Greenhorn’s Guide to All of the Assessment Types

Peak InfoSec

All of the Assessment Types

Table of Contents

Why “Greenhorn’s Guide”?

A Greenhorn is “an inexperienced or naive person.”[1] From the days of the early explorers of the North American continent to fresh troops entering combat for the first time, the term was used to describe those who tend to get themselves killed in by doing “dumb” stuff.

Our “Greenhorn’s Guides” are meant to help educate and keep the reader from doing stupid ####.

This guide is NOT meant to be an exhaustive fount of wisdom for everything Controlled Unclassified Information (CUI), Cybersecurity Maturity Model Certification (CMMC) and NIST SP 800-171 under the sun.

Greenhorn Survival Tips

Key Point, Business Rule, et al

Fire to a greenhorn and an “old-timer” is life in the wilderness. We will use callout like the box to the left to signify critical things greenhorns should remember.

Department of Defense (DoD) Guidance

Given the majority of the CUI Greenhorn’s are going to be working with DoD’s Covered Defense Information (CDI), the guide will highlight DoD differences or pointers using a purple box with DoD logo and related guidance.

DoD guidance is…

[1] C.f., https://www.merriam-webster.com/dictionary/greenhorn

All of the Assessment Types

A Conformity Assessment???

What is an assessment? If your organization is involved in NIST SP 800-171 and CMMC, you will notice the ecosystem refers to everything as assessments of one type or another. This can become very confusing trying to keep all the different types straight.

The point of this whitepaper is to add clarity to this space. In doing so, we will explain all of the assessment types and what they mean within Peak InfoSec and the rest of the CMMC ecosystem.

Why is it called a Conformity Assessment?

Reviews of an organization's compliance are called assessments because the DoD has directed all authorized CMMC 3rd Party Assessment Organizations (C3PAO) to get certified In Accordance With (IAW) International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17020:2012, Conformity Assessment — Requirements for the operation of various types of bodies performing inspection.

Why? Per DoD, the Authorized C3PAO will be the Certifying body attesting to your compliance to, or more properly, conformity to, NIST SP 800-171 and other specified DoD requirements.

This is why all formal assessments are properly called Conformity Assessments.

This now brings in ISO's definition of Conformity Assessments:

> *"The process of conformity assessment demonstrates whether a product, service, process, claim, system or person meets the relevant requirements. Such requirements are stated in standards, regulations, contracts, programmes, or other normative documents."*
>
> *ISO - Conformity assessment*

NIST's Definition of Assessments

NIST and ISO/IEC have a love/hate relationship and copy one another and then spin the definition. NIST has done the same thing with Conformity Assessment.

> *"The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization."*
>
> *assessment - Glossary | CSRC (nist.gov), NIST SP 800-171 R3*

We do need to explain the part about "*testing or evaluation of security controls … with respect to meeting the security requirements.*"

NIST SP 800-171 and SP 800-172 establish the Security Requirements for components that process, store or transmit CUI or the components used to protect CUI per 32 CFR Part 2002, Controlled Unclassified Information (CUI). When a Security Requirement is implemented, it becomes a Security Control.

So, in the context of CUI for contractors, a tailored definition of an Assessment is:

> *"The testing or evaluation of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for the non-Federal organization's information system."*

You can see the underlined text changes we made in the tailored version. Why these changes?

- a non-Federal organization: Everything being covered is about a non-Federal organization because NIST SP 800-171 only applies to non-Federal organizations.
- NIST SP 800-171: 32 CFR 2002.14(h)(2) specifies "NIST SP 800-171 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part."
- Federal Agency specified: The prior citation covers basic CUI. By definition, every CUI Category is CUI Specified when under a DoD contact because DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, adds specified security requirements (e.g., FedRAMP Moderate or higher cloud services).
- the non-Federal organization's information system: Simply, because we are assessing your contractor information system. We need to emphasize *Information* here because protecting CUI under NIST SP 800-171 is Information-centric, whether is it is on Information Technology component or not. In short, wherever the information flows, that defines the scope.

DoD's Definition of an Assessment

From §170.4, Acronyms and definitions, of the Draft 32 CFR Part 170 Cybersecurity Maturity Model Certification (CMMC) Program rule, we find DoD's derivative definition:

> *"Assessment means the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization, as defined in § 170.15 to § 170.18. (CMMC-custom term)"*
>
> *https://www.federalregister.gov/d/2023-27280/p-1030*

DoD's term simply adds to NIST's definition the additional references to CMMC Levels:

- §170.15, CMMC Level 1 Self-Assessment and Affirmation requirements.
- §170.16, CMMC Level 2 Self-Assessment and Affirmation requirements.
- §170.17, CMMC Level 2 Certification Assessment and Affirmation requirements.
- §170.18, CMMC Level 3 Certification Assessment and Affirmation requirements.

While the CMMC Ecosystem operates under the auspices of ISO/IEC 17020:2012 for conducting Conformity Assessments for certifications, we will use the DoD's definition going forward in this whitepaper because that is the formal Regulatory definition.

Types of Assessments for CMMC & NIST SP 800-171

Department of Defense Specific Assessments

DoD conducts its own types of assessments. For these next three assessments, DoD and, specifically the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), follows the NIST Definition.

DIBCAC Medium Assessments

A DIBCAC Medium Assessment is a non-voluntary Examination-only assessment of a DoD contractor. DIBCAC normally calls on a Monday morning and tells the contractor they have until close of business on Friday to provide copies their of System Security Plan (SSP) and all related evidence. No interviews or tests will be conducted by DIBCAC.

A DIBCAC Medium Assessment is then scored and will result in DIBCAC entering a DoD Assessment Methodology (DoDAM) score in the Supplier Performance Risk System (SPRS) for the contractor.

All of the Assessment Types

DIBCAC Medium Assessments can generate negative contracting reviews and corrective actions as deficiencies are fed to the contractor's contracting officers.

DIBCAC High Assessments

Like a DIBCAC Medium Assessment, a DIBCAC High Assessment is also non-voluntary but is generally conducted onsite and involves examination, interviews, and testing "to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements."

Likewise, this also generates a SPRS entry by DIBCAC and can lead to negative contracting follow-up actions.

Joint Surveillance Voluntary Assessments (JSVA)

A JSVA is a voluntary DIBCAC lead High Assessment where the contractor hires an Authorized C3PAO to conduct the assessment and provide the results to DIBCAC. DIBCAC is the final arbiter of conformity and the best way to understand the C3PAO's and their staff's role is they are "deputized" DIBCAC auditors.

While JSVAs tend to be more lenient by DIBCAC, a JSVA generates a SPRS entry by DIBCAC and can still lead to negative contracting follow-up actions.

JSVA's will cease to exist when the CMMC Program begins and C3PAOs are conducting formal Certification Assessments.

Self-Assessments

DoD's definition of Assessments includes three sub-definitions, of which one includes Self-Assessments. Per DoD,

> *"(i) Self-Assessment is the term for the activity performed by an entity to evaluate its own CMMC Level, as applied to Level 1 and some Level 2."*

In this case, DoD expects the organization's self-assessment to be used for their submission into SPRS. Organizations may do multiple self-assessments prior to submitting in SPRS because Plans of Action & Milestones (POA&M) are not allowed at all for Level 1 while Level 2 has very limited POA&M eligible Security Requirements under NIST SP 800-171.

Merging all of this together, our Self-Assessment definition is:

> *"A Self-Assessment means the organization conducts the testing or evaluation of its security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for the organization's information system."*

Certification Assessments

The term Certification Assessment is another pair of sub-definitions created by DoD in the DRAFT 32 CFR Part 170, CMMC Program. Specifically,

> *"(ii) CMMC Level 2 Certification Assessment is the term for the activity performed by a C3PAO to evaluate the CMMC Level of an OSC.*
>
> *(iii) CMMC Level 3 Certification Assessment is the term for the activity performed by the Department of Defense to evaluate the CMMC Level of an OSC."*

All of the Assessment Types

To be technically clear, a Certification Assessment is a Conformity Assessment that may result in the assessing organization issuing a certificate. Failure to meet POA&M thresholds means that an organization is not eligible for a conditional certificate and a final certificate can only be issued when all Security requirements are met. Bringing the definition back together we get:

> *"A Certification Assessment means a 3rd party organization conducts the testing or evaluation of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for CMMC Level 2 and NIST SP 800-172 for CMMC Level 3 for the non-Federal organization's information system. The results of a Certification Assessment are reported to DoD."*

Gap Assessments

Gap Assessments are nearly synonymous to a Self-Assessment. The only distinction is, in our consideration, a Gap Assessment is done by a 3rd Party. So, tailoring the Self-Assessment definition, we would get:

> *"Gap Assessment is the term for the activity performed by a 3rd party entity to evaluate an organizations CMMC Level, as applied to Level 1 and some Level 2."*

That is clunky and inconsistent, so, our definition is:

> *"A Gap Assessment means a 3rd party organization conducts the testing or evaluation of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for the non-Federal organization's information system. In a Gap assessment, the 3rd party organization may provide consultative advice on how to remediate deficiencies."*

Mock Assessments

A Mock Assessment is the same as a Certification Assessment except the results are not submitted to DoD. Our definition for a Mock Assessment is:

> *"A Mock Assessment means a 3rd party organization conducts the testing or evaluation of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for CMMC Level 2 and NIST SP 800-172 for CMMC Level 3 for the non-Federal organization's information system. The results of a Certification Assessment are not reported to DoD."*

Conformity Assessment Readiness Review (CARR)

The CARR is, per the old CMMC Assessment Procedure:

> *"is to determine whether the assessment team and OSC (host unit, supporting functional units and any enclaves) are ready to conduct the assessment as planned, and in the time allocated. The readiness review addresses several aspects of readiness to conduct the assessment, which include at a minimum: OE readiness, assessment team readiness, logistics readiness, assessment risk status, and overall assessment feasibility. The readiness review results in a decision to continue as planned, replan or reschedule, or cancel the assessment. The Certified Assessor and Assessment Sponsor are*

> *responsible for identifying and recording the criteria that will determine whether an assessment will proceed, but that criteria must be reviewed and approved by the C3PAO and AB."*
>
> *CMMC Assessment Method, Version 2.0_Baseline, Para 1.3.3*

While the intent remains the same, we also assess 12 NIST SP 800-171 Security Requirements during the CARR. These are critical requirements that if you fail these, they cause cascade issues with all of the other Security Requirements.

By doing this, we can help the Organization Seeking Certification (OSC) know if they are truly ready or if it makes sense to defer the assessment. In short, this is a risk mitigation before the OSC invests lots more money during the later phases of the Certification Assessment.

We expect the CARR to remain in the new CMMC Assessment Procedure (CAP) that will replace the current draft CAP, which was to supersede the CMMC Assessment Method above.

Our definition of a CARR is:

> *"A Conformity Assessment Readiness Review (CARR) means a 3rd party organization conducts the testing or evaluation of a limited set of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for CMMC Level 2 and NIST SP 800-172 for CMMC Level 3 for the non-Federal organization's information system. The results of a CARR are not reported to DoD and are used as a milestone decision point prior to entering into the full-scope Certification Assessment."*

Assessment Types Quick Reference Table

Assessment Type	Conducted Internally	Conduct by a 3rd Party	Recommendations Provided	Reported to DoD	Includes all 110 Security requirements + Specifications	Limited # of Requirements
Self-Assessment *A Self-Assessment means the organization conducts the testing or evaluation of its security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for the organization's information system.*	P		P		P	

All of the Assessment Types

Assessment Type	Conducted Internally	Conduct by a 3rd Party	Recommendations Provided	Reported to DoD	Includes all 110 Security requirements + Specifications	Limited # of Requirements
Certification Assessment *A Certification Assessment means a 3rd party organization conducts the testing or evaluation of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for CMMC Level 2 and NIST SP 800-172 for CMMC Level 3 for the non-Federal organization's information system. The results of a Certification Assessment are reported to DoD.*		P		P	P	
Gap Assessment *A Gap Assessment means a 3rd party organization conducts the testing or evaluation of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for the non-Federal organization's information system. In a Gap assessment, the 3rd party organization may provide consultative advice on how to remediate deficiencies.*		P	P		P	
Mock Assessment *A Mock Assessment means a 3rd party organization conducts the testing or evaluation of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for CMMC Level 2 and NIST SP 800-172 for CMMC Level 3 for the non-Federal organization's information system. The results of a Certification Assessment are not reported to DoD.*		P			P	
Certification Assessment Readiness Review (CARR) *A Conformity Assessment Readiness Review (CARR) means a 3rd party organization conducts the testing or evaluation of a limited set of a non-Federal organization's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the NIST SP 800-171 and Federal Agency specified security requirements for CMMC Level 2 and NIST SP 800-172 for CMMC Level 3 for the non-Federal organization's information system. The results of a CARR are not reported to DoD and are used as a milestone decision point prior to entering into the full-scope Certification Assessment.*		P				P

Revisions

Date	Revision
31 May 2024	Initial Publication of the whitepaper. Corrections and suggestions can be submitted to cmmc@peakinfosec.us.

Acronyms

C3PAO	CMMC 3rd Party Assessment Organization
CAP	CMMC Assessment Procedure
CARR	Conformity Assessment Readiness Review
CFR	Code of Federal Regulations
CUI	Controlled Unclassified Information
CDI	Covered Defense Information
CMMC	Cybersecurity Maturity Model Certification
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
DoDAM	DoD Assessment Methodology
EO	Executive Order
FCI	Federal Contract Information
IAW	In Accordance With
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
JSVA	Joint Surveillance Voluntary Assessments
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OSC	Organization Seeking Certification
SP	Special Publication
SPRS	Supplier Performance Risk System
SSP	System Security Plan