

CYBER RESILIENCE REVIEW (CRR) AND CISA CYBER ASSESSMENTS OVERVIEW



Jason Schaum
Supervisory Cybersecurity Advisor
Region III (MD, PA, DE, DC, VA, WV)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency



Cybersecurity Assessments

- Cyber Resilience Review (CRR - Strategic) →
- External Dependencies Management (EDM - Strategic) →
- Cyber Infrastructure Survey (CIS - Strategic) →
- Cybersecurity Performance Goals (CPG - Tactical) →
- Ransomware Readiness Assessment (RRA – Tactical) →
- Vulnerability Scanning / Hygiene (CyHy - Technical) →
- Validated Architecture Design Review (VADR - Technical) →
- Remote Penetration Test (RPT - Technical) →
- Risk and Vulnerability Assessment (RVA - Technical) →



Cybersecurity Evaluation Tool

CSET

Tools

Resource Library

Help

JASON.SCHAUM

New Assessment

My Assessments

Search



Popular Assessments

CISA Cross-Sector Cybersecurity Performance Goals (CPG)

The CPGs are a prioritized subset of IT and operational technology (OT) cybersecurity practices that critical infrastructure owners and o...

CISA Ransomware Readiness Assessment (RRA)

Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and government agencies. Rans...

NIST CSF: Framework for Improving Critical Infrastructure Cybersecurity v1.1

This approach is a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organization...

Network Diagram/Components Based Assessment

A Network Architecture and Diagram Based assessment. This assessment requires that you build or import an assessment into CSET and cre...

Land Mobile Radio Rapid Assessment (LMR)

This module is designed to assist system owners in assessing key aspects of a LMR system's current cybersecurity status based on a subset of NIST S...

CISA Sponsored (Resilience and Maturity)

CISA Cyber Infrastructure Survey (CIS)

The CIS goal is to assess the foundational and essential cybersecurity practices of an organization's critical service to identify depende...

CISA Cyber Resilience Review (CRR)

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices...

CISA External Dependencies Management (EDM)

The External Dependencies Management (EDM) Assessment evaluates an organization's management of external dependencies. This ass...

CISA Ransomware Readiness Assessment (RRA)

Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and government agencies. Rans...

CISA Minimum Viable Resilience Assessment (MVRA) - DRAFT

MVRA assesses the critical service or services essential to the success of an organization's mission and, if disrupted, would severely impact t...



<https://www.cisa.gov/downloading-and-installing-cset>

Cross Sector Cyber Performance Goals (CPGs)

- A prioritized subset of 38 cybersecurity practices
- For IT and OT
- Prioritized for risk reduction
- Informed by threats observed by CISA and its government and industry partners
- Applicable across all CI sectors
- Intended to meaningfully reduce risks to both CI operatives and the American people
- Intended to supplement the NIST CSF
- Benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity
- Highlights the Cost Impact and Complexity per goal
- Coached assessment with a CISA CSA or self assessment using the CSET tool

<https://www.cisa.gov/cpg>



1.A Asset Inventory ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7 CURRENT ASSESS

COST: \$\$\$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM

TACTIC, TECHNIQUE, AND PROCEDURE (TTP) OR RISK ADDRESSED:
 Hardware Additions (T1200)
 Exploit Public-Facing Application (T0819, ICS T0819)
 Internet-accessible device (ICS T0883)

RECOMMENDED ACTION: Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.

FREE SERVICES AND REFERENCES: [Cyber Hygiene Services](#), "Stuff Off Search" Guide or email vulnerability@cisa.dhs.gov

DATE:

IMPLEMENTED

IN PROGRESS

SCOPED

NOT STARTED

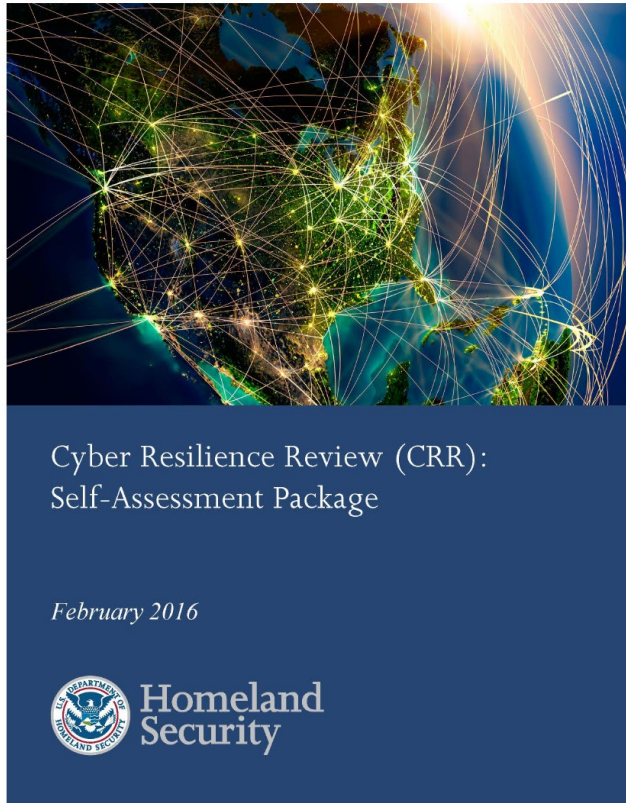
ORGANIZATIONAL CYBERSECURITY LEADERSHIP

OUTCOME	RECOMMENDED ACTION			
A single leader is responsible and accountable for cybersecurity within an organization.	A named role/position/title is identified as responsible and resourcing, and execution of cybersecurity activities. This role, such as managing cybersecurity operations at the senior level, budget resources, or leading strategy development to inform			
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">TTP or RISK ADDRESSED</th> <th style="width: 50%;">SCOPE</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Lack of sufficient cybersecurity accountability, investment, or effectiveness.</td> <td style="padding: 5px; text-align: center;">N/A</td> </tr> </tbody> </table>		TTP or RISK ADDRESSED	SCOPE	Lack of sufficient cybersecurity accountability, investment, or effectiveness.
TTP or RISK ADDRESSED	SCOPE			
Lack of sufficient cybersecurity accountability, investment, or effectiveness.	N/A			

OT CYBERSECURITY LEADERSHIP

OUTCOME	RECOMMENDED ACTION			
A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.	A named role/position/title is identified as responsible and resourcing, and execution of OT-specific cybersecurity activities. This may be the same position as identified in 4.1.			
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">TTP or RISK ADDRESSED</th> <th style="width: 50%;">SCOPE</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Lack of accountability, investment, or effectiveness of OT cybersecurity program</td> <td style="padding: 5px; text-align: center;">N/A</td> </tr> </tbody> </table>		TTP or RISK ADDRESSED	SCOPE	Lack of accountability, investment, or effectiveness of OT cybersecurity program
TTP or RISK ADDRESSED	SCOPE			
Lack of accountability, investment, or effectiveness of OT cybersecurity program	N/A			

DHS Cyber Resilience Review (CRR)



- A U.S. *Department of Homeland Security (DHS) initiative* intended to help the nation's critical *infrastructure providers* assess their organization's operational resilience and cybersecurity practices:
 - as it relates to a specific critical service
 - across ten foundational cybersecurity domains
 - based on the organization's unique risk profile



CRR Overview

- Interview-based assessment that evaluates an organization's operational resilience and cybersecurity practices on an organizations critical service.
- Derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience.
- Evaluates that maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the 10 domains.
- Consists of 299 questions.



10 CRR Domains

CRR Domains

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



Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
 - Public release under Freedom of Information Act requests,
 - Public release under State, local, tribal, or territorial disclosure laws,
 - Use in civil litigation and
 - Use in regulatory purposes.

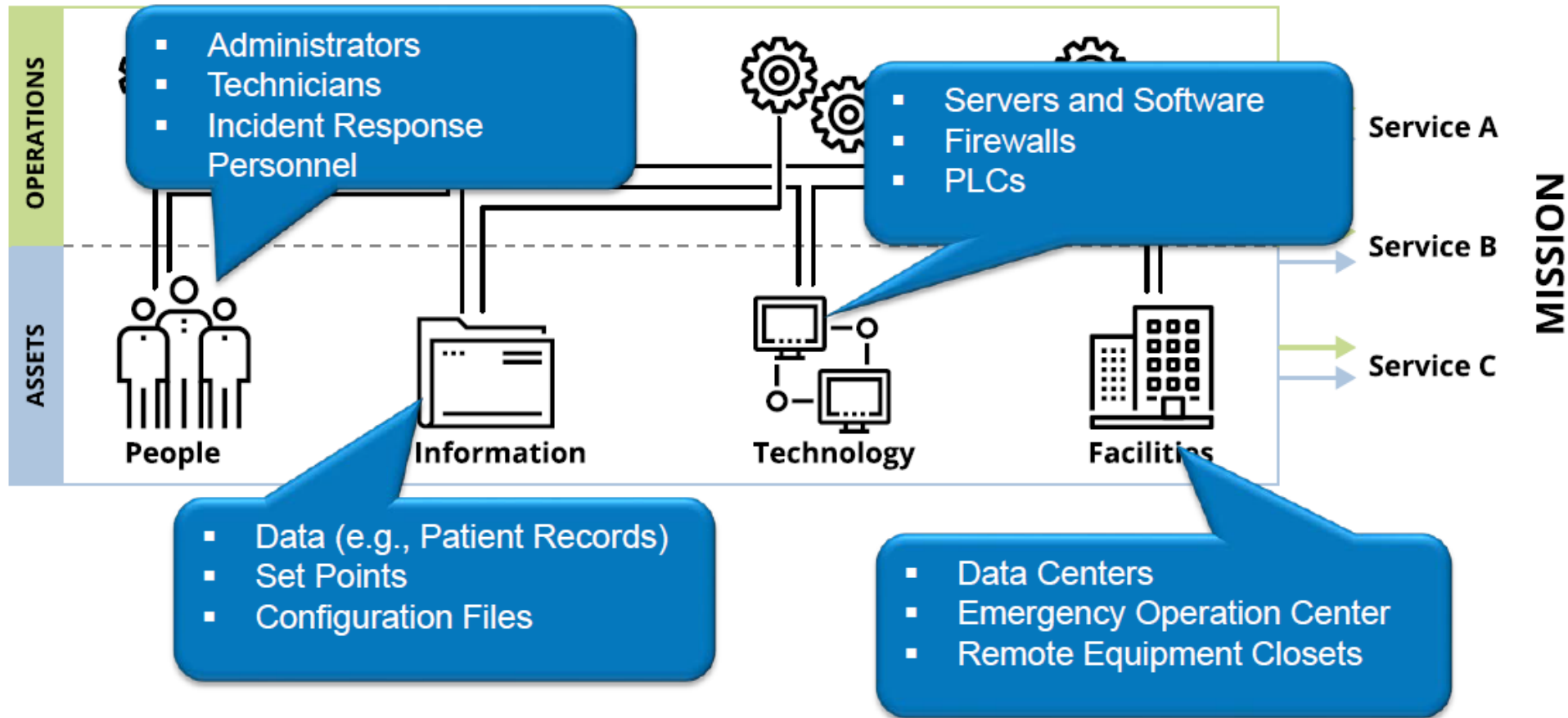


Critical Service Identification

- The CRR has a “service-oriented” approach, meaning that **one of the foundational principles of the CRR is that an organization deploys its assets (people, information, technology, and facilities) to support specific operational missions (or services).**
- The CRR is aligned with the delivery of core missions of organizations, labeled **Critical Services**. Critical services are sets of activities an organization carries out in the performance of a duty or in the production of a product that are so critical to the success of the organization that, if disrupted, would severely impact continued operations or success in meeting the organization’s mission. *Examples of critical services include transmission/distribution of electricity in energy providers, treatment of water/wastewater in water utilities, management of electronic health records in hospitals, ATM network operations in financial institutions, and police/fire dispatch in local governments.*
- CISA strives to align services to critical infrastructure sector functions in order to discover how an organization’s operations align to national security interests. Therefore, ideally, the identified critical service is connected to (or is a portion of) the sector functions (i.e., services) outlined in that sector’s Sector Specific Plan

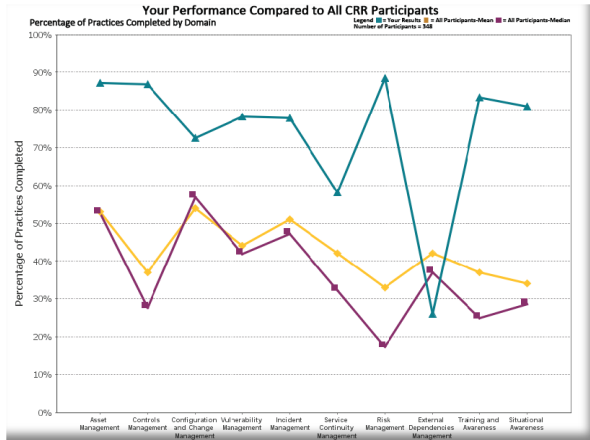


Critical Service Identification Examples



CRR Sample Report

Each CRR report includes:



Comparison data with other CRR participants
*facilitated only



A summary “snapshot” graphic, related to the NIST Cyber Security Framework.

Domain performance of existing cybersecurity capability and options for consideration for all responses

DOMAIN 1: ASSET MANAGEMENT

Legend: MML-1, MML-2, MML-3, MML-4, MML-5; G1, G2, G3, G4, G5, G6, G7

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 - Identify & prioritize critical services	Response
1. Are critical services identified? [SC.SG2.SP1]	Yes
2. Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC.SG2.SP2]	Incomplete

Q2 CERT-RMM Reference: [SC.SG2.SP1] Identify and inventory critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission.
Additional Reference: NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)

Goal 2 - Inventory assets, and establish the authority and responsibility for these assets	Response
1. Are the assets that directly support the critical service inventoried? [ADM.SG1.SP1]	People: Incomplete Information: Incomplete Technology: Incomplete Facilities: Yes

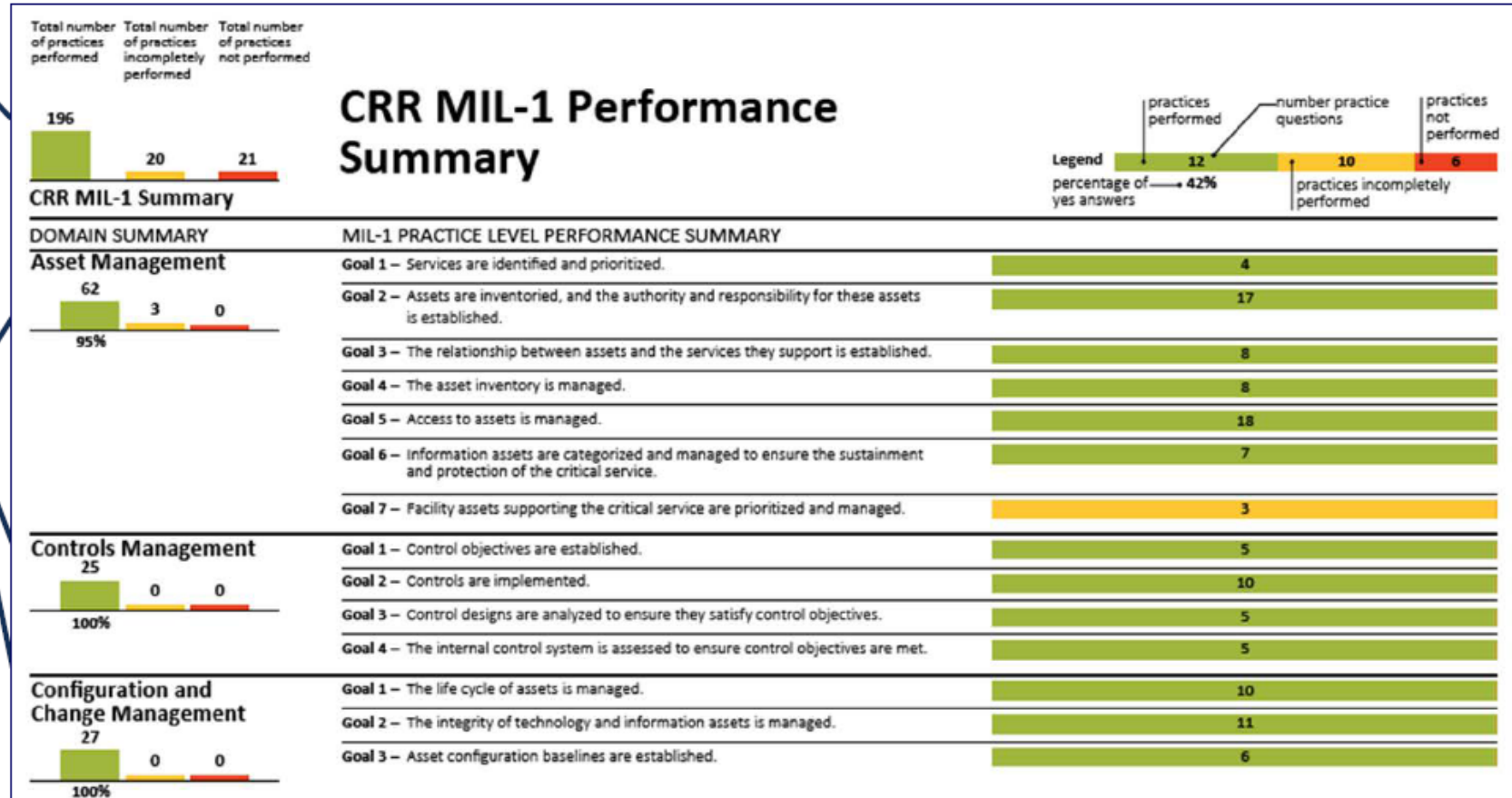
Q1 CERT-RMM Reference: [ADM.SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support.
Additional Reference: NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)



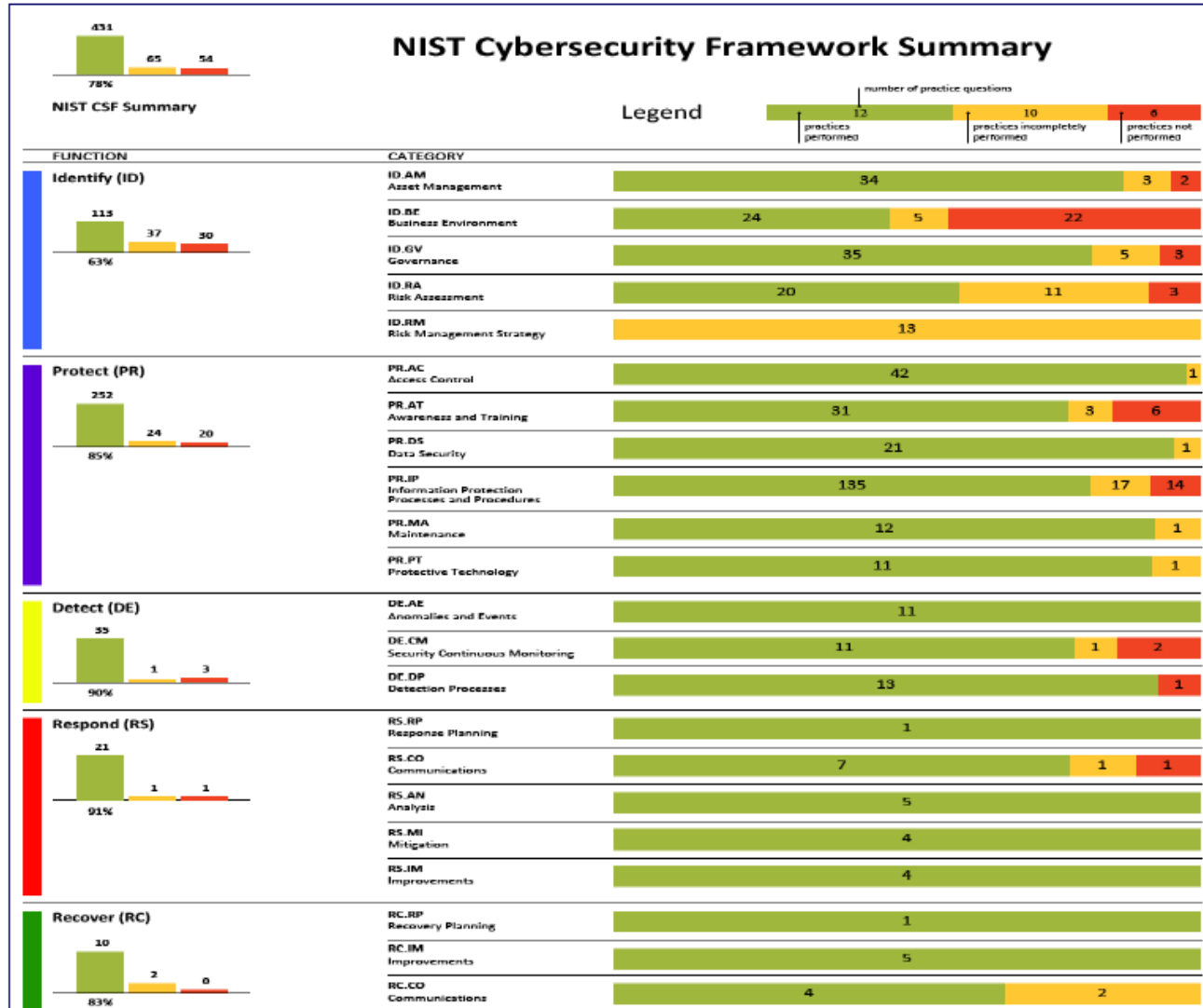
Performance Summary

Summarizes Entire CRR at MIL1

Summarizes Practice Performance for Each Domain



NIST CSF Summary



Overview of CRR Results



Asset Management

1 Asset Management



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]	Yes
3.	Is the organization's mission, vision, values, and purpose, including the organization's place in critical infrastructure, identified, and communicated? [EF:SG1.SP1]	Yes
4.	Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3]	Yes
Option(s) for Consideration:		
Q1	<p>CERT-RMM Reference [SC:SG2.SP1] Identify the organization's high-value services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission.</p> <p>Additional References Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 15-18</p> <p>NIST CSF References: ID.BE</p>	
Q2	<p>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.</p> <p>Additional References Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 16-18</p> <p>NIST CSF References: ID.AM-5, ID.BE</p>	



Getting Started - CRR Assessment Process

