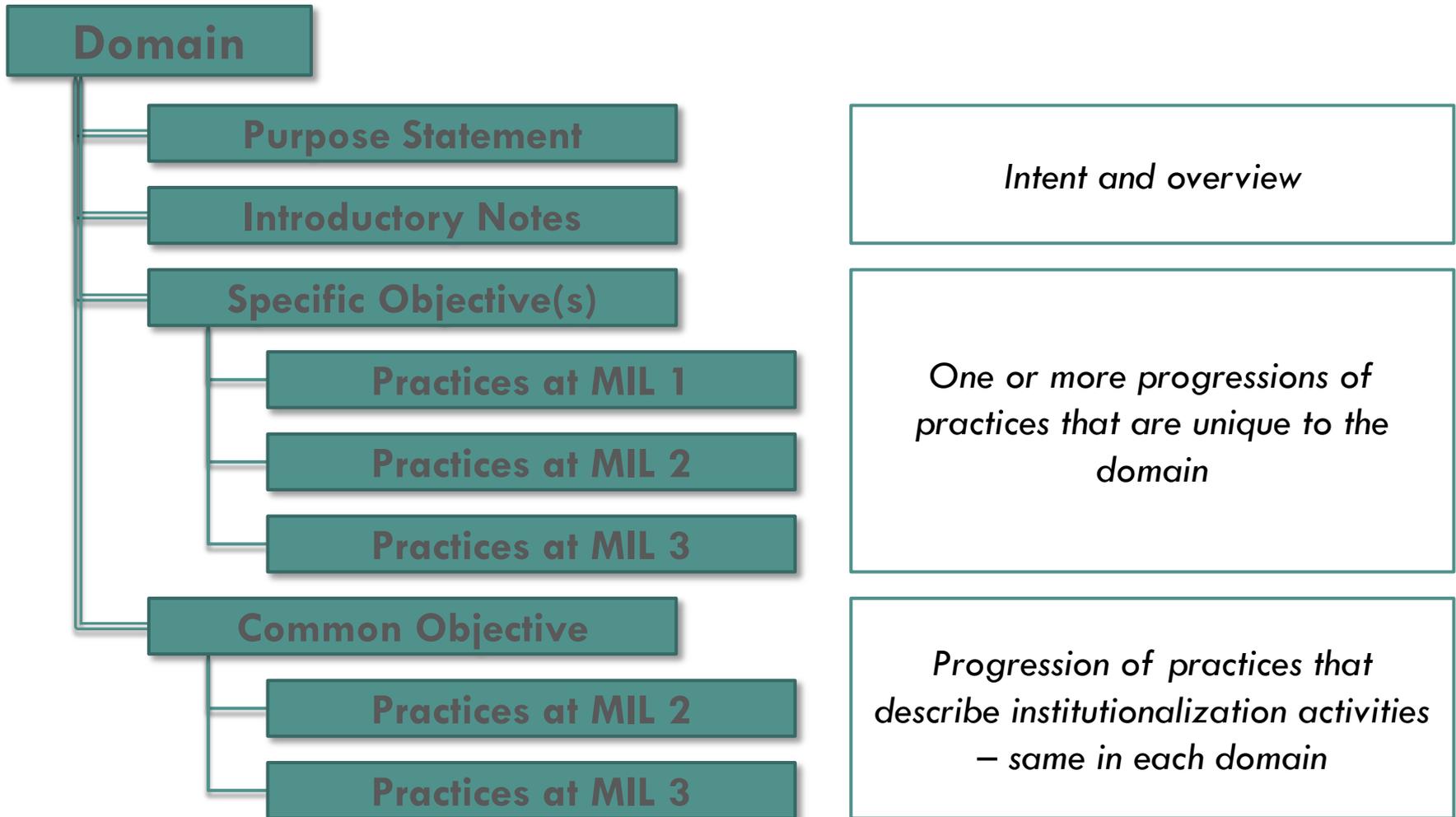
Maturity Indicator Level Descriptions

10

Level	Name	Description
MIL0	Not Performed	<ul style="list-style-type: none">• MIL1 has not been achieved in the domain
MIL1	Initiated	<ul style="list-style-type: none">• Initial practices are performed, but may be ad hoc
MIL2	Performed	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

Domain Structure

11



Example Objective: ASSET-3

12

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

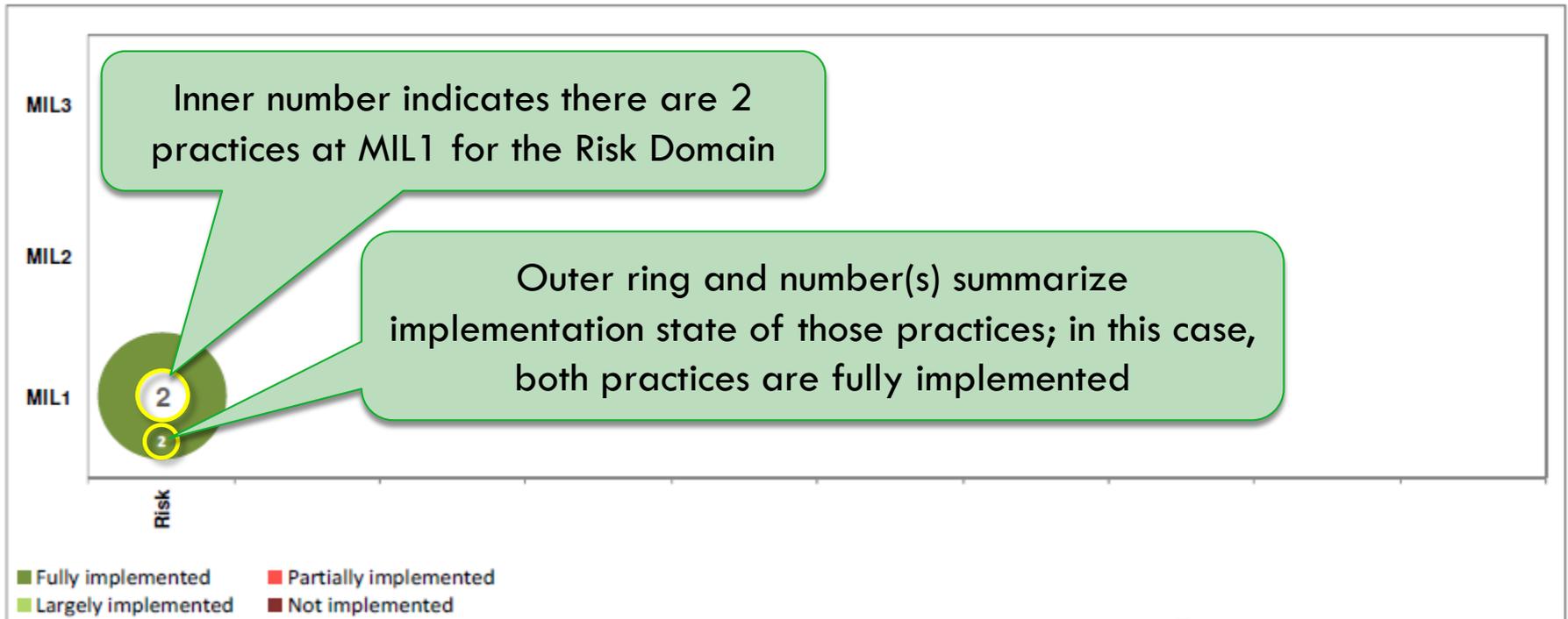
ASSET DOMAIN

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) |

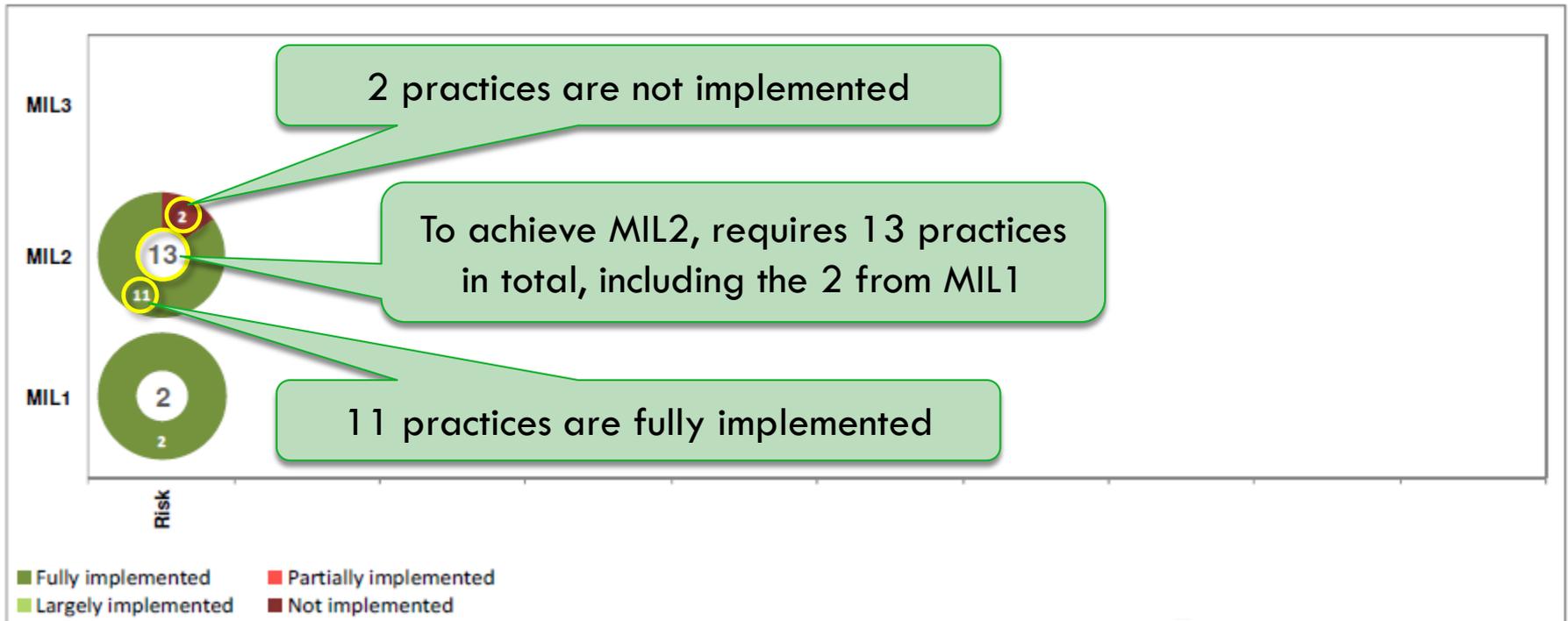
Sample Summary Score

13



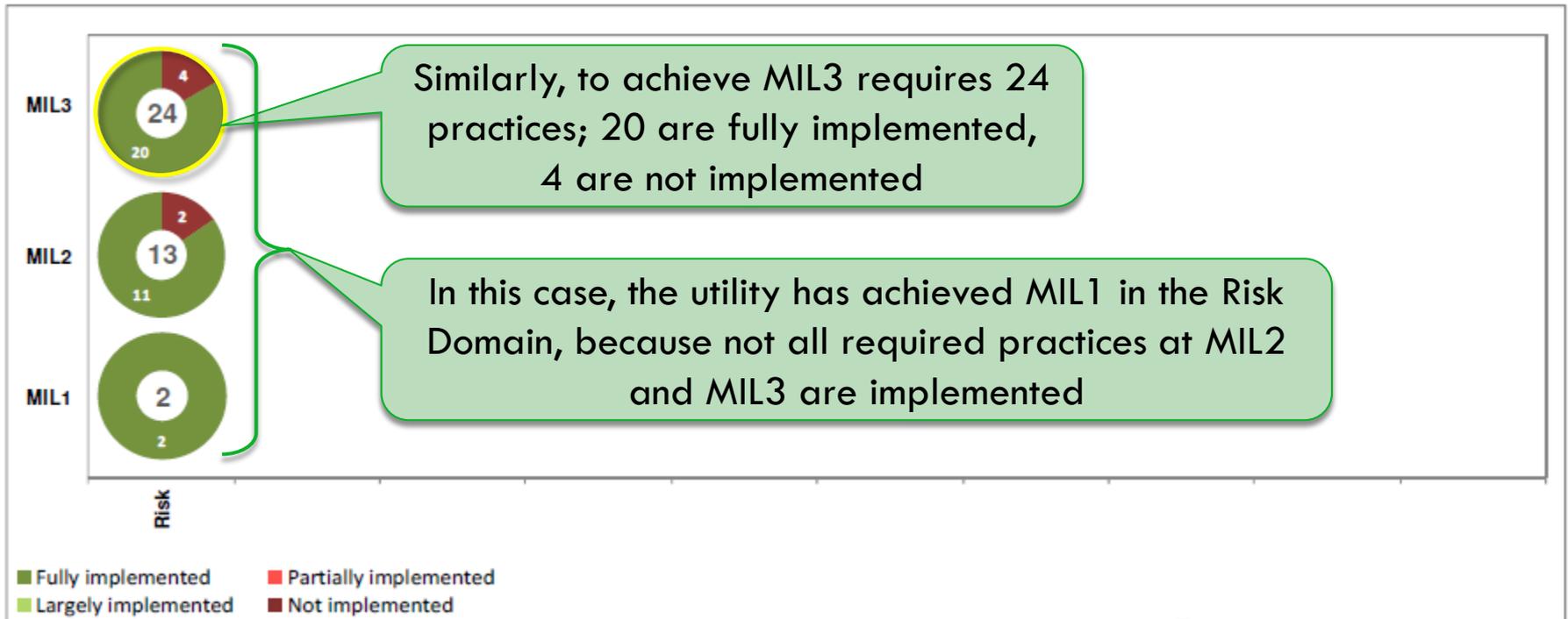
Sample Summary Score

14



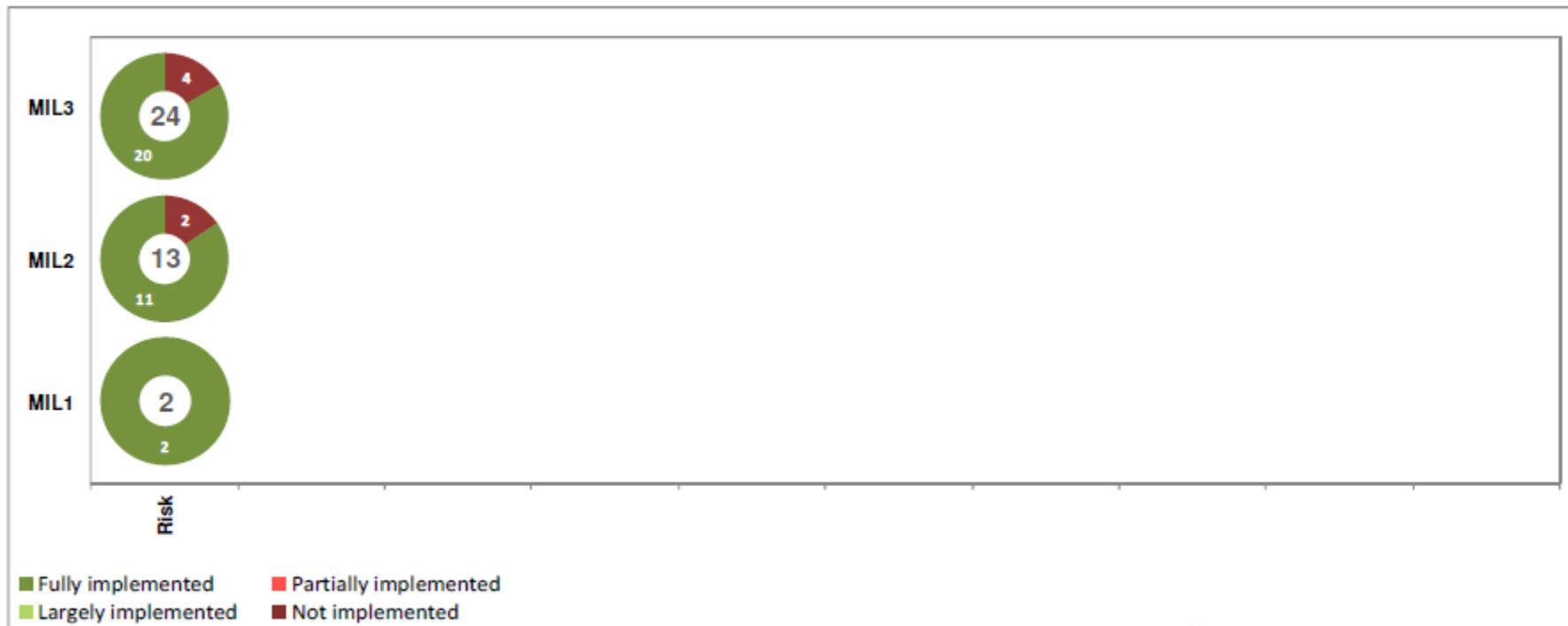
Sample Summary Score

15



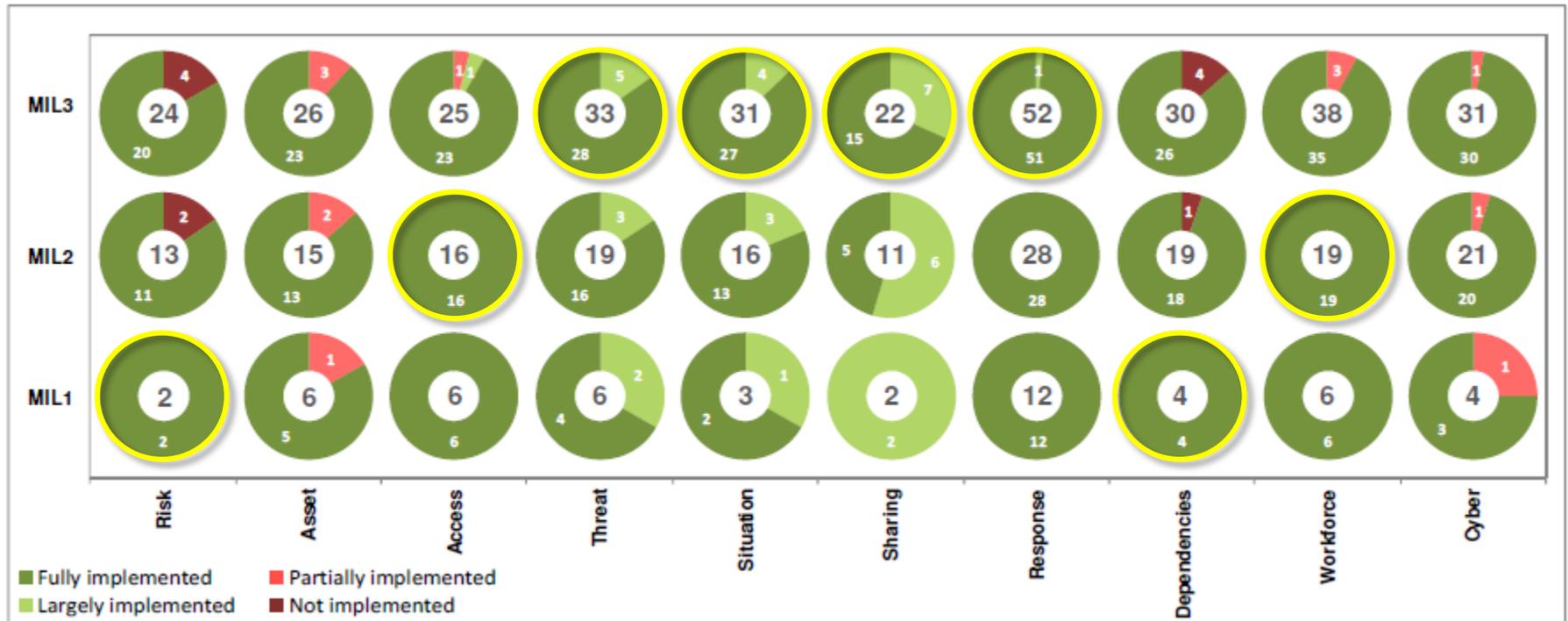
Sample Summary Score

16



Sample Summary Score

17



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

Sample Domain Data

18

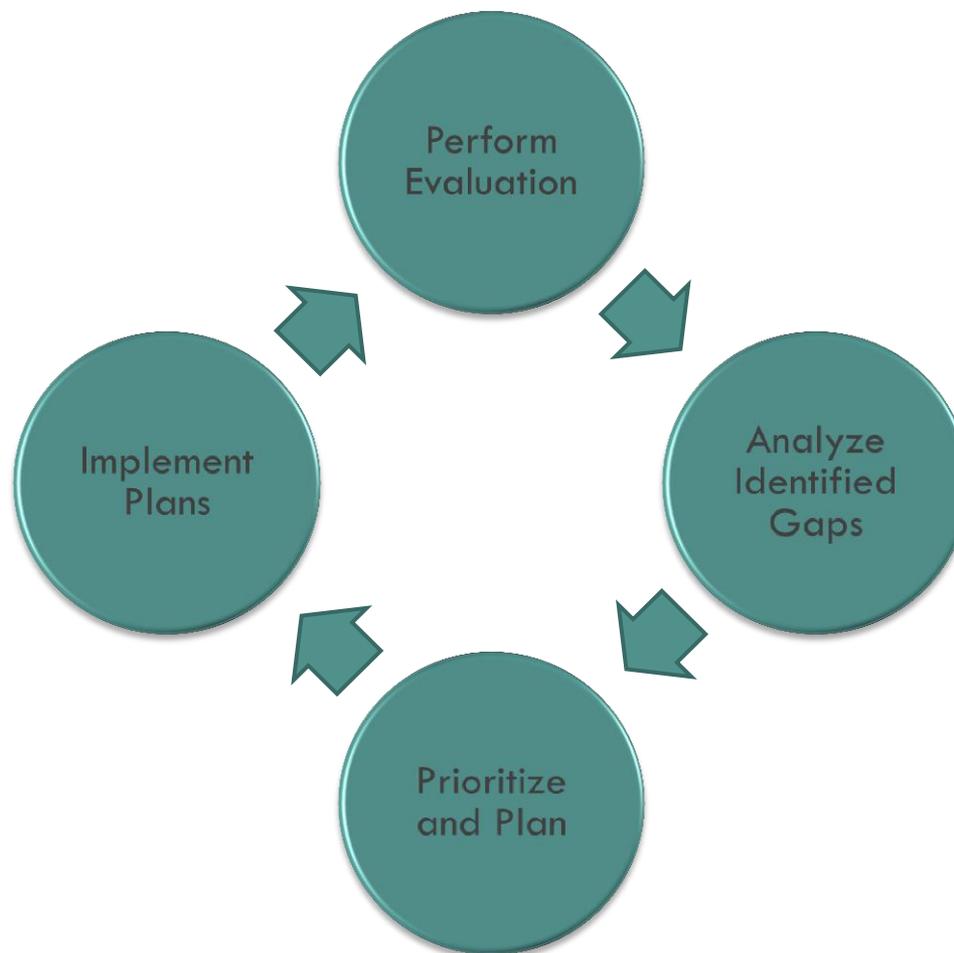


1. Establish Cybersecurity Risk Management Strategy

MIL1	<i>No practice at MIL1</i>	
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

Using the model

19



Links and Contact Info

20

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

Matt Light

Program Mgr, DOE

matthew.light@hq.doe.gov

Dave White

Tech Mgr, SEI/CERT

dwhite@cert.org

CSWG Privacy Subgroup Current Activities

Rebecca Herold

CSWG Privacy Subgroup Lead

rebeccaherold@rebeccaherold.com

CSWG Privacy Subgroup

- Formed in June, 2009
- Close to 100 volunteer members from wide range of organizations
- Very busy since the publication of NISTIR 7628 in September 2010
- Meets bi-weekly, occasionally with guest speakers
- Over 10 sub-teams making additional work products since September 2010
- Finished draft update; NISTIR 7628 Vol 2 version 2

CSWG Privacy Subgroup Work (1/7)

Smart Grid Privacy Training & Awareness Team

- This team created multiple sets of “train the trainer” slides, with an abundance of speaker notes, to help those who provide training within the many smart grid related entities to understand privacy implications of the smart grid and what to use for possible training tools.
- The first set completed is for use by utilities. The second set for use by PUCs. The third set is for organizations to provide to consumers. The fourth set is for third parties.

CSWG Privacy Subgroup Work (2/7)

Third Party CEUD Privacy Protection Team

1. Third Party Privacy Recommendations
 - a) Established data protection categories and mapped to California rules, ASAP-SG, and Fair Information Privacy Practices (FIPPS) to determine sampling of current guidance.
 - b) Recommendations for protecting privacy whenever any type of third party entity (e.g., vendors who work directly with consumers) collects, uses or otherwise accesses CEUD .
2. Mapped the NAESB Third Party Data Sharing recommendations to the NISTIR 7628 Volume 2 recommendations from 2010.

CSWG Privacy Subgroup Work (3/7)

Privacy Use Cases Team

- Throughout 2011 a 3-person team worked on incorporating privacy considerations and checks into the use cases that were published in NISTIR 7628.
- At end of 2011 sent the updated use cases (151 pages) to the full NIST privacy group.
- Throughout 2012 a larger group incorporated the feedback into the use cases.
- Final version will be included in 2nd version of NISTIR 7628 as well as provided to other organizations to distribute.

CSWG Privacy Subgroup Work (4/7)

Plug-in Electric Vehicle (PEV) Team

- Had little activity until November
- Including some preliminary information into next version with contributions from PEV and privacy technology experts
- Depending on SGIP 2.0, hope to increase the work in this area for the next version

CSWG Privacy Subgroup Work (5/7)

NSTIC Team

- Started late in 2010 at request of then Department of Commerce Secretary to determine what, if any, impact NSTIC will have upon the smart grid.
- Providing a section discussing privacy impact to the smart grid based upon NSTIC guidance published so far.

CSWG Privacy Subgroup Work (6/7)

Updated the Legal Discussions Section

- Based on new laws since 2010
- Based on court actions since 2010
- Not legal opinion, but merely discussion for which entities involved in the smart grid should be aware

CSWG Privacy Subgroup Work (7/7)

Emerging Smart Grid Privacy Risks

- Identified 15 areas to keep an eye on for potential smart grid privacy risks.
- Including overview discussions in NISTIR 7628 Volume 2 version 2.

CSWG Privacy Subgroup

Next meeting:

- Friday, December 21, 11am Eastern
- Guest speaker: Roger Levy
Currently leading the Lawrence Berkeley National Laboratory assessment of the smart meter HAN, including privacy issues.
- Dial-in information:
Telecon number: 866-793-6322 (203-277-9670 toll version)
Participant code: 3836162

CSWG Privacy Subgroup

To Join Group (until SGIP 2.0) Send Email To

- Rebecca Herold, Subgroup Leader:
rebeccaherold@rebeccaherold.com
- Tanya Brewer, NIST sponsor/representative:
tanya.brewer@nist.gov

SGIP 2.0 Briefing and Q&A

Mike Coop/George Bjelovuk

Grid-Interop



TM

WINTER 2012 FACE-TO-FACE
IRVING, TEXAS

SGiP