A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

DoD–Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

WHAT IS A CYBER RESILIENCE ANALYSIS (CRA)?

- An evaluation of processes and practices across 10 security domains that provides insight into an organization's operational resilience and ability to manage cyber risk
- A review of the overall health of an organization's cybersecurity program as it relates to a specific critical service which helps to:
  - Develop an understanding of existing process-based cybersecurity capabilities
  - Develop meaningful indicators of operational resilience
  - Improve organizational ability to manage cyber risk to its critical services and related assets

"From a CMMC perspective, it's incredibly valuable for a level 4 & 5 maturity. The CRA allows you to look at the qualitative data rather than just the quantitative aspect. Once we get through the fine tuning, it will help us out tremendously."
–Cory C, DIB CS Partner

"The CRA was completed last month and we had the review of the report today. It was very helpful in getting a feel for where we are in compliance with NIST SP 800-171, how we do with regards to the Cyber Security Framework, and helping prepare for CMMC."
–Frank K, DIB CS Partner

The CRA now includes mappings to the NIST CSF Ransomware Profile. Based on how an organization answers the CRA questions, depictions are created that show how an organization is performing practices that relate to ransomware protections.

At A Glance:

- The CRA is a structured survey that may be conducted during a one day, DC3 facilitated session, or it may be downloaded from DIBNet-U and performed as a self-assessment.
- The CRA findings are captured in a comprehensive report that provides the organization with suggested options for consideration on various aspects of the 10 security domains.
- Security domains and organizational practices are mapped to the NIST SP 800-171 requirements to protect CUI and the NIST Cybersecurity Framework.

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center

WHAT IS A CYBER RESILIENCE ANALYSIS (CRA)?

How Would the CRA Benefit My Organization?

- Provides an understanding of which cybersecurity practices inform specific NIST SP 800-171 requirements, as well as how those practices align with the NIST CSF and CMMC v2.0
- Provides an easy to understand, comprehensive final report indicating the relative maturity of organizational resilience and cybersecurity capabilities that includes:
  - A baseline that aids in improvement efforts
  - Visual scoring depictions for performance across the various security domains
  - Recommendations for organizational process improvement

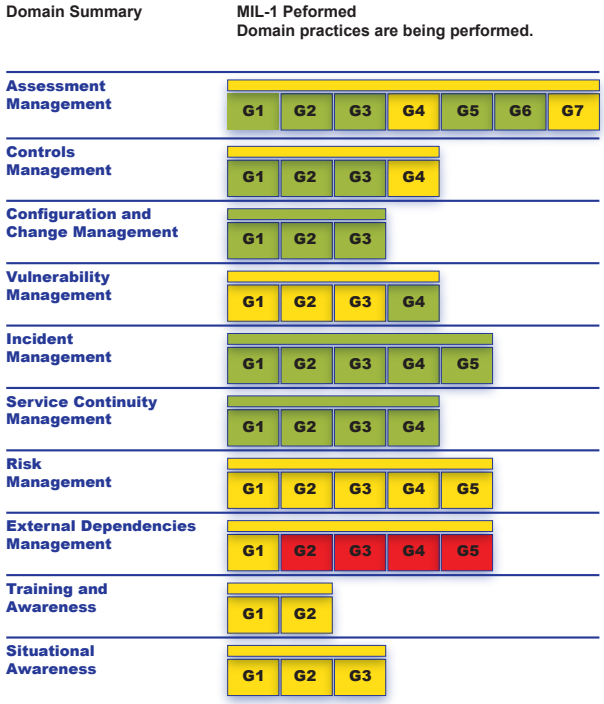
Cyber Hygiene– A Baseline Set of Practices

The CRA includes cyber hygiene guidance that will establish a solid baseline for your organization, strengthen existing best practices, and identify actionable next steps

These key practices include:

- Identify and prioritize key organizational services, products and their supporting assets
- Identify, prioritize, and respond to risks to the organization's key services and products
- Establish an incident response plan
- Conduct cybersecurity education and awareness activities
- Establish network security and monitoring
- Control access based on least privilege and maintain the user access accounts
- Manage technology changes and use standardized secure configurations
- Implement controls to protect and recover data
- Prevent and monitor malware exposures
- Manage cyber risks associated with suppliers and external dependencies
- Perform cyber threat and vulnerability monitoring and remediation

CRA Performance Summary



Snapshot of CRA assessment at Maturity Indicator Level (MIL) 1. The CRA evaluates capabilities across 5 MILs.

Ten Domains of Capability in CRA	
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

How Can I Learn More?

DCISE is eager to support our Partners by offering the CRA as a service. Please contact us by email at DC3.DCISE@us.af.mil or visit the CRA forum on DIBNet-U at https://dibnet.dod.mil/portal/intranet/forum.

Pub Date: 22 March 2022

DC3.DCISE@us.af.mil
877.838.2174 | 410.981.0104

DoD CYBER CRIME CENTER
410.981.6610 | www.dc3.mil | DC3.Information@us.af.mil

@DC3Forensics • @DC3DCISE
DC3 Cyber Crime Center