Reference 55

University of Alaska
Office of Information Technology

Department of Homeland Security

Cyber Resilience Review

Report to the Board of Regents
June 2013

What is it?

Reference 55

- Voluntary program review
- Guided, Self-reporting
- Service oriented approach
- Helps with understanding & measurement
- Indicators of organizational resilience
- Ability to manage cyber risk (protection)
- Managing consequences of risk (sustaining)

Focus Areas

Reference 55

- People
- Information
- Technology
- Facilities

Reference 55

Cyber Resilience Review Domains

1. Asset Management (AM)
2. Configuration and Change Management (CCM)
3. Controls Management (CNTL)
4. Vulnerability Management (VM)
5. Incident Management (IM)
6. Service Continuity Management (SCM)
7. Risk Management (RISK)
8. External Dependencies Management (EXD)
9. Training and Awareness (TRNG)
10. Situational Awareness (SA)

Looks at current state of cyber security & addresses:

Reference 55

- **Documentation in place** and periodically reviewed and updated
- **Communication and notification** to all those who need to know
- **Implementation**, execution and analysis in a consistent, repeatable manner; and
- **Alignment** of goals and practices within and across domains

Maturity Level Indicators

Reference 55

CRR MATURITY INDICATOR LEVELS

- A Maturity Indicator Level (MIL) is assigned to each CRR domain and represents:
- A consolidated view of maturity in performing key area
- Measures the level of process institutionalization
- Describes attributes indicative of mature capabilities
- Higher degrees of institutionalization translate to more stable processes that produce consistent results over time and that are retained during times of operational stress.

However, it should be noted that the maturity indicator level does not fully represent actual capability levels because a capability level can only be assigned through a formal appraisal process, not as the result of using an interview-based instrument. The CRR consists of six Maturity Indicator Levels, ranging from MIL-0 through MIL 5.

Maturity Level Indicators

Reference 55

MIL-0 (Incomplete) indicates that ***practices*** in a particular ***domain*** are not being performed, as measured by responses to the relevant practice questions in the CRR.

MIL-1 (Performed) indicates that all ***practices*** in a particular ***domain*** are being performed as measured by responses to the relevant practice questions in the CRR. MIL-1 means that there is sufficient and substantial support for the existence of the practices.

MIL-2 (Planned) indicates that all ***practices*** in a particular ***domain*** are not only performed

- (MIL-1), but are also:
- Established by the organization (i.e., the practice is documented and communicated to all who need to know);
- Planned (i.e., the practice is performed in accordance with a documented plan, policy, and procedure);
- Supported by stakeholders (i.e., the stakeholders of the practice are known, and these stakeholders are not only aware of the practice, but also their specific role in the practice); and
- Supported by relevant standards and guidelines (i.e., standards and guidelines that support the practice have been identified and implemented).

Reference 55

Maturity Level Indicators (cont'd)

- **MIL-3 (Managed)** indicates that indicates that all ***practices*** in a particular ***domain*** are not only performed (MIL-1) and planned (MIL-2), but also have basic infrastructure in place to support the process:
  - ***Governed by the organization*** (i.e., the practice is supported by policy, and there is appropriate oversight over the performance of the practice);
  - ***Appropriately staffed and funded*** (i.e., the staff and funds necessary to perform the practice is available);
  - ***Assigned to staff who are responsible and accountable*** for the performance of the practice (i.e., staff have been assigned to perform the practice, and are they responsible and accountable for the performance of the practice);
  - ***Performed by staff who are adequately trained*** (i.e., staff who perform the practice are adequately skilled and trained);
  - ***Produces work products that are expected*** from performance of the practice, and are placed under appropriate levels of configuration control (i.e., the practice produces artifacts and work products that are expected from performing the practice, and the configurations of these artifacts and work products are managed); and
  - ***Managed for risk*** (i.e., risks related to the performance of the practice are identified, analyzed, disposed of, monitored, and controlled).

Reference 55

Maturity Level Indicators (cont'd)

- **MIL-4 (Measured)** indicates that all ***practices*** in a particular ***domain*** are not only performed (MIL-1), planned (MIL-2), and managed (MIL-3), but are also:
  - ***Periodically evaluated for effectiveness*** (i.e., the practice is periodically reviewed to ensure that it is effective and producing intended results);
  - ***Monitored and controlled*** (i.e., appropriate implementation and performance measures are identified, applied, and analyzed);
  - ***Objectively evaluated against its practice description and plan*** (i.e., the practice is periodically evaluated to ensure that it adheres to the practice description and its plan); and
  - ***Periodically reviewed with higher-level management*** (i.e., higher-level management is aware of any issues related to the performance of the practice).

Reference 55

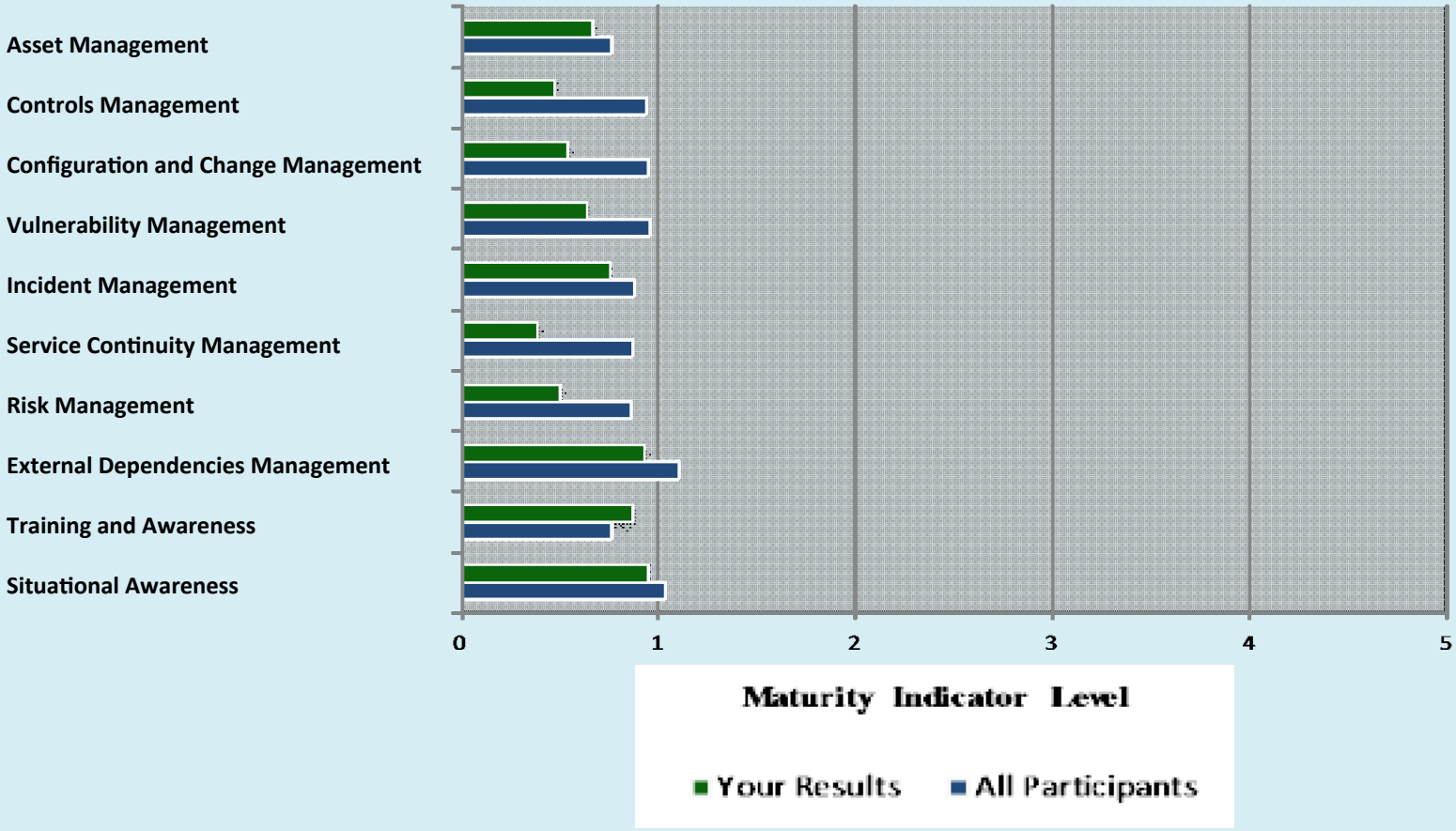
Maturity Level Indicators (cont'd)

- **MIL-5 (Defined)** indicates that all ***practices*** in a particular ***domain*** are performed (MIL-1), planned (MIL-2), managed (MIL-3), measured (MIL-4), and are also consistent across all internal constituencies who have a vested interest in the practice. At MIL-5, a process or practice is:
  - ***Defined by the organization and tailored by organizational units for their*** use (i.e., there is an organization-sponsored definition of the practice from which organizational units can derive practices that fit their unique operating circumstances); and
  - ***Supported by improvement information that is collected by and shared amongst organizational units for the overall benefit of the organization*** (i.e., practice improvements are documented and shared so that the organization as a whole reaps benefits from consistent performance of practices across organizational units and that all organizational units can benefit from improvements realized in any single organizational unit).

Summary Results

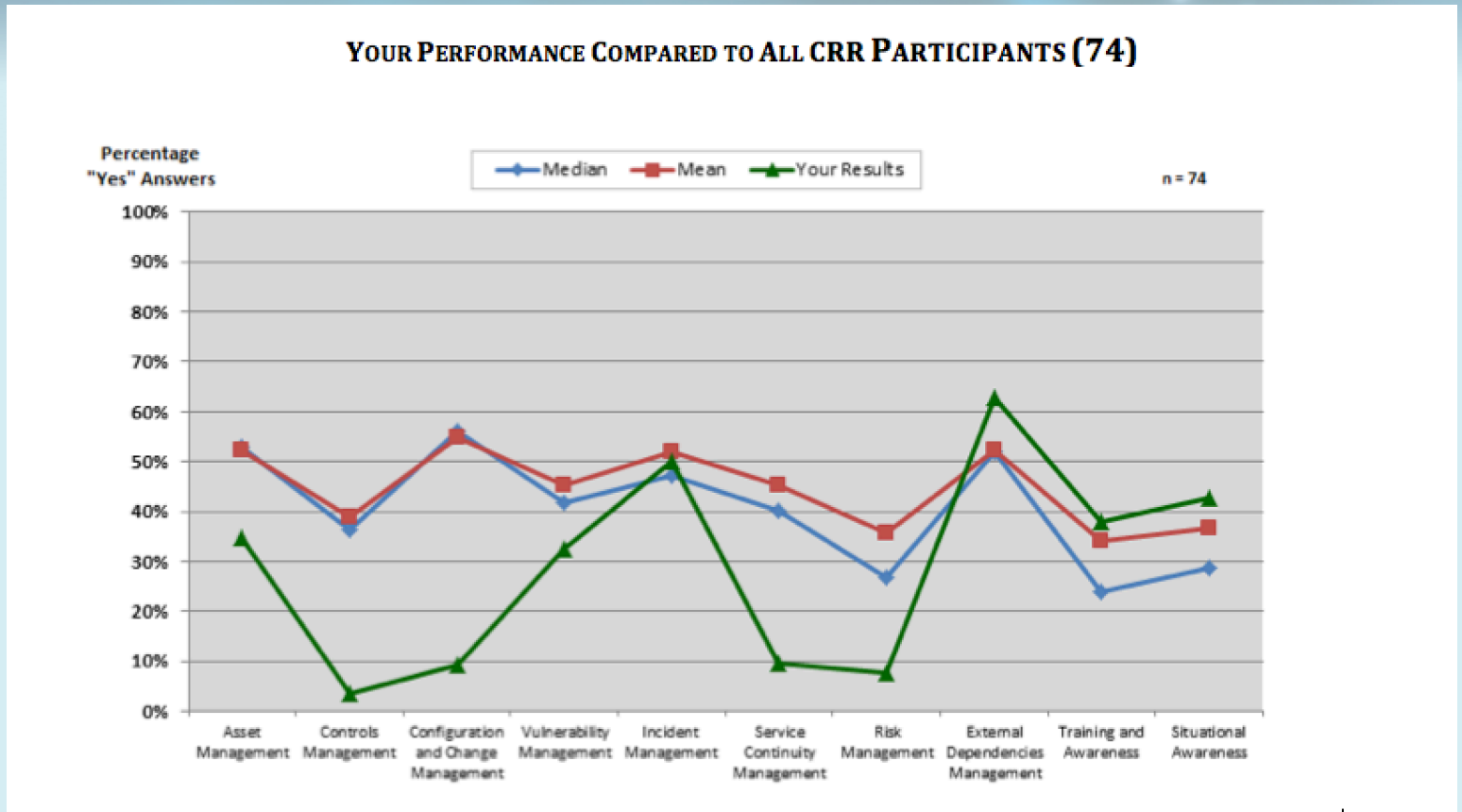
Reference 55

Maturity Indicator Level by Domain



Summary Results

Reference 55



This graph represents the median and mean "yes" scores across all CRR participants, and includes the domain practices as well as yes scores for the questions related to process maturity. The line labeled "Your Results" represents your "Yes" scores. The Median represents the midpoint score for the entire CRR participant population (the size of the data set is identified as the "n" value in the upper right corner of the graphic). The Mean is the average of total "yes" scores per domain for the CRR participant population.

Summary Results

Reference 55

OVERVIEW OF CRR RESULTS

	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

Sample Domain Report

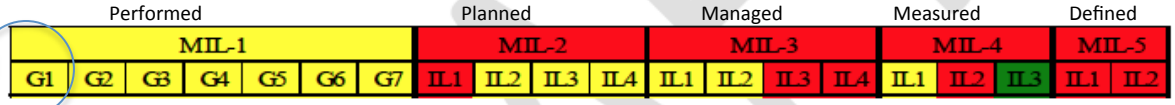
Reference 55

DOMAIN 1: ASSET MANAGEMENT

The purpose of **Asset Management (AM)** is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in **Asset Management:**

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the **Asset Management** domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.



Goal 1 – Services are identified and prioritized.		
1.	Are services identified? [SC:SG2.SP1]	Yes
2.	Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	Incomplete
Option(s) for Consideration:		
Q1	**References** Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 15-18	
Q2	**CERT-RMM Reference** **[SC:SG2.SP1]** Prioritize and document the list of high-value services that must be provided if a disruption occurs. 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.	

Performed/Achieved = Green
Incomplete=Yellow
Not performed/achieved =Red
Not addressed = Grey

Specific Resources for guidance on improving process

Outcomes

Reference 55

- Promotes Continuous Process Improvement
- Fosters Continued maturity
- Drives Systemic change
- Helps us become a better organization

Reference 55

Questions or Comments?