



TRI - REGIONAL JETS 2025



Fortifying the Future: Mastering Cyber Resilience for Critical Operations



Fortifying the Future: Mastering Cyber Resilience for Critical Operations

Panelist:

- Chris Biegun, Associate Vice President, Black & Veatch

Moderator:

- Doug DeFazio



PANELIST

Chris Biegung, MBA,

PMP, ITIL, CCP

Black & Veatch

Associate Vice President



BLACK & VEATCH

- **Sports Teams:** Washington Redskins, Capitals, Nationals, KU, UofA, UCF
- **Vacation Spots:** *Anywhere with Sand, Sun, Surf*
- **Did You Know:** *I am a member of the International Brotherhood of Magicians*
- **Hobbies:** *Golf, Woodworking, Auto Restoration*
- **Coolest Project(s):** *Clear Radar Upgrade - "PCS'ing a Radar"*

Learning Objectives

- Understand the specialized requirements of OT Control Systems.
- Learn the Cybersecurity Resilience Review (CRR) assessment methodology including purpose, background, components, and roles to be able to begin your resilience journey.
- Know how to validate CRR responses and produce a CRR Report that the organization can use to take real action and improve its resilience.
- How to debrief your organization and assist with recommendations for improvement.

Agenda

- Frame the Context – Specialized Requirements of OT Control Systems
- Purpose of Cyber Security Resilience Review (CRR)
- CRR Domains and Association with Common Frameworks
- CRR Assessment Methodology
- What does it look like?
- Response Validation & Reporting
- Debrief and Assist with Remediation
- Q&A / Discussion

Do you have a working definition of CRR?

- a) Yes
- b) Kind of?
- c) Never heard of it

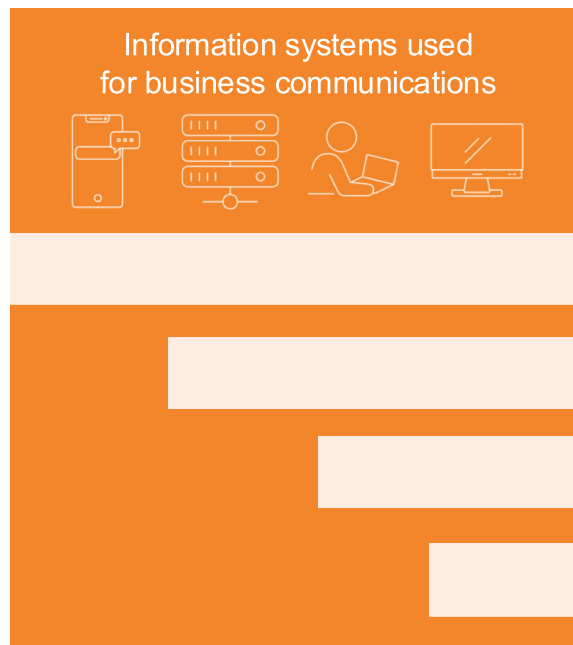


Understand the Specialized Requirements of OT Control Systems



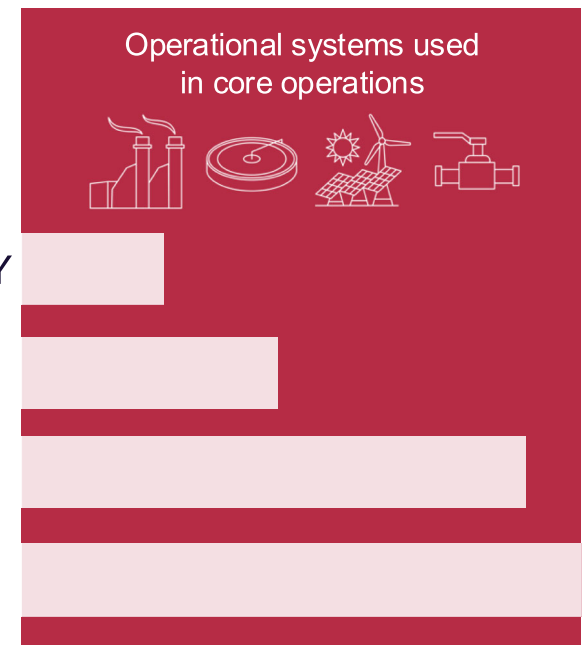
IT/OT Difference and Its Effect in the CIA Triad

IT



+ IMPORTANCE -

OT



- IMPORTANCE +

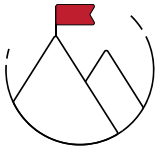
CONFIDENTIALITY

INTEGRITY

AVAILABILITY

SAFETY

Growing Concerns About Cyberattacks Calls for Additional Guidance



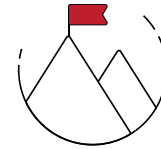
Top 5 Challenging Issues in Critical Infrastructure

- Aging Infrastructure
- Aging Workforce
- Funding
- Expanding Regulation
- Managing Capital Costs



Clients' Top Objectives in Digital Solutions Strategy

- Asset Monitoring, Measurement and Analysis
- Cybersecurity
- Operations Planning and Control
- Monitoring and Compliance
- Capital Improvement Plan (CIP) Development/Optimization
- System Resilience



Top 5 Challenges Implementing OT Cybersecurity Programs

- Resources (Staff)
- Budget (Funding)
- Cyber Expertise
- Clear and Actionable Plan
- Control Systems Expertise

Accelerated
Adoption of
Emerging
Technology



Artificial Intelligence (AI)
Industrial Internet of Things (IIoT)
Cloud-Based and Remote Access
Smart Technology
Machine Learning (ML)

Poor Cyber
Resilience
is a **Safety Risk**
and Uptime
Issue

Lack of
Visibility and
Control Over
Your OT
Assets

70% of
vulnerabilities
reside deep within the network*.



Skill Set
Gaps

Lack of in-house OT
cybersecurity
professionals due to
resources and/or
shortage of OT
cybersecurity
professionals.



Over the past year,
ransomware attacks
against industrial
organizations
increased **87%***

Increase in
Ransomware
and
Cyberattacks
to Critical
Infrastructure

Increase in
attacks, growing
technology
dependence and
stronger
regulations
have made
**Industrial
Cybersecurity
an operational
reality and a
business
imperative.**

Purpose of a Cybersecurity Resilience Review (CRR)



Cyber Resilience Review (CRR)

A Cyber Resilience Review (CRR) is a 1-Day assessment designed to evaluate an organization's operational resilience and cybersecurity practices. Conducted through interviews, the CRR helps organizations understand their ability to manage cyber risks during both normal operations and times of stress or crisis.

Cyber Resilience Review (CRR)

Developed by Carnegie Mellon University's Software Engineering Institute

- More information: <http://www.cert.org/resilience/rmm.html>
- Derived from the Computer Emergency Response Teams (CERT ®)
- CERT® Resilience Management Model (CERT® RMM), a process improvement model for managing operational resilience

Cybersecurity & Infrastructure Security Agency (CISA) CRR Assessment Tool

- Focus on one critical IT/OT service in your cyber security program.
- Assess cyber security and operational risk management practices.
 - Normal operations (protection & sustainment)
 - Times of operational stress and crisis (survivability & resilience)

Assess Against Critical Services



Chemical



Commercial Facilities



Communications



Critical Manufacturing



Dams



Defense Industrial Base



Emergency Services



Energy



Financial Services



Agriculture and Food



Government Facilities



Healthcare and Public Health



Information Technology



Nuclear Reactors, Materials & Waste



Transpiration Systems



Water & Wastewater Systems

CRR Benefits

Per DHS/CISA, a CRR assessment:

- **Improves** enterprise-wide awareness for effective cybersecurity management
- Reviews the capabilities essential to the **continuity of critical services** during operational challenges and crisis
- Achieves a better understanding of the **interconnectedness** of the organization and its role **in critical infrastructure**
- **Strengthens** the organization's cybersecurity posture in support of its mission
- Provides a comprehensive road map for **improvement**

The 10 CRR Domains



The 10 CRR Domains

Evaluate
maturity of an
organization's
capacities and
capabilities
across 10
domains

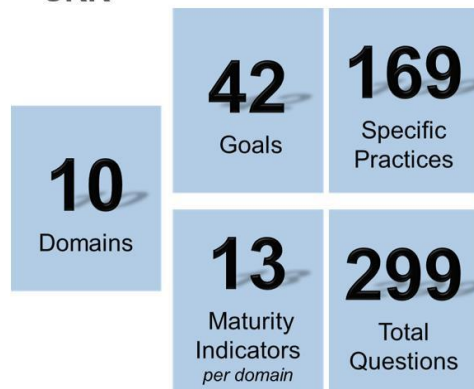
	Asset Management
	Controls Management
	Configuration and Change Management
	Vulnerability Management
	Incident Management
	Service Continuity Management
	Risk Management
	External Dependencies Management
	Training and Awareness
	Situational Awareness

Maturity Indicator Level (MIL) Scale

CRR – Higher maturity translates into **higher capable** and stable processes that:

- Produce consistent results over time
- Are retained during times of stress

CRR



*Processes are acculturated,
defined, measured, and governed*

*Practices are performed
Practices are incompletely
performed, or not performed*

MIL Level 5 – Defined
MIL Level 4 – Measured
MIL Level 3 – Managed
MIL Level 2 – Planned
MIL Level 1 – Performed
MIL Level 0 – Incomplete



CRR Supports Different Cyber Standards



OT Policies & Procedures – Modifications Required

General	Policies & Procedures	System	Component
62443-1-1 Concepts and models	62443-2-1 Security program requirements or IACS asset owners	62443-3-1 Security technologies for AICS	62443-4-1 Secure product development lifecycle requirements
62443-1-2 Master glossary of terms and abbreviations	62443-2-2 Security Protection Rating	62443-3-2 Security risk assessment and system design	62443-4-2 Technical security requirements for IACS components
62443-1-3 System security conformance metrics	62443-2-3 Patch management in the IACS environment	62443-3-3 System security requirements and security levels	
62443-1-4 IACS security lifecycle and use-cases	62443-2-4 Requirements for IACS service providers		
	62443-2-5 Implementation guidance for IACS asset owners		

IEC 62443 - Globally recognized series of standards developed to address challenges in Industrial Automation and Control Systems (IACS)

- Part 1 – General
- Part 2 – Policies & Procedures
- Part 3 – System
- Part 4 – Component

Part 2-1: Establishing an IACS security program.

Requirements to define and implement effective IACS security programs

Part 3-2: Security risk assessment for system design

addresses cybersecurity risk assessment and system design. The output of this standard is the zone and conduit model, the associated risk assessments, and target security levels. These are documented in the Cybersecurity Requirements Specifications.

Part 3-3: System security requirements and security levels

describes the requirements for an IACS system based on security level. The principal audience includes control systems suppliers, system integrators, and asset owners.

CRR Alignment to IEC 62443



Asset Management



Controls Management



Configuration and Change Management



Vulnerability Management



Incident Management



Service Continuity Management



Risk Management



External Dependencies Management



Training and Awareness



Situational Awareness

ANSI/ISA-62443-4-2-2018

Second Printing August 28, 2019

Security for industrial automation and control systems,
Part 4-2: Technical security requirements for IACS components

Foundational Requirements 7 – Resource availability

- CR 7.1 – Denial of service protection
 - RE (1) Manage communication load from component
- CR 7.2 – Resource management
- CR 7.3 – Control system backup
 - RE (1) Backup integrity verification
- CR 7.4 – Control system recovery and reconstitution
- CR 7.5 - Emergency Power
- CR 7.6 – Network and security configuration settings
 - RE (1) Machine-readable reporting of current security settings
- CR 7.7 – Least functionality
- CR 7.8 – Control system component inventory

CRR Mapped to NIST Cybersecurity Framework



NIST Cybersecurity Framework



CRR Mapped to CMMC Domains



Asset Management

Controls Management

Configuration and Change Management

Vulnerability Management

Incident Management

Service Continuity Management

Risk Management

External Dependencies Management

Training and Awareness

Situational Awareness

Access Control

Systems and Communications Protection

Configuration Management

System And Information Integrity

Incident Management

Risk Assessment

Awareness Training

Situational Awareness

CMMC Model

LEVEL 3

Model	Assessment
134 requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800- 172)	- DIBAC certification assessment every 3 years - Annual Affirmation

LEVEL 2

110 requirements aligned with NIST SP 800-171 R2	- C3PAO certification assessment every 3 years, or - Self assessment every 3 years for select programs - Annual Affirmation
---	---

LEVEL 1

15 requirements aligned with FAR 52.204-21	- Annual Self Assessment - Annual Affirmation
---	--

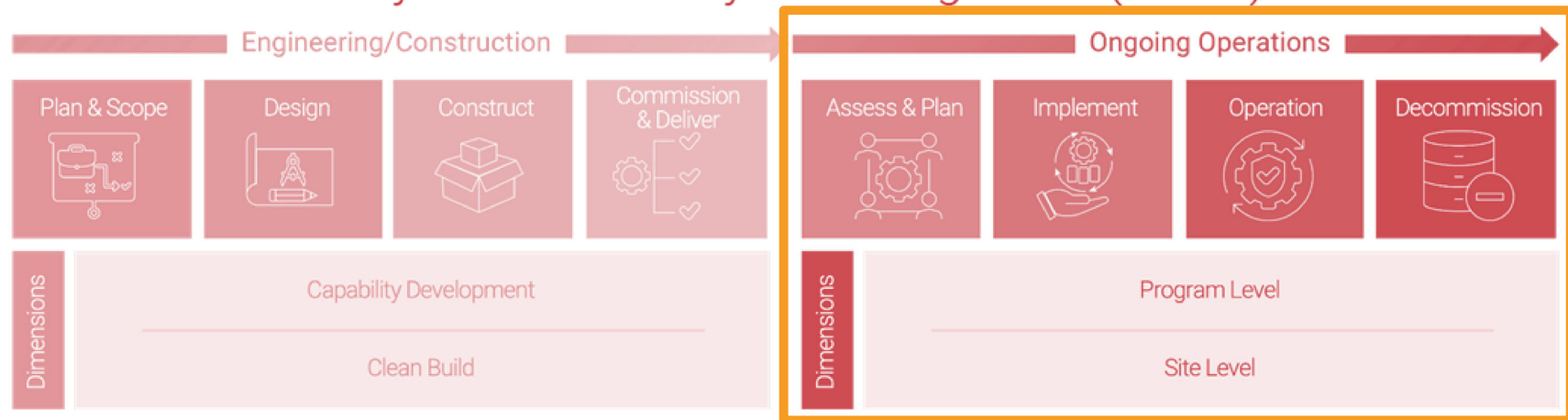
Learn the CRR Assessment Methodology



Complete OT Asset Lifecycle Protection

The cybersecurity program needs to address the cyber-physical nature of the attacks that could impact the operations to provide solutions with a consequence-driven approach.

Cyber Asset Lifecycle Management (CALM)

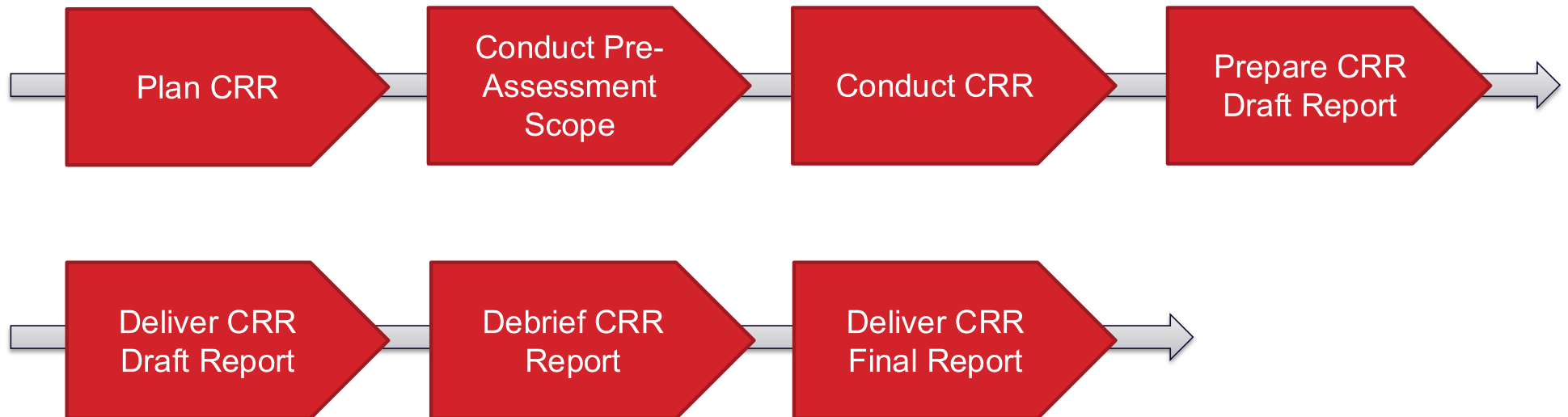


Build a clean and long-term robust cybersecurity program

Develop a roadmap that keeps the operations running during unexpected events

Secure the necessary funding and align the company's strategy with the overall cybersecurity goals.

CRR Assessment Process



CRR Assessment PLAN

Plan CRR

Organization Information

- Seek Senior Management Involvement - Sponsor
 - Approval to Conduct CRR Assessment
- Organization Point of Contact: Name, Title, Email, Phone Number
- What, if any, standards or bodies of practice are being used, regulations govern the organization?
- Location (city, state)

CRR Assessment SCOPE

Plan CRR

Conduct Pre-
Assessment
Scope

- Understanding the organization and its dependencies
- Collecting demographic information
- Identify the critical service
- Diverse set of participants ensures accuracy and completeness
- Scheduling the assessment

CRR Assessment CONDUCT

Plan CRR

Conduct Pre-
Assessment
Scope

Conduct CRR



CYBER RESILIENCE REVIEW (CRR)

Self-Assessment Package

CRR Assessment Tool

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]	☐	☐	☒	☐
3. Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified, and communicated? [EF:SG1.SP1]	☒	☐	☐	☐
4. Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3]	☒	☐	☐	☐

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 (technology includes hardware, software, and external information systems)? [ADM:SG1.SP1]	☒	☐	☐	☐
People	☒	☐	☐	☐

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]

G

☐
☐
☐

C

2. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]

G

☐
☐
☐

C

Question Intent: To determine if services are prioritized based on analysis of the potential impact if the services are disrupted.

- The organization should conduct analysis of identified services (e.g., a business impact analysis) to determine the impact to the organization of the loss or disruption of each service.
- The results of this analysis should then be used to prioritize the organizational services.

Goal 1
re
Typical work products:

- results of risk assessment and business impact analyses
- prioritized list of organizational services, activities, and associated assets

Criteria for "Yes" Response:

- The organization has prioritized all services (identified in G1:Q1).

Criteria for "Incomplete" Response:

- The organization has prioritized some services.

Facilities

☐
☐
☐

C

2. Do ass

Key Takeaway: Use the Guidance

3 Configuration and Change Management

The purpose of Configuration and Change Management is to establish processes to ensure the integrity of assets using change control and change control audits.

Goal 1 - The life cycle of assets is managed.

		Yes	Incomplete	No	
1.	Is a change management process used to manage modifications to assets? [ADM:SG3.SP2]				
	Information	☐	☐	☒	☐
	Technology	☐	☐	☒	☐
	Facilities	☐	☐	☒	☐
2.	Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3]				
	Information	☐	☐	☒	☐
	Technology	☐	☐	☒	☐
	Facilities	☐	☐	☒	☐
3.	Is capacity management and planning performed for assets? [TM:SG5.SP3]	☒	☐	☐	☐
4.	Are change requests tracked to closure? [TM:SG4.SP3]	☐	☐	☒	☐
5.	Are stakeholders notified when they are affected by changes to assets? [ADM:SG3.SP2]	☒	☐	☐	☐

3 Configuration and Change Management

Each CRR domain concludes with Maturity Indicator Level (MIL) questions*

- MIL-1 = Performed
- MIL-2 = Planned
- MIL-3 = Managed
- MIL-4 = Measured
- MIL-5 = Defined

		Yes	Incomplete	No	
MIL2-Planned	1. Is there a documented plan for performing change management activities?	☐	☐	☒	☐
	2. Is there a documented policy for change management?	☐	☐	☒	☐
	3. Have stakeholders for change management activities been identified and made aware of their roles?	☐	☐	☒	☐
	4. Have change management standards and guidelines been identified and implemented?	☐	☐	☒	☐
MIL3-Managed	1. Is there management oversight of the performance of the change management activities?	☐	☐	☒	☐
	2. Have qualified staff been assigned to perform change management activities as planned?	☐	☐	☒	☐
	3. Is there adequate funding to perform change management activities as planned?	☐	☐	☒	☐
	4. Are risks related to the performance of planned change management activities identified, analyzed, disposed of, monitored, and controlled?	☐	☐	☒	☐
MIL4-Measured	1. Are change management activities periodically reviewed and measured to ensure they are effective and producing intended results?	☐	☐	☒	☐
	2. Are change management activities periodically reviewed to ensure they are adhering to the plan?	☐	☐	☒	☐
	3. Is higher-level management aware of issues related to the	☐	☐	☒	☐

Key Takeaway: Answer All 10 Domain Maturity Questions

Know How to Validate CRR Responses and Produce a CRR Report

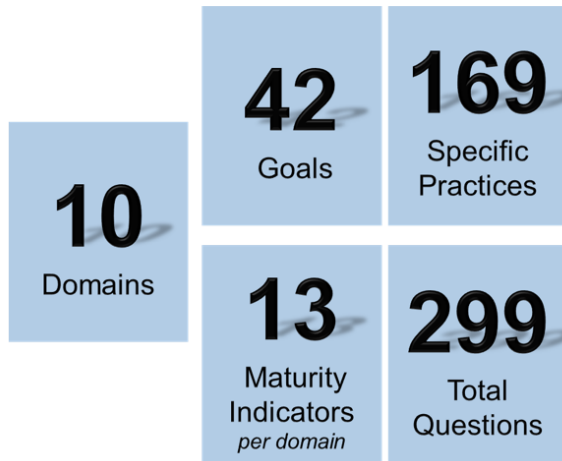


Maturity Indicator Level (MIL) Scale

CRR - Higher maturity translates into higher capable and stable processes that:

- Produce consistent results over time
- Are retained during times of stress

CRR



Processes are acculturated, defined, measured, and governed

*Practices are performed
Practices are incompletely performed, or not performed*

MIL Level 5 - Defined

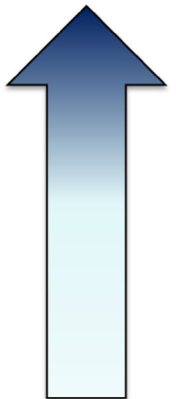
MIL Level 4 - Measured

MIL Level 3 - Managed

MIL Level 2 - Planned

MIL Level 1 - Performed

MIL Level 0 - Incomplete



CRR Assessment DRAFT REPORT

Plan CRR

Conduct Pre-
Assessment
Scope

Conduct CRR

Prepare CRR
Draft Report

Deliver CRR
Draft Report

- Draft report 30 days after the assessment
- Before forwarding to the organization encrypt the report
- Give SMEs/participants 10 days to respond with any comments

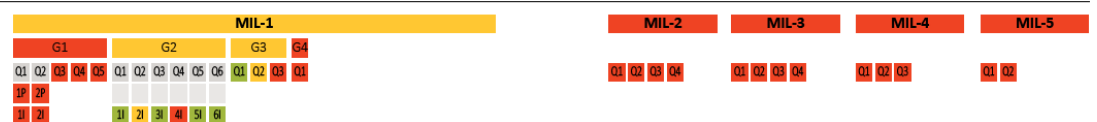
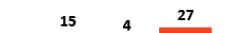
PLEASE USE THE BUTTONS BELOW TO GENERATE THE REPORT, REVISE THE ASSESSMENT, PRINT THE REPORT, OR PRINT THE ASSESSMENT

Generate Report

Print Assessment Form

The buttons on this page are enabled based upon the state of your assessment and report.

- Initially, when in assessment mode, the **Generate Report** and **Print Assessment Form** buttons are available.



Provides Question-Level
References to Help
Organizations Focus on
Specific Practices for
Improvement

Goal 1-A process for identifying, analyzing, responding to, and learning from incidents is established.		
1.	Does the organization have a plan for managing incidents? [IMC:SG1.SP1]	No
2.	Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	No
3.	Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]	No
4.	Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]	No
Option(s) for Consideration:		
Q1	CERT-RMM Reference [IMC:SG1.SP1] Establish the incident management plan. The incident management plan should address at a minimum: - the organization's philosophy for incident management - the structure of the incident management process - the requirements and objectives of the incident management process relative to managing operational resilience - a description of how the organization will identify incidents, analyze them, and respond to them - the roles and responsibilities necessary to carry out the plan - applicable training needs and requirements - resources that will be required to meet the objectives of the plan - relevant costs and budgets associated with incident management activities Additional References Special Publication 800-61 "Computer Security Incident Handling guide" Handbook for Computer Security Incident Response Teams (CSIRTs) NIST CSF References: DE.DP-1, PR.IP-9, ID.SC-5	
Q2	CERT-RMM Reference [IMC:SG1.SP1] Revise the plan and commitments as necessary. Additional References NIST SP 800-53 Rev. 4 IR-8 NIST CSF References: DE.DP-5, PR.IP-10, ID.SC-5	

Key Takeaway: Draft Assessment Report Gives You the Roadmap

Debrief Organization and Assist with Recommendations for Improvement



CRR Assessment DRAFT REPORT

Plan CRR

Conduct Pre-
Assessment
Scope

Conduct CRR

Prepare CRR
Draft Report

Deliver CRR
Draft Report

Debrief CRR
Report

Deliver CRR
Final Report

- Within 14 calendar days schedule and conduct an Assessment Report Debrief
- Recommendations for improvements

What is the MIL Score for each of the following domains?

Summarizes How
MIL Questions
Were Answered

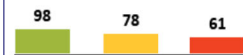
CRR Performance Summary																								
Domain Summary		MIL-1 Performed Domain practices are being performed.							MIL-2 Planned: Domain practices are supported by planning, policy, stakeholders, and standards.				MIL-3 Managed: Domain practices are supported by governance and adequate resources.				MIL-4 Measured: Domain practices are supported by measurement, monitoring, and executive oversight.			MIL-5 Defined: Domain practices are supported by enterprise standardization and analysis of lessons learned.				
Asset Management		G1	G2	G3	G4	G5	G6	G7	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Controls Management		G1	G2	G3	G4				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Configuration and Change Management		G1	G2	G3					Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Vulnerability Management		G1	G2	G3	G4				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Incident Management		G1	G2	G3	G4	G5			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Service Continuity Management		G1	G2	G3	G4				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Risk Management		G1	G2	G3	G4	G5			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
External Dependencies Management		G1	G2	G3	G4	G5			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Training and Awareness		G1	G2						Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			
Situational Awareness		G1	G2	G3					Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q1	Q2			

MIL 0
MIL 1
MIL 2
MIL 0
MIL 4
MIL 5
MIL 0
MIL 0
MIL 5
MIL 0

Summarizes
Entire CRR
at MIL1

Summarizes
Practice
Performance
for Each
Domain

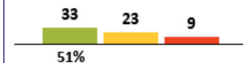
Total number
of practices
performed
Total number
of practices
incompletely
performed
Total number
of practices
not performed



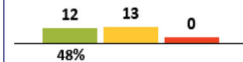
CRR MIL-1 Summary

DOMAIN SUMMARY

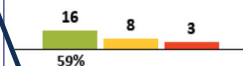
Asset Management



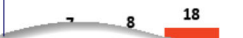
Controls Management



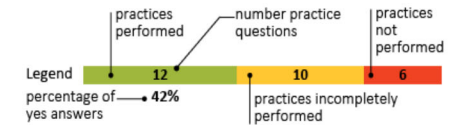
Configuration and Change Management



Vulnerability Management



CRR MIL-1 Performance Summary



MIL-1 PRACTICE LEVEL PERFORMANCE SUMMARY

Goal 1 – Services are identified and prioritized.	2	2	
Goal 2 – Assets are inventoried, and the authority and responsibility for these assets is established.	11	6	
Goal 3 – The relationship between assets and the services they support is established.	3	4	1
Goal 4 – The asset inventory is managed.	2	3	3
Goal 5 – Access to assets is managed.	9	5	4
Goal 6 – Information assets are categorized and managed to ensure the sustainment and protection of the critical service.	5	1	1
Goal 7 – Facility assets supporting the critical service are prioritized and managed.	1	2	
Goal 1 – Control objectives are established.	3	2	
Goal 2 – Controls are implemented.	7	3	
Goal 3 – Control designs are analyzed to ensure they satisfy control objectives.	2	3	
Goal 4 – The internal control system is assessed to ensure control objectives are met.		5	
Goal 1 – The life cycle of assets is managed.	5	3	2
Goal 2 – The integrity of technology and information assets is managed.	6	4	1
Goal 3 – Asset configuration baselines are established.	5	1	
Goal 1 – Preparation for vulnerability analysis and resolution activities is conducted.	3	4	4
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	4	3	11
Goal 3 – Vulnerabilities are managed.	1		

CRR Final Report



- Provide guided interpretation of the final report and action plans for improvement
- CERT ® Division collected the results of nearly **500 CRRs** over a four-year period

Key Takeaway: Most Organizations had an Average MIL Score of Less than MIL-1

Cyber Resilience Review (CRR)

- U.S. Cybersecurity & Infrastructure Security Agency (CISA) initiative is intended to help the nation's critical infrastructure providers assess their organization's operational resilience and cybersecurity practices
- CRR assesses a specific critical service
- Across ten foundational cybersecurity domains
- Based on the organization's unique risk profile
- CRR improves your adopted framework
- How to access the CRR assessment tool:

CISA

<https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr>

Cyber Security Evaluation Tool (CSET) Github

<https://github.com/cisagov/cset/releases>



Cyber Resilience Review Downloadable Resources

Revision Date: December 17, 2020

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#), [CYBER THREATS AND ADVISORIES](#),



Available are the downloadable content and guides for the Cyber Resilience Review Self-Assessment.

Resource Materials

Resource Name	File Type	File Size	Language
CRR Self-Assessment [PDF] 1	PDF	8.03 MB	
CRR User Guide [PDF] 2	PDF	6.22 MB	
CRR Question Set with Guidance [PDF] 3	PDF	1.78 MB	
CRR NIST Framework Crosswalk [PDF] 4	PDF	5.21 MB	

<https://www.cisa.gov/resources-tools/resources/cyber-resilience-review-downloadable-resources>

CRR - Cyber Security Evaluation Tool (CSET)

<https://github.com/cisagov/cset/releases>

CSET v12.2.1.0

Latest

What's New:

- The NIST Cybersecurity Framework (CSF) 2.0: The NIST CSF provides guidance to industry, government agencies, and other organizations to reduce cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The Framework does not prescribe how outcomes should be achieved. Rather, it maps to resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. Building on previous versions, CSF 2.0 contains new features that highlight the importance of governance and supply chains.
- Cybersecurity Maturity Model Certification (CMMC) 2.0: The CMMC framework consists of the security requirements from NIST SP 800-171 Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and a subset of the requirements from NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171. The CMMC model measures the implementation of cybersecurity requirements at three levels.
- **Feedback:** Contact email updated to CSET_PMO@cis.dhs.gov.
- **GitHub:** CSET downloads are now available exclusively from GitHub.
- Bug fixes and general quality of life improvements.

Algorithm: SHA256

Hash: 8361E0331069F430F69EC0BA9EA77789EB2260870C982014222437AECE6F6B73

Path: CSETStandAloneV12210.exe

▼ Assets 7

CSET.12.2.1.slick.sheet_Public.pdf	344 KB	Feb 17
CSETAddUser.zip	63.3 MB	Dec 11, 2024
CSETDatabaseUpgradeV12210.zip	139 MB	Dec 11, 2024
CSETStandAloneV12210.exe	1.49 GB	Nov 5, 2024
CSETv12210_Enterprise_Binaries.zip	1.29 GB	Dec 11, 2024
Source code (zip)		Jun 13, 2024

Q&A / Discussion





Contact Us



Chris Biegun
biegunc@bv.com



Dean Rock
dean.rock@steeltoad.com



TRI - REGIONAL JETS 2025

