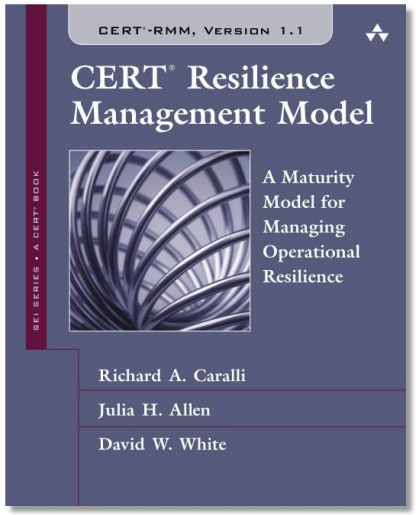
Department of Homeland Security Cyber Resilience Review (Case Study)

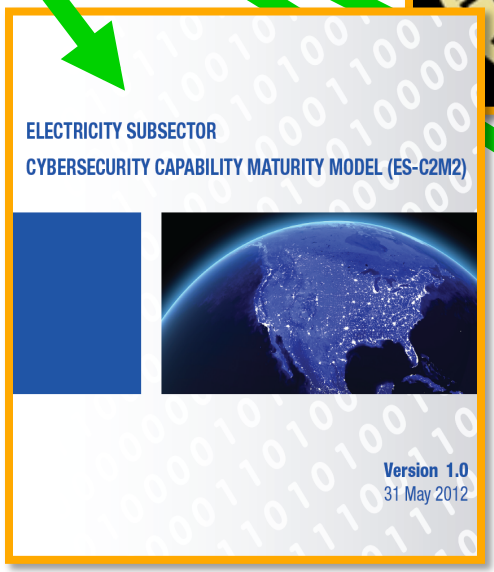
Matthew Butkovic
Technical Manager - Cybersecurity Assurance, CERT® Division

Matthew Butkovic is a Technical Manager – Cybersecurity Assurance in the CERT Program at the Software Engineering Institute (SEI). Butkovic performs critical infrastructure protection research and develops methods, tools, and techniques for managing risk.

Butkovic has more than 15 years of managerial and technical experience in information technology (particularly information systems security, process design and audit) across the banking and manufacturing sectors. Prior to joining CERT in 2010, Butkovic was leading information security and business continuity efforts for a Fortune 500 manufacturing organization. Butkovic is a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA).

A Sampling of CERT® Resilience Management Model Applications and Derivatives





Overview

What is the Cyber Resilience Review (CRR)?

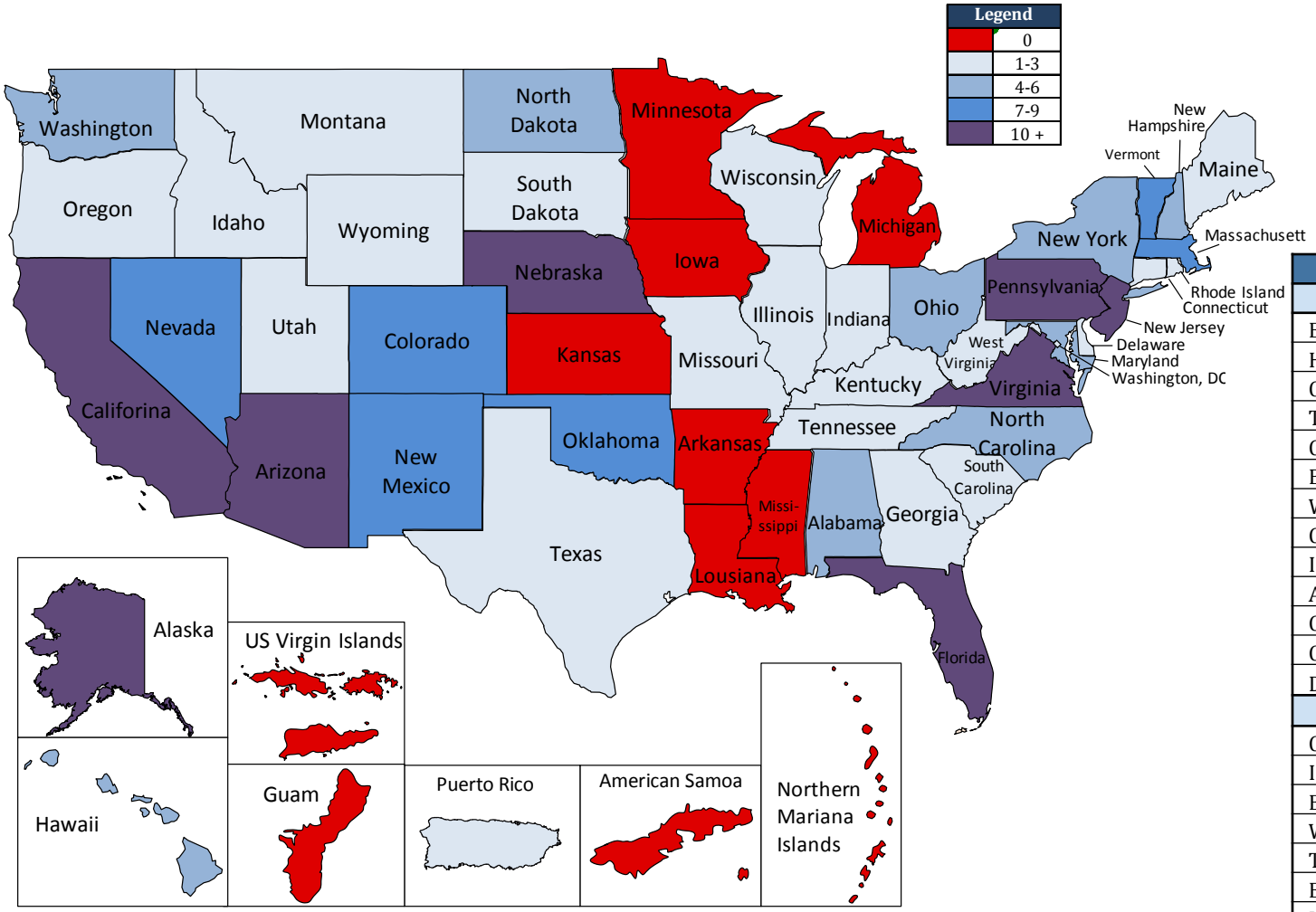
- Examines cybersecurity practices in critical infrastructure organizations
- Is conducted in partnership with the U.S. Department of Homeland Security
- Evaluates the resilience of critical services
- Utilizes the goals and practices found in the CERT Resilience Management Model (CERT-RMM)
- Is completely voluntary and protected by PCII
- Is a one-day expert-facilitated workshop (typically 6–8 hours)
- Provides participants with a detailed report containing suggestions for improvement
- Collects data for the purpose of analyzing aggregated (non-attributable) results

CRR Benefits Participating Organizations

How the CRR helps organizations improve cyber resilience

- Identify their cybersecurity posture
- Develop a shared cyber resilience vision and roadmap
- Learn where to get help and information about cyber resilience
- Communicate using a common language
- Prioritize options and support decision making
- Measure their progress in improving cyber resilience
- Prepare for and facilitate change

CRR Assessment *(v1 and v2) summary*



Sector	Count
CIKR (Private)	128
Energy	31
Healthcare and Public Health	23
Commercial Facilities	13
Transportation Systems	12
Government Facilities	11
Banking and Finance	11
Water	10
Critical Manufacturing	6
Information Technology	5
Agriculture and Food	3
Chemical	1
Communications	1
Dams	1
CIKR (SLTT)	140
Government Facilities	31
Information Technology	30
Emergency Services	27
Water	24
Transportation Systems	20
Energy	5
Healthcare and Public Health	2
Banking and Finance	1
Grand Total	**268**

Between FY 2009 and present (as of 11/25/2013) CSEP conducted 268 CRRs.

CRR Data Analysis: Selected Highlights

Summary Findings (115 organizations, 43 states, 12 sectors)

Asset Management: More than 70% of organizations identify critical services; however, less than 50% of organizations assessed have identified the assets that support critical services.

Vulnerability Management: More than 55% of organizations have not developed a strategy to guide their vulnerability management efforts.

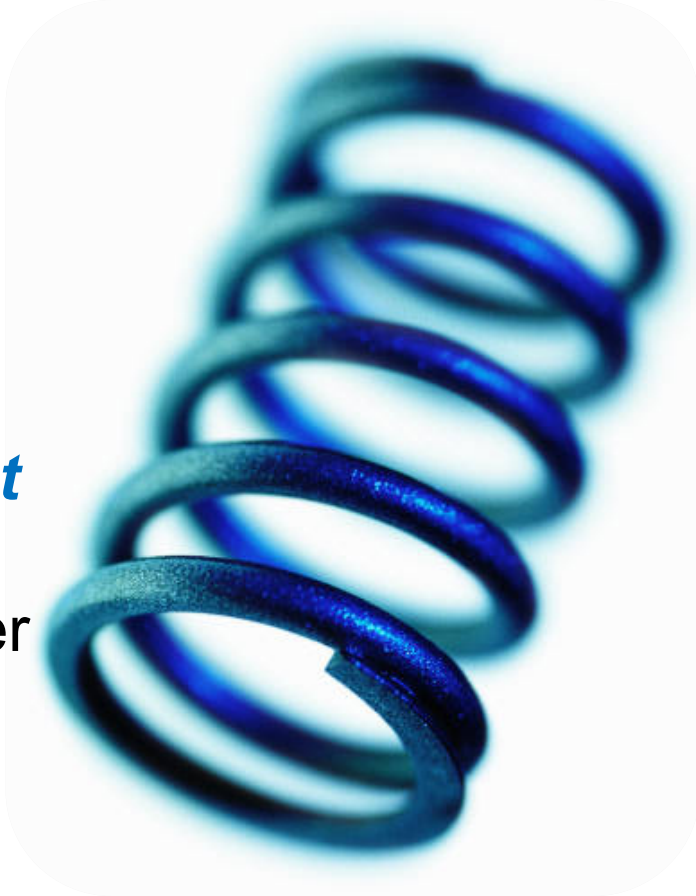
Incident Management: 65% of organizations lack a process to escalate and resolve incidents.

External Dependencies Management: More than 80% of the organizations assessed identify external dependencies that are vital to the delivery of critical services.

Operational Resilience Defined

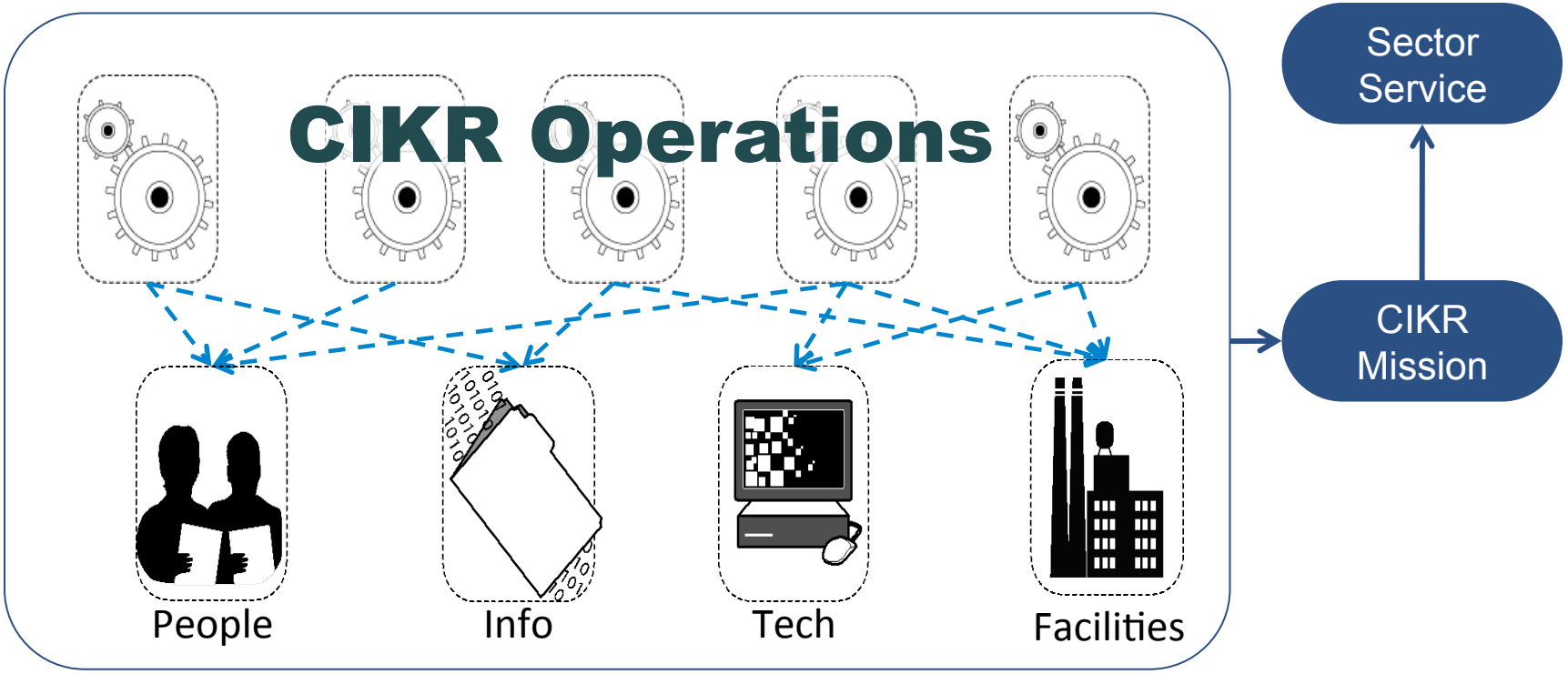
Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]

Operational resilience: The ***emergent*** property of an ***organization*** that can ***continue to carry out its mission*** after ***disruption*** that ***does not exceed*** its ***operational*** limit [CERT-RMM]

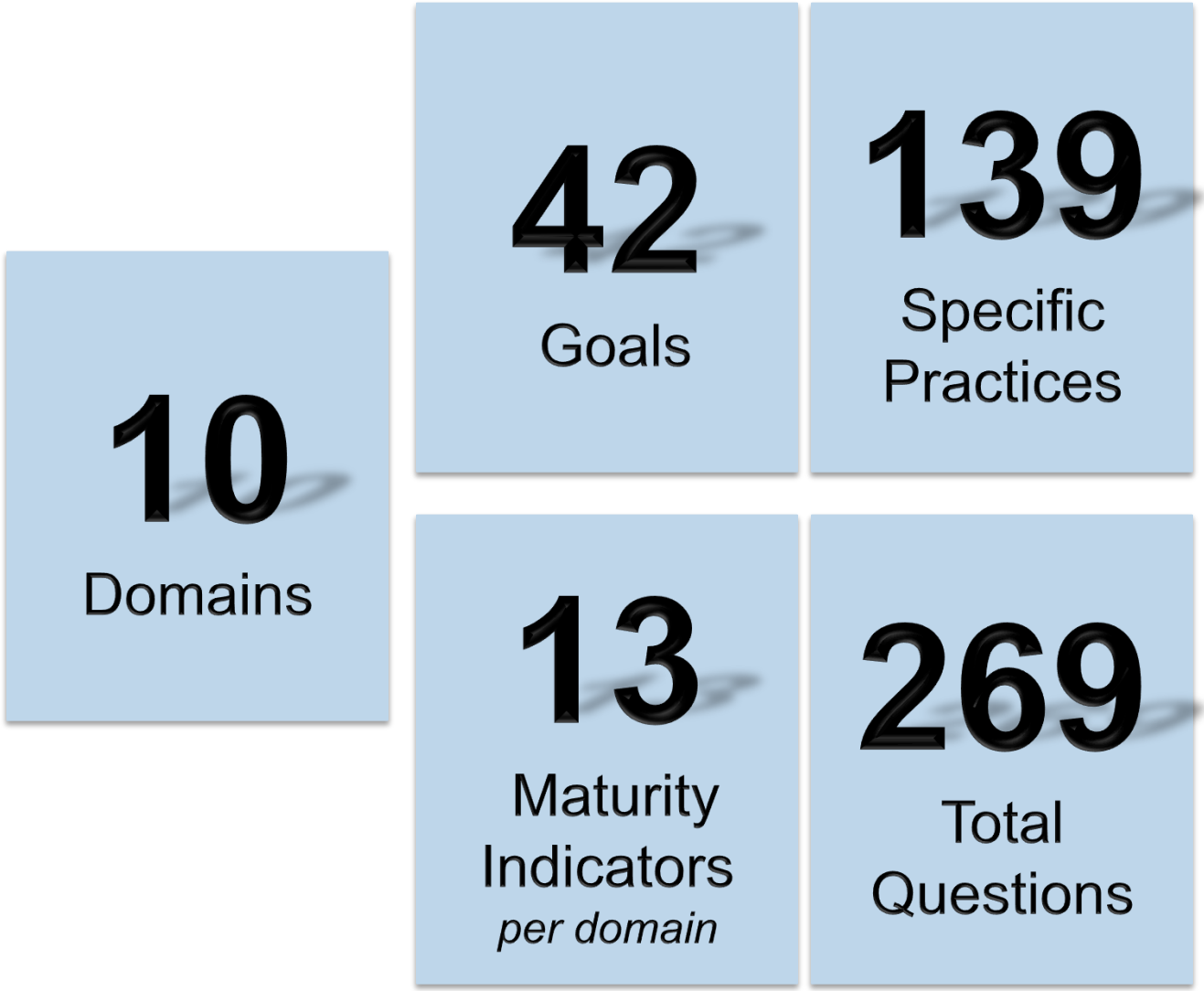


Where does the **disruption** come from? Realized risk.

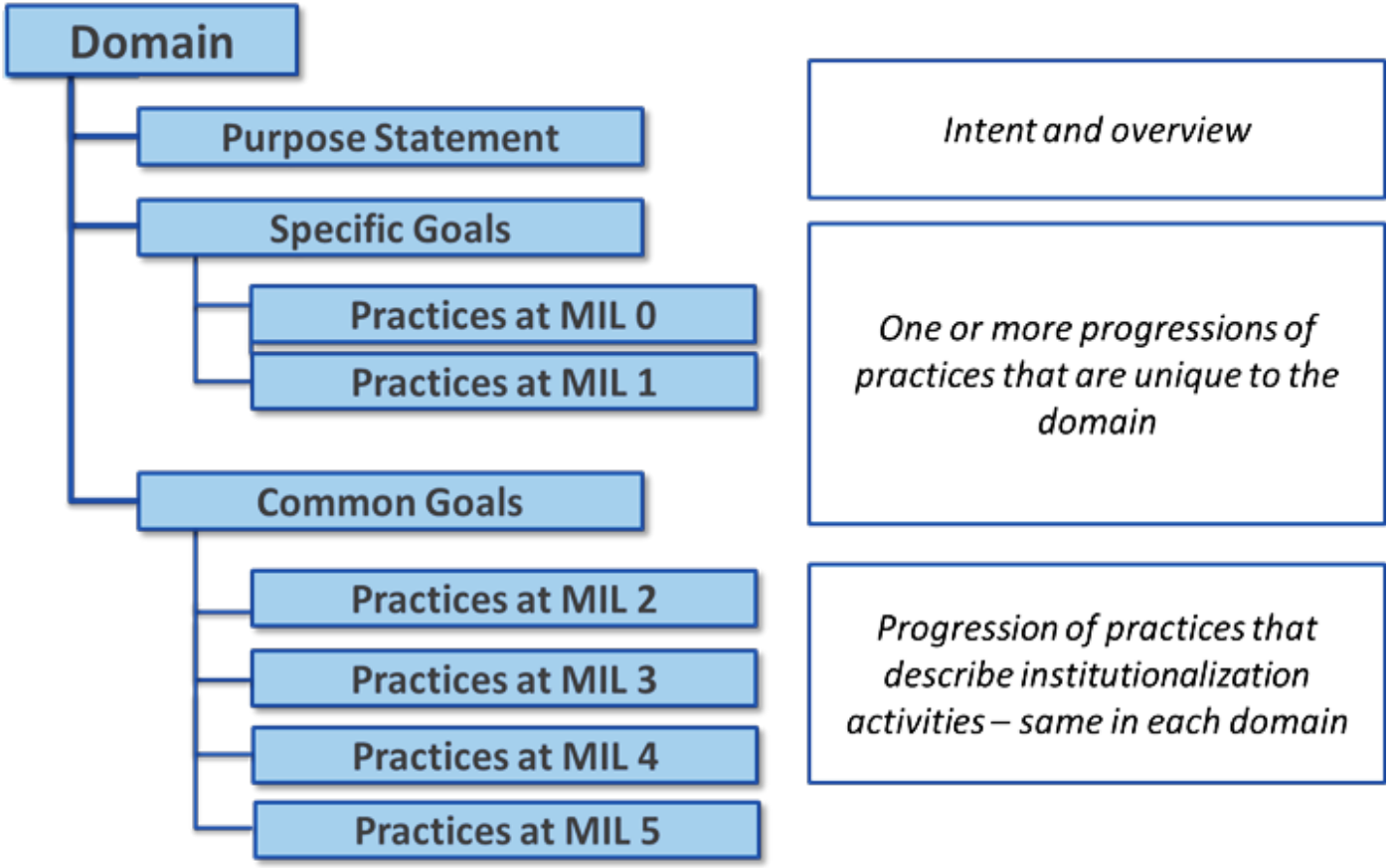
Establishing a Critical Service Focus



Cyber Resilience Review by the Numbers



Domain Structure



Process Institutionalization in the CRR

Maturity indictor levels (MIL) are used in CRR v2 to measure process institutionalization

Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete

Level 5-Defined

Level 4-Measured

Level 3-Managed

Level 2-Planned

Level 1-Performed

Level 0-Incomplete

Higher degrees of institutionalization translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

Ten Domains of Cybersecurity Capability

The ten domains in CRR v2 represent important areas that contribute to the cyber resilience of an organization.

The domains focus on practices that an organization should have in place to assure the protection and sustainment of its critical service.

CRR Domains	
AM	Asset Management
CCM	Configuration and Change Management
RM	Risk Management
CTRL	Controls Management
VM	Vulnerability Management
IM	Incident Management
SCM	Service Continuity Management
EXD	External Dependencies Management
TA	Training and Awareness
SA	Situational Awareness

Domain Details

CRR Domain	Number of Goals	Number of Goal Practices	Number of MIL Practices
Asset Management	7	24	13
Controls Management	4	7	13
Configuration and Change Management	3	15	13
Vulnerability Management	4	12	13
Incident Management	5	23	13
Service Continuity Management	4	15	13
Risk Management	5	13	13
External Dependencies Management	5	14	13
Training and Awareness	2	8	13
Situational Awareness	3	8	13

Model Domains (1–2 of 10)

Domain	Description
Asset Management (AM)	The purpose of Asset Management is to identify, document, and manage organizational assets during their life cycle to ensure sustained productivity to support the critical service. Asset Management includes activities that an organization conducts to deploy its people, information, technology, and facilities that support critical services. This section focuses on whether the organization inventories its high-value assets and how it maintains asset-to-service traceability. This traceability is important as it serves as a basis for understanding cybersecurity requirements for assets.
Configuration and Change Management (CCM)	The purpose of Change and Configuration Management is to establish processes to maintain the integrity of all assets (technology, information, and facilities) required for delivery of the critical service. Configuration and Change Management focuses on how the organization manages asset configurations, and how the organization ensures that it remains in control of changes to these assets. With particular attention paid to technology assets, Configuration and Change Management also investigates whether the traceability established in Asset Management benefits the organization as it manages changes.

Model Domains (3–4 of 10)

Domain	Description
Risk Management (RM)	The purpose of Risk Management is to identify, analyze, and mitigate risks to organizational assets that could adversely affect the operation and delivery of services. It has six goals: prepare for risk management, establish risk parameters and focus, identify risk, analyze risk, mitigate and control risk, and use risk information to manage resilience. Risk Management examines how the organization identifies, analyzes, and mitigates cybersecurity risk. This domain includes discussions about how the organization performs cybersecurity risk assessments, how it makes decisions about cybersecurity risk, and how the organization benefits from an active cybersecurity risk management program.
Controls Management (CTRL)	The purpose of Controls Management is to establish, monitor, analyze, and manage an internal control system that ensures the effectiveness and efficiency of operations through assuring mission success of high-value services and the assets that support them. It has four specific goals: establish control objectives, establish controls that support control objectives, analyze controls to ensure they satisfy control objectives, and assess control effectiveness.

Model Domains (5–6 of 10)

Domain	Description
Vulnerability Management (VM)	The purpose of Vulnerability Management is to identify, analyze, and manage vulnerabilities in the assets that support delivery of the critical service. Vulnerability Management involves practices that identify and resolve weaknesses in assets that may affect critical services. Practices discussed include the discovery of vulnerabilities, how the organization manages exposure to vulnerabilities, and how the organization works to ensure that the root cause of vulnerabilities is discovered.
Incident Management (IM)	The purpose of Incident Management and Control is to establish processes to identify and analyze events, detect incidents, and determine and implement an appropriate organizational response. Incident Management examines how the organization identifies and responds to cyber-security incidents that affect the critical service. It has five goals: establish the incident management and control process, detect events, declare incidents, respond to and recover from incidents, and establish incident learning.

Model Domains (7–8 of 10)

Domain	Description
Service Continuity Management (SCM)	Service Continuity Management examines how the organization conducts contingency planning for the continuity of the critical service. Activities discussed include how plans are developed, tested, and maintained in order to ensure that they are realistic and actionable during times of operational stress.
External Dependencies Management (EXD)	External Dependencies Management focuses on establishing and managing an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities. Outsourcing services, development, production, and even asset management have become normal and routine operational elements for many organizations. Increasingly, organizations are also exposing technology systems, information, and other high-value assets to customers to enable the seamless and efficient flow of business processes. This domain focuses on how the organization identifies these dependencies and manages risk to the critical service that arises from the failure of these relationships.

Model Domains (9–10 of 10)

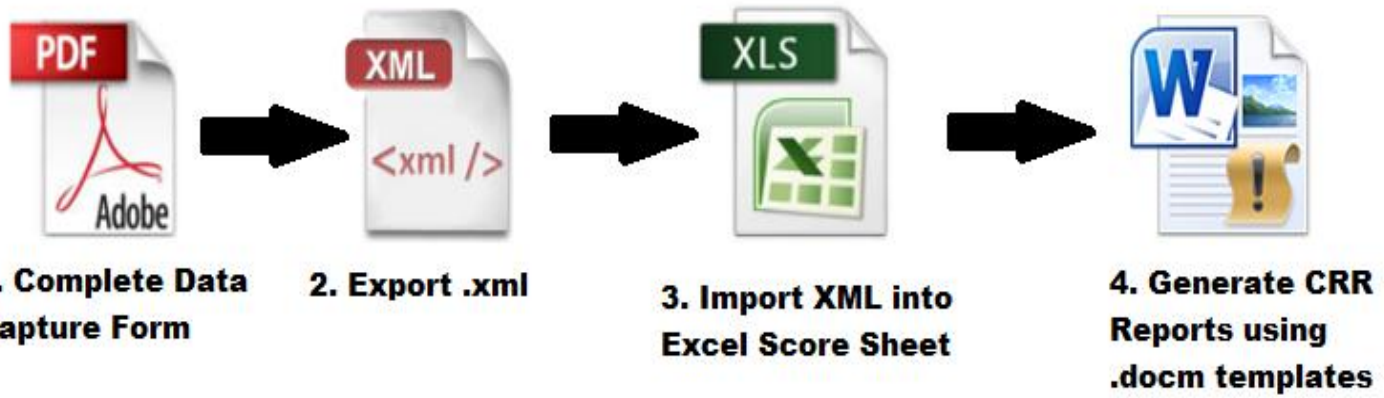
Domain	Description
Training and Awareness (TA)	The purpose of Training and Awareness is to promote awareness in and develop skills and knowledge of people in support of their roles in attaining and sustaining operational resilience. It focuses exclusively on skills, knowledge, and cognizance for resilience activities, not generalized training across the organization. However, these resilience training and awareness activities should integrate with and be supported by the organization's overall training and awareness program and plan. Training and Awareness involves examining how the organization manages cybersecurity education of its employees that support the critical service. In this context, *training* is the development of new skills, and *awareness* involves the dissemination of current cyber-security information. Activities reviewed include how the organization identifies training and awareness needs and works to ensure that it meets those needs reliably.
Situational Awareness (SA)	The purpose of Situational Awareness is to actively discover and analyze information related to immediate operational stability and security and the coordination of such information across the enterprise to ensure that all organizational units are performing under a common operating picture. Activities examined include how the organization maintains operational stability and cyber-security via a common operating picture, and whether or not the organization has identified prudent and practical steps it might take to reduce its attack surface, safeguarding the critical service.

3-Point Answer Scale

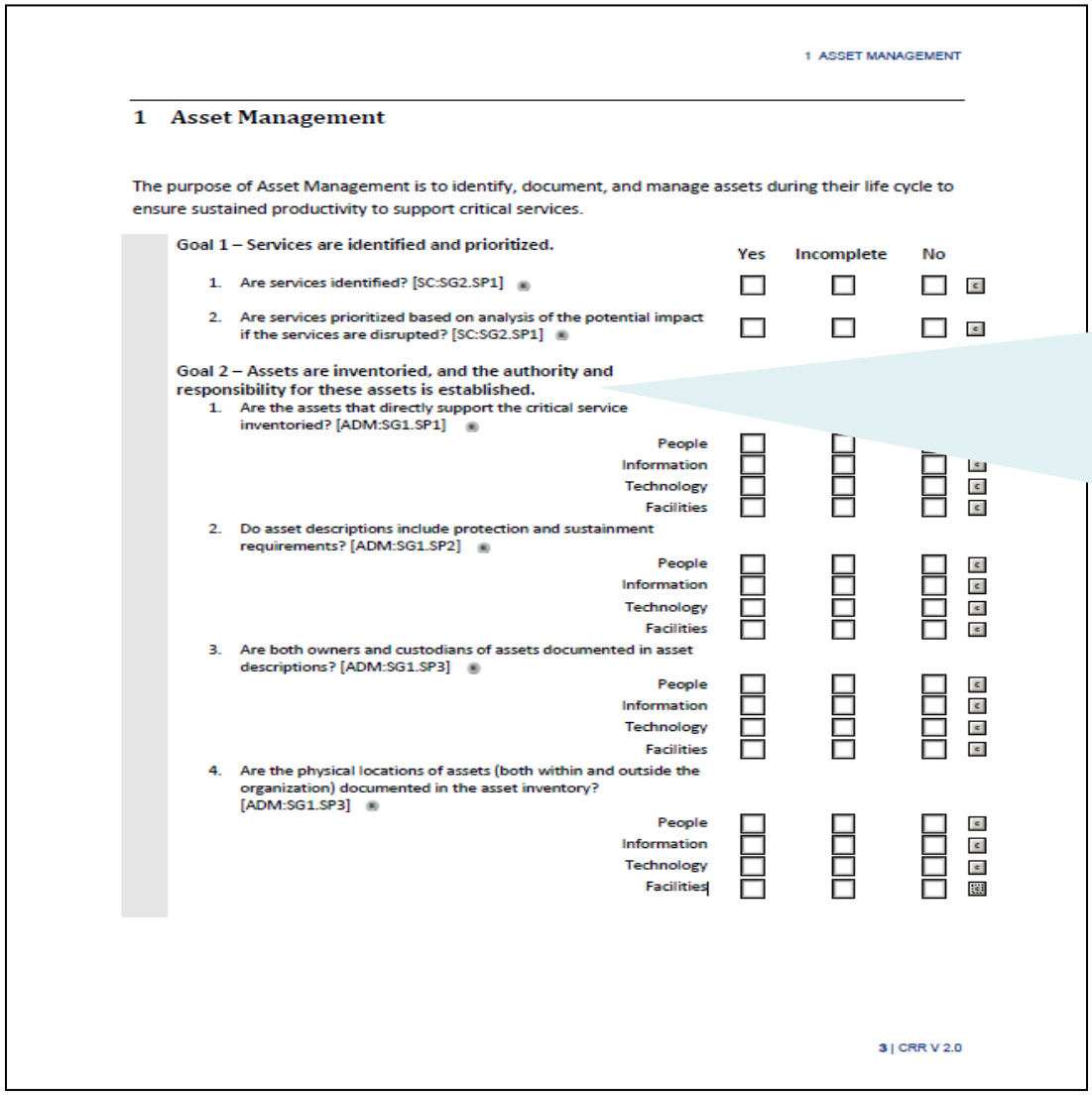
3-point answer scale	The organization's performance of the practice described in the model is …
Yes	Complete
Incomplete	Incomplete; there are multiple opportunities for improvement
No	Absent; the practice is not performed in the organization

CRR Analysis and Report Generation Overview

The analysis and report generation is performed in four steps. The first step is completed in the CRR workshop.



CRR Data Capture Form - 1



1 ASSET MANAGEMENT

1 Asset Management

The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.

Goal 1 – Services are identified and prioritized.

	Yes	Incomplete	No
1. Are services identified? [SC:SG2.SP1]	☐	☐	☐
2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	☐	☐	☐

Goal 2 – Assets are inventoried, and the authority and responsibility for these assets is established.

	Yes	Incomplete	No
1. Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]			
People	☐	☐	☐
Information	☐	☐	☐
Technology	☐	☐	☐
Facilities	☐	☐	☐
2. Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]			
People	☐	☐	☐
Information	☐	☐	☐
Technology	☐	☐	☐
Facilities	☐	☐	☐
3. Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]			
People	☐	☐	☐
Information	☐	☐	☐
Technology	☐	☐	☐
Facilities	☐	☐	☐
4. Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]			
People	☐	☐	☐
Information	☐	☐	☐
Technology	☐	☐	☐
Facilities	☐	☐	☐

3 | CRR V 2.0

Guidance for Questions

Consideration of the consequences of the loss of high-value organizational services is typically performed as part of a business impact analysis. In addition, the consequences of risks to high-value services are identified and analyzed in risk assessment activities. The organization must consider this information when prioritizing high-value services.

Typical work products:

1. Prioritized list of organization's services, activities, and associated assets
2. Results of security risk assessment and business impact analyses

A "yes" answer means that the services documented in AM1-1 include a priority, or that there is a separate repository of information that prioritizes services based on their potential impact of disruption.

CRR Data Capture Form - 2

Each domain concludes with Maturity Indicator Level (MIL) questions

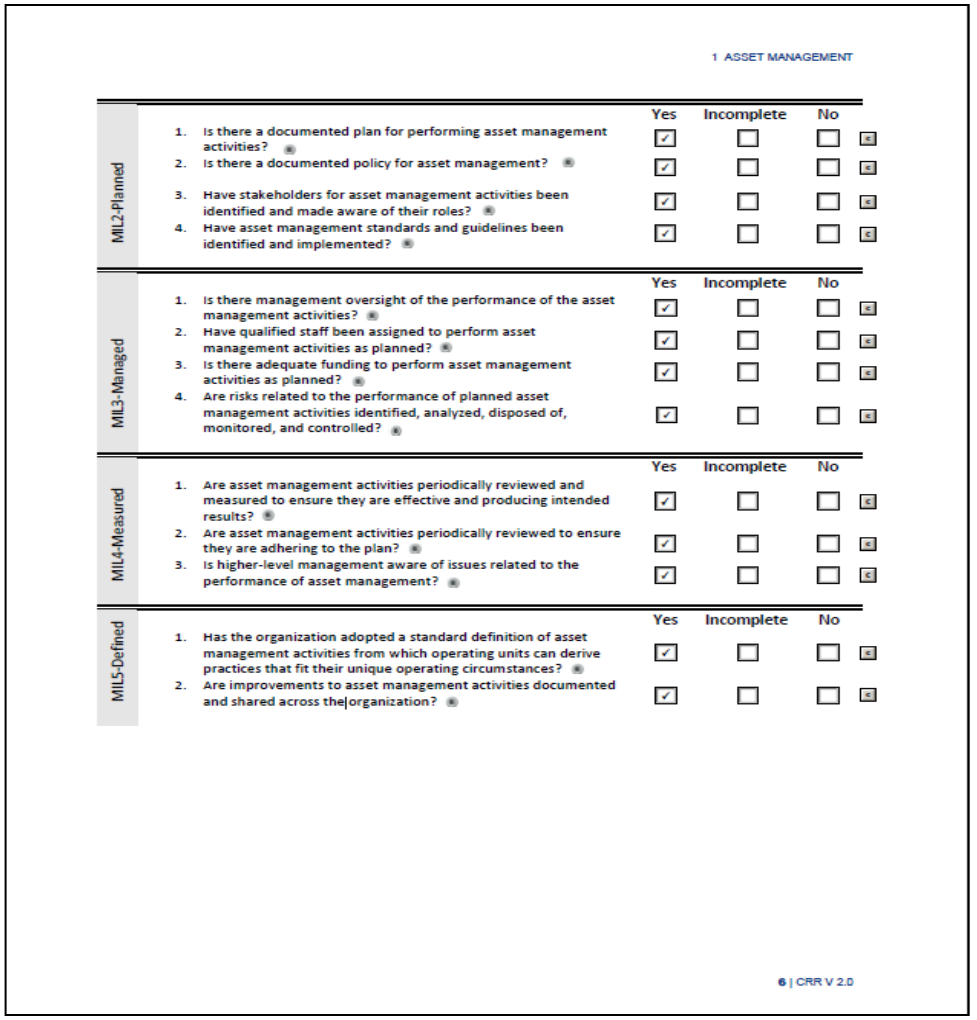
MIL 1 = *Performed*

MIL 2 = *Planned*

MIL 3 = *Managed*

MIL 4 = *Measured*

MIL 5 = *Defined*



1 ASSET MANAGEMENT

MIL2-Planned

	Yes	Incomplete	No
1. Is there a documented plan for performing asset management activities?	☑	☐	☐
2. Is there a documented policy for asset management?	☑	☐	☐
3. Have stakeholders for asset management activities been identified and made aware of their roles?	☑	☐	☐
4. Have asset management standards and guidelines been identified and implemented?	☑	☐	☐

MIL3-Managed

	Yes	Incomplete	No
1. Is there management oversight of the performance of the asset management activities?	☑	☐	☐
2. Have qualified staff been assigned to perform asset management activities as planned?	☑	☐	☐
3. Is there adequate funding to perform asset management activities as planned?	☑	☐	☐
4. Are risks related to the performance of planned asset management activities identified, analyzed, disposed of, monitored, and controlled?	☑	☐	☐

MIL4-Measured

	Yes	Incomplete	No
1. Are asset management activities periodically reviewed and measured to ensure they are effective and producing intended results?	☑	☐	☐
2. Are asset management activities periodically reviewed to ensure they are adhering to the plan?	☑	☐	☐
3. Is higher-level management aware of issues related to the performance of asset management?	☑	☐	☐

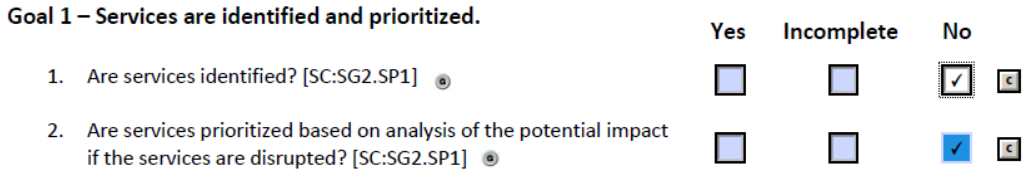
MIL5-Defined

	Yes	Incomplete	No
1. Has the organization adopted a standard definition of asset management activities from which operating units can derive practices that fit their unique operating circumstances?	☑	☐	☐
2. Are improvements to asset management activities documented and shared across the organization?	☑	☐	☐

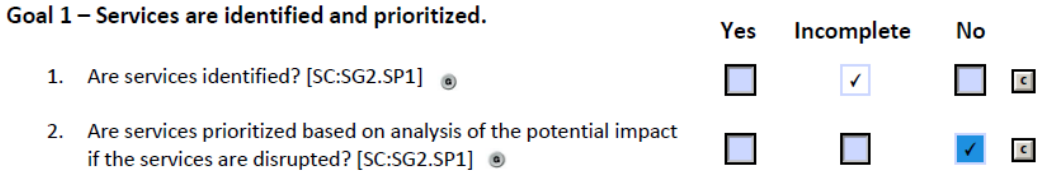
6 | CRR V 2.0

CRR Data Capture Form - 3

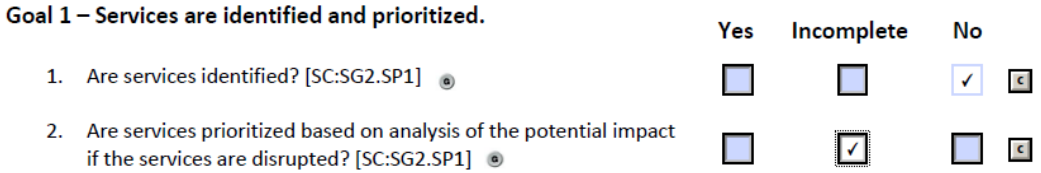
When there is a “No” answer to a question that has linked dependent questions, the answer shows in both questions, with the dependent question highlighted in blue as shown below.



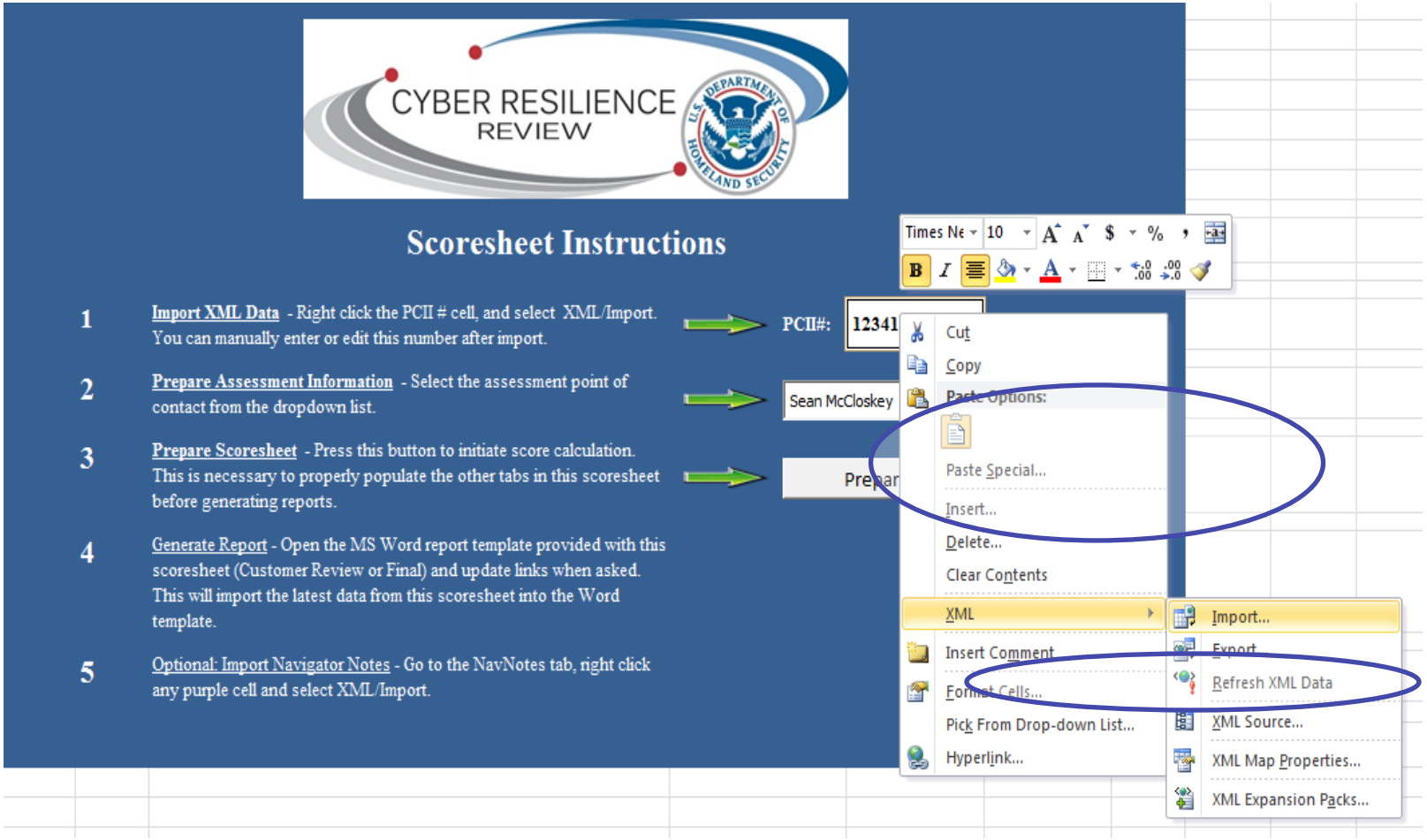
If the answer to the original question is changed, the dependent question remains unchanged.



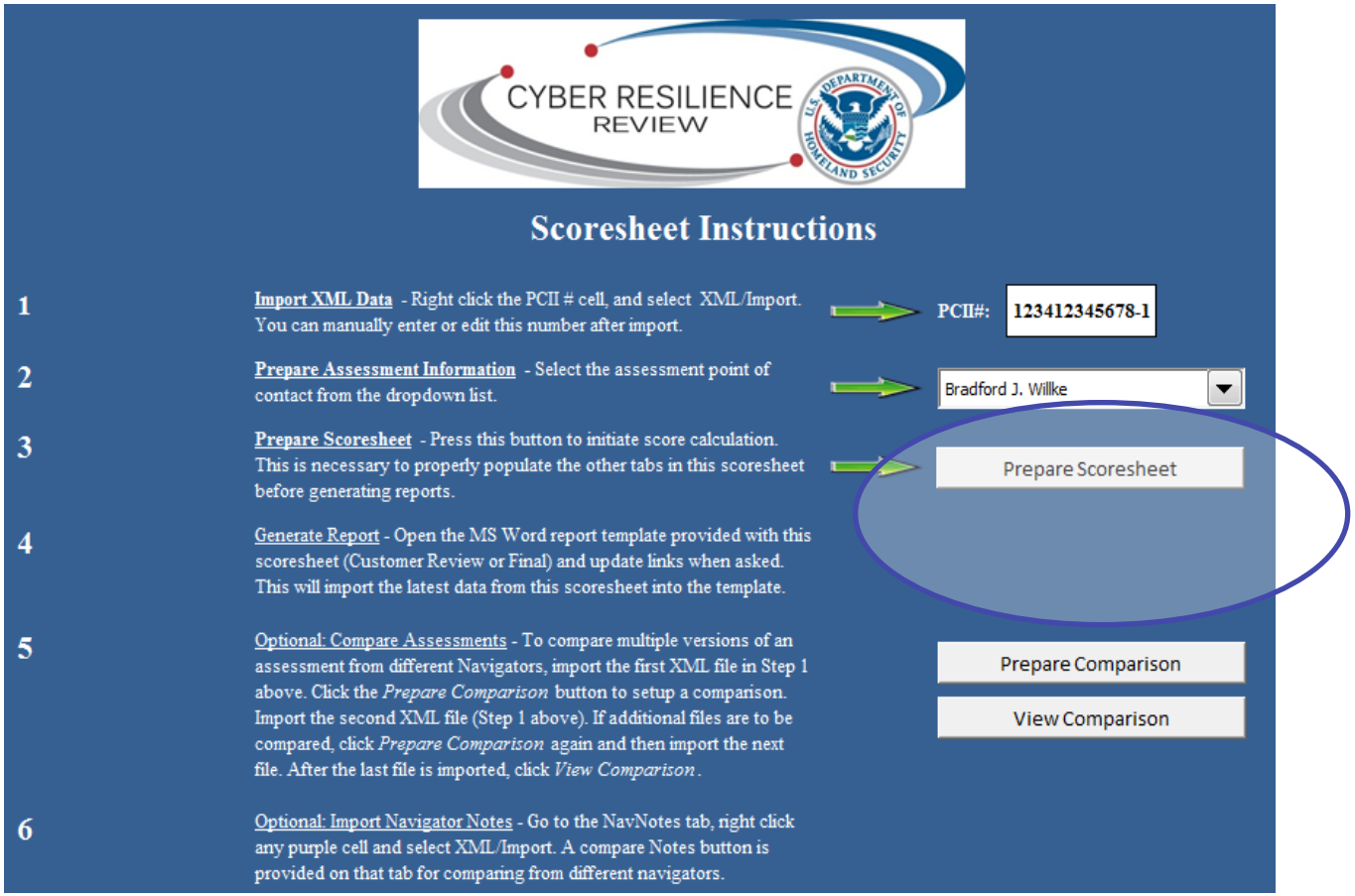
If the answer to the dependent question is changed, the highlighting is removed and the new answer appears. You may need to revisit the first question.



Data is imported from the capture form



Reports are generated



Basic CRR Scoring Information

1. Practices are either “Yes” (Performed), “Incomplete” (Incompletely Performed), or “No” (Not Performed).
2. MIL questions are either “Yes” (Performed), “Incomplete” (Incompletely Performed), or “No” (Not Performed).
3. A goal is “Achieved” only if all practices are performed.
   - Practices must be performed for a goal to be “Achieved.”
4. A domain is scored at MIL 1 if all of the goals in the domain are achieved.
5. Scores for MILs 2–5 apply only to those practices that are performed (are awarded a “Yes” answer).

The CRR Scoring Rubric

Step 1: Score Each Practice Question

- A practice is scored as “Performed” when the practice question is answered with a “Yes.”
- A practice is scored as “Not Performed” when the practice question is answered with an “Incomplete” or a “No.”

Step 2: Score Each Domain Goal

- A goal is scored as “Achieved” when all practices are performed.
- A goal is “Partially Achieved” when some practices are performed.
- A goal is “Not Achieved” when no practices are performed.

Step 3: Score MIL Questions

- A MIL question is scored as “Performed” when the question is answered with a “Yes.”
- A MIL question is scored as “Not Performed” when the question is answered with an “Incomplete” or a “No.”

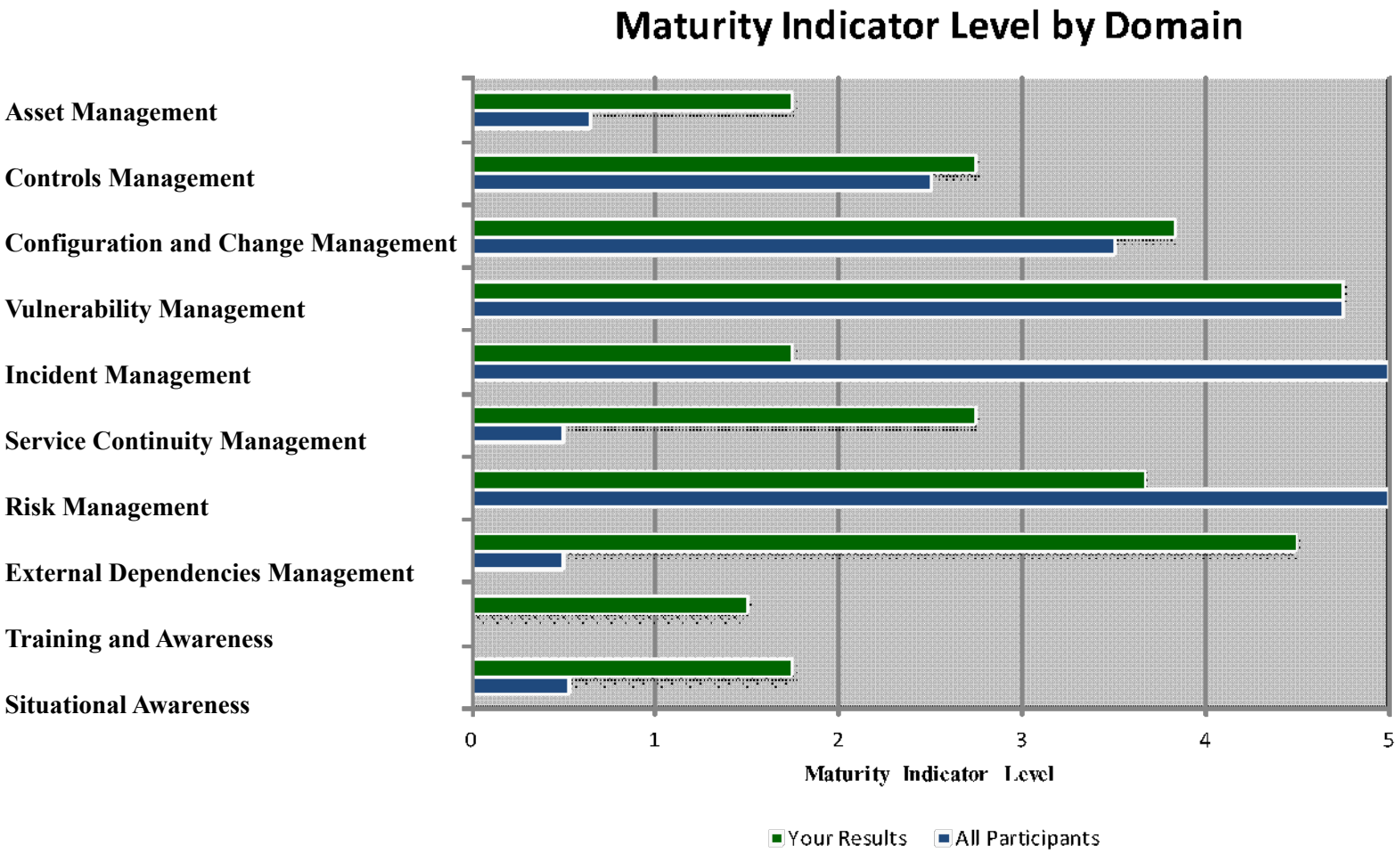
Report Example – Practice Detail and Options

Goal 2 – Assets are inventoried, and authority and responsibility for these assets is established.		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	No
	Information	Incomplete
	Technology	Yes
	Facilities	Yes
2.	Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]	
	People	No
	Information	No
	Technology	No
	Facilities	No
3.	Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]	
	People	No
	Information	No
	Technology	Incomplete
	Facilities	No
4.	Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]	
	People	No
	Information	No
	Technology	Yes
	Facilities	Yes
	Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[ADM:SG1.SP1]** Identify and inventory high-value assets. An organization must be able to identify its high-value assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to services. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems", Page 2-3	
Q2	**CERT-RMM Reference** **[ADM:SG1.SP2]** Update the asset database with asset profile information. All information relevant to the asset (collected from the asset profile) should be contained with the asset in its entry in the asset database. Strategies to protect and sustain an asset may be documented as part of the asset profile.	

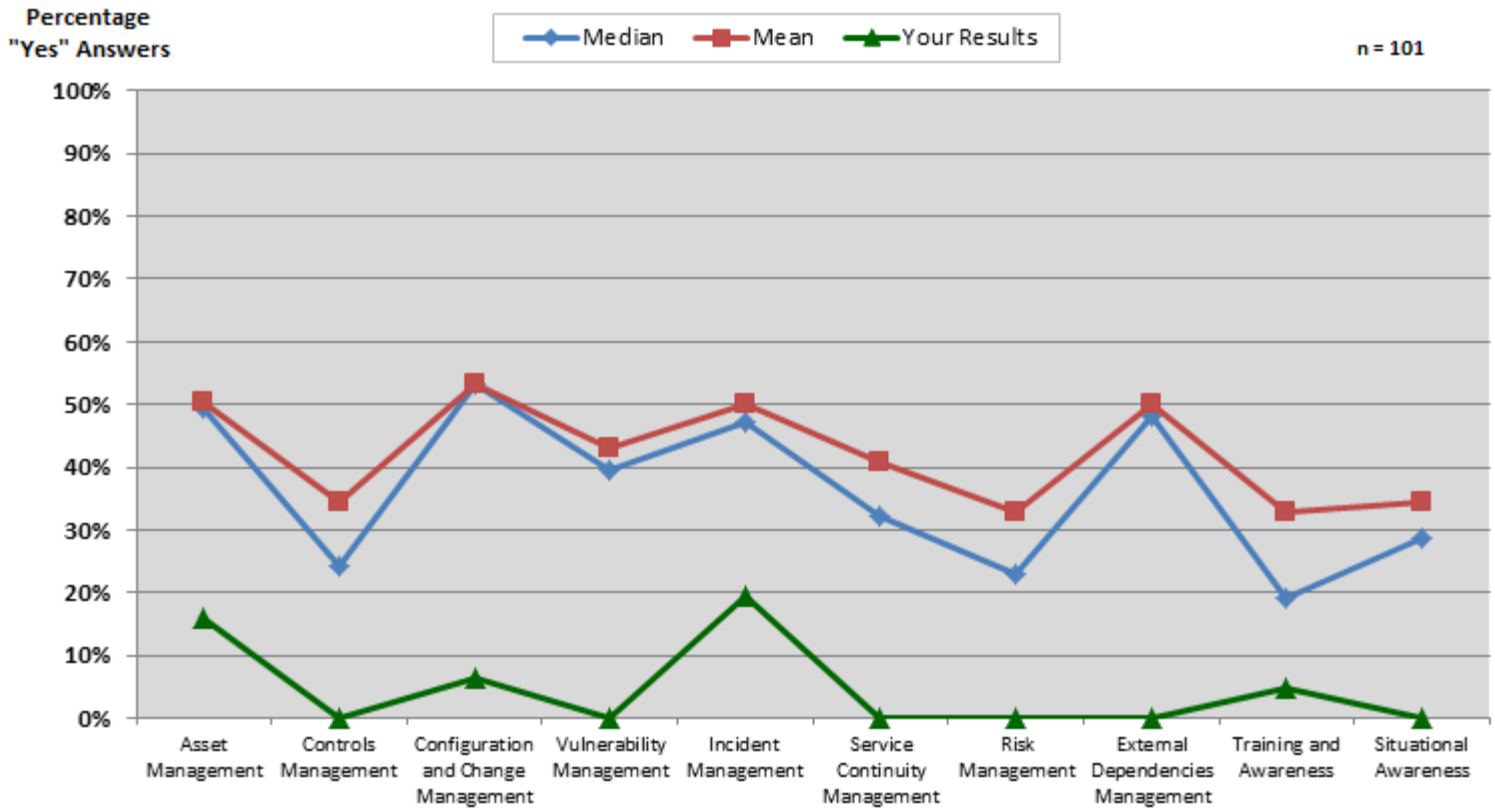
Report Example – Summary Heat Map

	MIL-1							MIL-2				MIL-3				MIL-4			MIL-5	
1 Asset Management	G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
2 Controls Management				G1	G2	G3	G4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
3 Configuration and Change Management					G1	G2	G3	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
4 Vulnerability Management				G1	G2	G3	G4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
5 Incident Management		G1	G2	G3	G4	G5		IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
6 Service Continuity Management				G1	G2	G3	G4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
7 Risk Management		G1	G2	G3	G4	G5		IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
8 External Dependencies Management		G1	G2	G3	G4	G5		IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
9 Training and Awareness					G1	G2		IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
10 Situational Awareness					G1	G2	G3	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

Report Example – MIL Scores



Report Example – Results Compared



Questions?

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0000506

SEI Training

Introduction to the CERT Resilience Management Model

February 18 - 20, 2014 (SEI, Arlington, VA)

June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document