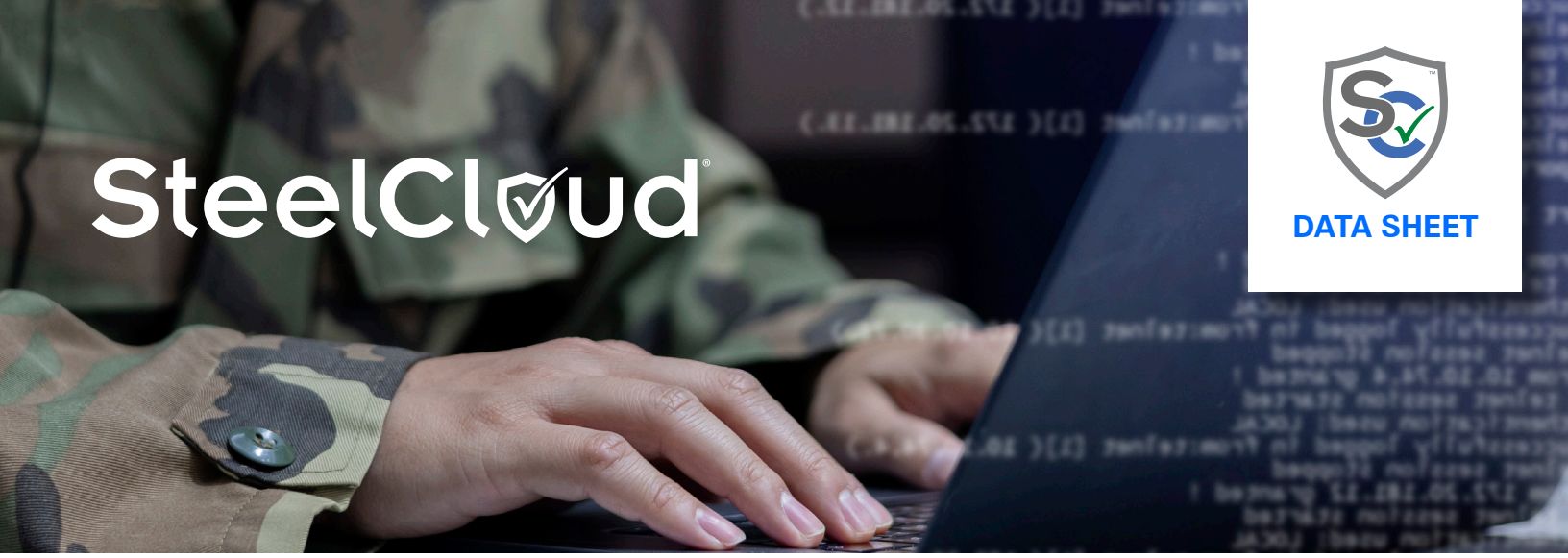

SteelCloud

DATA SHEET

Everything you need to know about CORA

Get ready for your assessment—and stay CORA-ready with automation.

Established in 2010 by DISA, the Command Cyber Readiness Inspection (CCRI) was known to cause sweat to break out on the brows of DoD cybersecurity professionals. In March 2024, the DoD renamed the program, reengineered it and made the process more composed. Today, it's called the Cyber Operational Readiness Assessment (CORA) and it has different requirements and expectations.

Six things to know about the shift to CORA.

1. Devised to verify and strengthen DoD cybersecurity compliance
2. Moved from a checklist inspection to an assessment of current operational readiness
3. Replaced previous grading scale with recommendations to strengthen your posture in the future
4. Evolved into an agile, resilient approach that takes multiple factors—and the changing landscape—into consideration
5. Intended to relieve the strain on resources and create a right-sized assessment for each agency and department
6. Recommended the use of automation wherever possible

Why CORA is a fundamental improvement in cybersecurity assessment.

By shifting to the assessment mindset, CORA enables leaders to see where they are and make better-informed decisions when applying cybersecurity resources. It also recognizes that your cybersecurity posture is a living, breathing organism that changes over time as threats and remediation techniques change over time. This allows CORA to adapt and respond to the shifting landscape so agencies can concentrate limited resources on addressing the highest risk areas first.

We can't tell you what they'll INSPECT in your agency.

To determine which organizations get assessments, what gets assessed, and how often, the CORA program uses a risk calculus that tailors each assessment to the agency and department they are assessing. Visits are based on a multifactor analysis that takes needs and team resources into account.

We can tell you what your ASSESSMENT will be based on.

CORA prioritizes MITRE ATT&CK mitigations and threat intelligence to minimize adversarial risk to the DoDIN. MITRE ATT&CK is a knowledge base of adversarial tactics, techniques and procedures (TTPs) and is used globally to not just protect and defend information systems and networks, but also to hunt bad actors. Here are some of the areas that will be assessed:

- ✓ **Compliance with DoD policies.** Maintaining STIG or CIS Benchmarks compliance, which require you to harden around known vulnerabilities.
- ✓ **Vulnerability management.** Identifying, assessing, and mitigating vulnerabilities across your systems and networks.
- ✓ **Threat intelligence.** Implementing robust logging and monitoring systems to detect suspicious activity, thwart potential breaches and stay ahead of emerging threats.
- ✓ **Continuous monitoring and remediation.** Conducting real-time scanning, remediation and monitoring of vulnerabilities.
- ✓ **Report maintenance.** Creating custom reports on your security processes and posture.
- ✓ **Network security.** Establishing a perimeter security model with strong access control and user training. We suspect this expectation will turn to Zero Trust in a few years.
- ✓ **Continuous improvement.** Developing a practice of ongoing improvement and taking a proactive stance to get ahead of threats.
- ✓ **Incident response plan.** Knowing and exercising what you're going to do in case of attack.

DoD leaders recommend AUTOMATION.

From the director of DISA to leaders at JFHQ-DoDIN, automation is recommended wherever possible. SteelCloud's ConfigOS has been proven over a decade within the DoD to automate STIG compliance and enable continuous compliance and robust reporting. ConfigOS's DashView makes continuous monitoring possible, and the application integrates with other service tools like STIG Viewer, eMASS, Xacta, Splunk, and ServiceNow.

Requirements you can AUTOMATE:

- ✓ Compliance with DoD policies
- ✓ Vulnerability management
- ✓ Threat intelligence
- ✓ Continuous monitoring and remediation
- ✓ Report maintenance

Requirements that need HUMAN intervention:

- ✓ Network security
- ✓ Continuous improvement
- ✓ Incident response plan

For more information on CORA

SteelCloud

20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**