GRC Platforms Within the CMMC Boundary

What the Compliance Tool Holds, Why It Is in Scope, and What the Cloud Rule Requires of the Specific Offering

David W. Koran
CyberAB Registered Practitioner Advanced
May 27, 2026

The Tool Bought to Prove Compliance

A defense manufacturer subject to CMMC will, at some point, adopt a system specifically to manage the program: the governance, risk, and compliance (GRC) platform. Of all the systems brought into a contractor's CMMC boundary, this one is the least examined.

In the past year, nearly every major compliance-automation platform has added a CMMC module, and the category is marketed as the path to certification. “Connect your systems, collect evidence automatically, generate the System Security Plan and the Plan of Action and Milestones, and watch a dashboard report your readiness”. The platform is sold as the solution that produces compliance. The question this paper asks is the one that marketing does not. What is the tool itself within the contractor's CMMC environment, what does it hold, and what does the framework require of it? The answers place the GRC platform within the assessment scope rather than outside it, and they make the choice of platform and the custody of its data matters that the contractor cannot delegate to a vendor's sales page. The CMMC program, codified at 32 CFR Part 170 and effective December 16, 2024, requires that the 110 security requirements of NIST Special Publication 800-171 Revision 2 be demonstrated through a Level 2 assessment.

What the Platform Actually Holds

To do its work, a GRC platform requires a detailed, up-to-date description of the contractor's security environment. It holds the System Security Plan, the asset inventory, the network and data-flow descriptions, the implementation status of each control, the results of vulnerability scans, and the Plan of Action and Milestones, which is the running record of every requirement not yet met. Taken together, it is a single, structured, continuously updated account of how the contractor's environment is defended, and in the Plan of Action and Milestones, precisely where the defense is incomplete.

The CMMC framework has a name for this kind of information. It is Security Protection Data, and the scoping guidance defines it as data stored or processed by security protection assets that is used to protect the assessed environment, and as security-relevant information that, if disclosed, could aid an attacker in compromising the system. The definition is the scoping guide's own, and what it describes is what a GRC platform actually holds. The tool a contractor adopts to demonstrate its security holds, in one place, the information that would most help an adversary defeat it.

Security Protection Data and the Asset It Sits On

Because the platform stores Security Protection Data and provides security and compliance functions, it falls within the scope of the assessment. The CMMC scoping guidance, and 32 CFR 170.19, sort every asset in the environment into categories, and the category that fits a GRC platform is the Security Protection Asset, an asset that provides security functions or capabilities for the CUI environment, even when it does not itself process CUI. The guidance provides an example of an external service that provides security information and event management capabilities. It may be logically separated and may never touch CUI, yet it contributes to meeting the requirements and is therefore within scope. A GRC platform that holds the System Security Plan, the scan results, and the Plan of Action and Milestones is the same case.

A Security Protection Asset is part of the CMMC Assessment Scope. It is assessed against the Level 2 requirements relevant to the capability it provides, and it must be listed in the asset inventory, described in the System Security Plan, and shown in the network and data-flow diagrams. Where the platform holds security-relevant data used to protect the assessed environment or manages the contractor's CMMC implementation status, it should not be treated as a Contractor Risk Managed Asset or an out-of-scope asset, as it performs a security-protection function within the assessment scope. The common error is to assume the opposite: that because the platform sits outside the contractor's network or does not hold CUI, it is out of scope. The scoping guidance explicitly states that an asset providing security protection for the CUI environment is not out of scope. The tool is within the boundary.

Whether the Tool Holds CUI Changes the Requirement

How far the requirement goes turns on what the contractor puts into the platform. Security Protection Data is not automatically CUI. It may be highly sensitive, security-relevant information without being CUI itself. A platform that holds only the System Security Plan, the inventory, the scan output, and the Plan of Action and Milestones is a Security Protection Asset, in scope and assessed and documented, but the cloud rule that requires FedRAMP authorization for a service holding CUI is not automatically triggered by Security Protection Data alone. The contractor remains responsible for protecting that data, and the external provider must be evaluated and

documented, but the strict FedRAMP threshold attaches when covered defense information is present.

The moment CUI enters the platform, the answer changes. If a contractor uploads evidence containing CUI, a screenshot of a controlled drawing, an exported configuration that includes controlled technical data, or a document bearing a CUI marking, and that information constitutes covered defense information under the contract, then the vendor's cloud service offering stores or processes that information. In that case, DFARS 252.204-7012, at paragraph (b)(2)(ii)(D), requires the contractor to ensure the cloud service provider meets security requirements equivalent to the FedRAMP Moderate baseline, which means the specific offering must be FedRAMP Moderate authorized or meet FedRAMP Moderate equivalency. The classification of the tool and the weight of the requirement, therefore, depend on a decision most contractors never make deliberately: what they allow to be loaded into it. A platform used with discipline as a Security Protection Asset and a platform used to store CUI-bearing evidence are two different assets under the framework, even when they are the same product.

A contractor can keep the platform in the Security Protection Asset lane deliberately rather than by accident. Prohibiting CUI-bearing evidence from being uploaded to the platform and documenting that restriction in procedure, in training, and in the evidence-handling rules holds the tool to a lighter classification and prevents the cloud rule from attaching. The alternative, allowing CUI-bearing evidence into a platform that does not meet the FedRAMP standard, converts a useful Security Protection Asset into a noncompliant CUI repository, and does so quietly, because nothing in the product prevents it.

The Specific Offering Is the Test

Where the cloud rule does attach, the test is the one established for any hosted service, and the GRC market makes the test necessary because it is not uniform. Some compliance-automation vendors now offer dedicated government or FedRAMP-authorized offerings. Others sell commercial software that relies on FedRAMP-authorized infrastructure underneath, which describes the cloud the platform runs on rather than an attestation for the offering itself, a platform-versus-offering gap that arises with any hosted service. And most commercial GRC offerings run in commercial cloud, which is a mismatch for a contractor whose CUI architecture is in a government cloud. These are not the same thing, and a CMMC module in the product is not a statement about any of them.

The conclusion is the same as for any cloud service that may hold CUI. The contractor verifies the specific offering it uses, not the vendor's separate government product, and not the infrastructure beneath it, by confirming a FedRAMP Marketplace authorization or obtaining the third-party equivalency body of evidence together with the customer responsibility matrix. A vendor that markets a CMMC module has told the contractor what the tool does. It has not told the contractor whether the specific offering it sells is a place where CUI may lawfully sit.

The GRC platform is in scope

Point	What it means
The platform is in scope	A GRC tool that holds the SSP, scan results, and POA&M is a Security Protection Asset within the CMMC Assessment Scope, as documented in the inventory, the SSP, and the diagrams.
What you load into it sets the requirement.	Security Protection Data keeps it a Security Protection Asset. CUI-bearing evidence may make the platform a CUI asset and, where the CUI is covered defense information under the contract, triggers the DFARS 252.204-7012 cloud-service requirement.
Verify the specific offering.	A Marketplace authorization or a third-party equivalency package for the offering the contractor actually uses, not the vendor's separate government product or the underlying infrastructure.

The Custody of the Description

What a GRC platform holds is itself a reason for concern, and the framework's own definition is the basis for that concern. Security Protection Data is, in the words of the scoping guidance, information that, if disclosed, could aid an attacker in compromising the system. A GRC platform aggregates that information for an entire environment into one external, hosted, continuously updated place, and across a vendor's customer base, it concentrates the same kind of data for many contractors at once. None of this implies that any particular vendor is unsafe. It means that the custody of the platform deserves the same consideration the contractor would give to any store of security-relevant data: who operates the service, where it is hosted, who on the vendor's side can reach the contractor's tenant, what the customer responsibility matrix assigns back to the contractor, and whether the specific offering meets the standard the data calls for. The tool built to demonstrate that an environment is defended is also the most efficient

description of how it might be defeated, and that quality is a reason to choose and govern it deliberately rather than to adopt it because it is marketed for CMMC.

The Dashboard Is Not the Boundary

A GRC tool organizes evidence, tracks status, and produces documentation. It does not implement controls. It records the implementation the contractor performs, and a green dashboard reports what has been entered, not what an assessor will find. A contractor that reads readiness from the dashboard without the underlying implementation has the readiness-wall problem, the gap between a tidy record and a defensible environment that surfaces when a pre-assessment begins. The platform is also built, in most cases, for continuous monitoring against many frameworks, and the contractor must ensure the tool is configured to enforce the CMMC-specific Plan of Action and Milestones rules, the limited set of requirements eligible for a plan of action, the strict 180-day closure window, and the conditional-status threshold, which standard commercial configurations do not always enforce out of the box. The tool is useful for keeping evidence organized and up to date. It is not a substitute for the implementation it records or for the judgment that determines whether the environment is actually ready.

What the Platform Can Prove About the Evidence

A related judgment concerns the evidence itself. The platform can demonstrate that an artifact has not changed since it was uploaded. It cannot demonstrate that the artifact accurately reflects the source system at any point in time. The integrity claim is post-upload and file-level, and a screenshot, a configuration export, or an attestation is a record produced at a single point in time, not a continuous reflection of the system.

Two gaps follow from this. The first is the pre-ingestion gap. The platform's chain of custody begins at the moment of upload, so the artifact may have been cropped, edited, or captured in a state the source system was not actually in, and the hash computed at upload cannot reach back to verify any of that. The second is the source-divergence gap. The system continues to change after the artifact is captured, and a record preserved exactly inside the platform says nothing about whether the underlying configuration still matches it.

The strongest evidence at assessment remains the live configuration or output at the source system, and the platform's value is as an index of where that evidence sits rather than as a substitute for it. A contractor that organizes the platform to direct assessors to

the source systems uses the tool to its greatest effect. A contractor that treats the platform as the authoritative evidence repository asks the assessor to trust an indirection that the platform cannot resolve.

A Diagnostic Sequence

The place of a GRC platform within the boundary can be worked out in sequence. The following moves from what the tool holds, through its classification and the cloud rule, to custody and the dashboard.

Working through the compliance platform

Question	What it determines
Does the platform hold the SSP, asset inventory, scan results, or POA&M?	If it does, it holds Security Protection Data and is a Security Protection Asset within scope.
Is the platform in the asset inventory, the SSP, and the network and data-flow diagrams?	This documentation is required for a Security Protection Asset.
Does the contractor load evidence that contains CUI into the platform?	If it does, the platform may become a CUI asset and, where the CUI is covered defense information under the contract, the DFARS 252.204-7012 cloud-service requirement attaches.
For the specific offering in use, is there a FedRAMP Marketplace authorization or a third-party equivalency package?	This is the cloud-rule test in which CUI is present and verified for the offering, not the infrastructure.
Has the contractor obtained and read the customer responsibility matrix?	It defines what the vendor operates and what the contractor retains.
Who operates the platform, who can access it, and where is it hosted?	The custody of Security Protection Data is a diligence item in its own right.
Does the dashboard reflect implemented controls, or only entered records?	A record is not an implementation, and the assessor evaluates the latter.
Does the platform model the CMMC POA&M rules correctly?	Eligibility, the closure window, and the conditional threshold are CMMC-specific.

The System Security Plan and the Evidence Behind It

The placement of a GRC platform within the boundary is part of the System Security Plan content. The plan lists the platform in the asset inventory, classifies it as a Security Protection Asset or, where it holds CUI, as a CUI asset, shows it in the network and data-flow diagrams, and records the verification of the specific offering and the customer responsibility matrix. The evidence supporting the plan includes the offering's FedRAMP authorization or equivalency package, the responsibility matrix, the platform's access and configuration records, and the contractor's determination of what may be loaded into it.

The determination rests on that evidence rather than on the vendor's description of the product. A GRC platform can be a legitimate and useful part of a CMMC program. It is not, by its presence, evidence of compliance, and it is not, by default, outside the boundary it is brought to help manage. The contractor that treats the platform as an asset to be classified, verified, and governed, rather than as a result to be purchased, has placed it correctly and can account for it in the assessment.

The Evidence Package

Because the determination rests on evidence, it helps to know in advance what that evidence consists of. The following items are the records a contractor assembles to account for a GRC platform within the boundary.

Evidence for the compliance platform

Evidence	What it supports
SSP entry listing the platform and classifying it as a Security Protection Asset or CUI asset	Scope and security planning
Asset inventory, network, and data-flow diagrams showing the platform	Required documentation for a Security Protection Asset
Determination of what data and evidence the contractor permits on the platform	Whether the cloud rule attaches
FedRAMP Marketplace authorization or a third-party equivalency body of evidence for the specific offering	The cloud rule where CUI is present

Customer responsibility matrix for the platform	The division of implementation between the vendor and the contractor
Access and configuration records for the platform	Assessment of the Security Protection Asset
Records showing controls are implemented, not only recorded	The gap between the dashboard and the environment

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced, and the founder of David Koran and Associates. He helps aerospace and defense manufacturers implement CMMC across systems, service providers, and tools that hold or protect CUI, and bring difficult environments into compliance. He is the author of The CMMC Decision and can be reached at dkoran@davidkoran.com and (802) 335-2662.

References

Cybersecurity Maturity Model Certification (CMMC) Program, 32 CFR Part 170, Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

CMMC Scoping, 32 CFR 170.19, Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-D/section-170.19

CMMC Assessment Scope, Level 2, Department of Defense Chief Information Officer. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2v2.pdf

NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

CMMC Acronyms and Definitions, 32 CFR 170.4, Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170/subpart-A/section-170.4

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, paragraph (b)(2)(ii)(D), Acquisition.gov. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting

FedRAMP Authorization and Equivalency, Cloud Requirements for the Defense Industrial Base, Department of Defense Chief Information Officer, February 2025. https://dodcio.defense.gov/Portals/0/Documents/CMMC/FedRAMP-AuthorizationEquivalency.pdf

FedRAMP Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings, Department of Defense Chief Information Officer, December 21, 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf

FedRAMP Marketplace, Federal Risk and Authorization Management Program. https://marketplace.fedramp.gov/