CIMCOR

TABLE OF CONTENTS

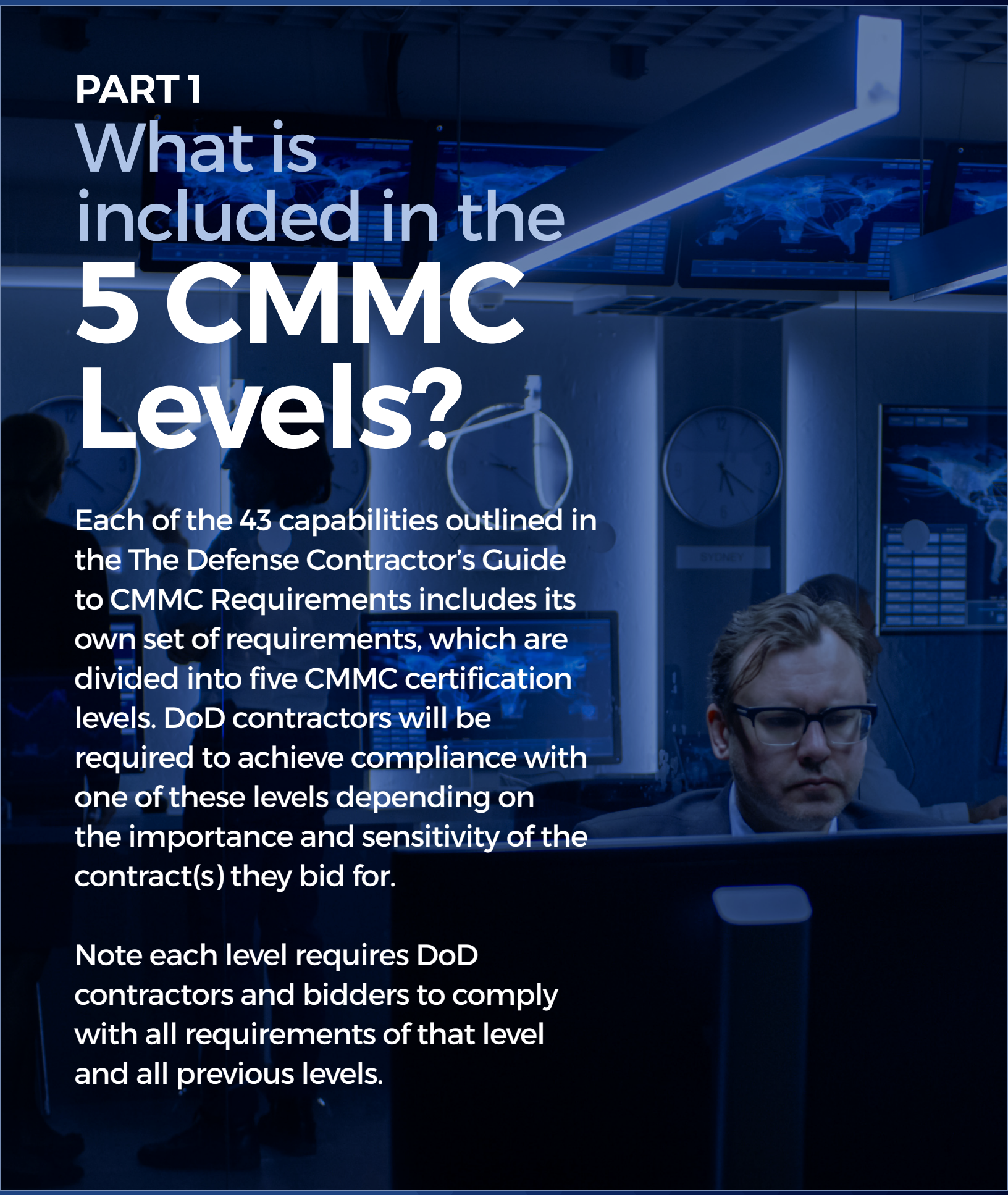
The Defense Contractor's Guide to CMMC Requirements

After years of self-assessing readiness against NIST 800-171, defense contractors are in for a change.

The DoD's new CMMC requirements are most comprehensive required by any security maturity model, including those issued by NIST, ISO, and CIS. They also require DoD contractors to pass an external assessment process, carried out by a Certified 3rd-Party Assessor Organization (C3PAO).

For defense contractors, meeting these new requirements ahead of the CMMC certification deadline will be a top priority.

DOMAIN	CAPABILITY
ACCESS CONTROL (AC)	» Establish system access requirements » Control internal system access » Control remote system access » Limit data access to authorized users and processes
ASSET MANAGEMENT (AM)	» Identify and document assets » Manage asset inventory
AUDIT AND ACCOUNTABILITY	» Define audit requirements » Perform auditing » Identify and protect audit information » Review and manage audit logs
AWARENESS AND TRAINING (AT)	» Conduct security awareness activities » Conduct training
CONFIGURATION MANAGEMENT (CM)	» Establish configuration baselines » Perform configuration and change management
IDENTIFICATION AND AUTHENTICATION (IA)	» Grant access to authenticated entities
INCIDENT RESPONSE (IR)	» Plan incident response » Detect and report events » Develop and implement a response to a declared incident » Perform post incident reviews » Test incident response
MAINTENANCE (MA)	» Manage maintenance
MEDIA PROTECTION (MP)	» Identify and mark media » Protect and control media » Sanitize media » Protect media during transport
PERSONNEL SECURITY (PS)	» Screen personnel » Protect CUI during personnel actions
PHYSICAL PROTECTION (PE)	» Limit physical access
RECOVERY (RE)	» Manage backups » Manage information security continuity
RISK MANAGEMENT (RM)	» Identify and evaluate risk » Manage risk » Manage supply chain risk
SECURITY ASSESSMENT (CA)	» Develop and manage a system security plan » Define and manage controls » Perform code reviews
SITUATIONAL AWARENESS (SA)	» Implement threat monitoring
SYSTEMS AND COMMUNICATIONS PROTECTION (SC)	» Define security requirements for systems and communications » Control communications at system boundaries
SYSTEM AND INFORMATION INTEGRITY (SI)	» Identify and manage information system flaws » Identify malicious content » Perform network and system monitoring » Implement advanced email protections



PART 1

What is included in the 5 CMMC Levels?

Each of the 43 capabilities outlined in the The Defense Contractor's Guide to CMMC Requirements includes its own set of requirements, which are divided into five CMMC certification levels. DoD contractors will be required to achieve compliance with one of these levels depending on the importance and sensitivity of the contract(s) they bid for.

Note each level requires DoD contractors and bidders to comply with all requirements of that level and all previous levels.

WHAT ARE THE CMMC LEVELS?

Level 1
PERFORMED

The first CMMC level requires DoD contractors to implement basic security controls needed for essential cyber hygiene. CMMC level 1 certification will be necessary for any organization bidding for (or currently holding) a DoD contract that requires them to store or process mildly sensitive information. This is likely to include Federal Contract Information (FCI) — anything higher in sensitivity will almost certainly require a higher level of CMMC certification. It is estimated that more than 90% of all Defense Industrial Base Sector (DIB) will need to achieve this level of certification in the immediate foreseeable future.

Level 2
DOCUMENTED

CMMC level 2 includes slightly more advanced controls in line with 'intermediate' cyber hygiene. As noted earlier, the combined requirements of CMMC certification levels 1 and 2 are very similar to those outlined in NIST 800-171. DoD contracts that require level 2 certification will see contractors hold or process FCI and potentially more sensitive Controlled Unclassified Information (CUI). Initial indication is that Level 2 is a requirements bridge for those DIB's needing to eventually meet Level 3.

Level 3
MANAGED

CMMC level 3 breaks new ground for DoD contractors, going above and beyond previous NIST requirements. This level requires contractors to achieve a moderate standard of cyber hygiene and is the first level to include requirements across all 43 CMMC capabilities. While the DoD has not yet made clear which level of certification will be required for different contracts, it seems likely that level 3 will be standard for the majority of DoD contracts that involve holding or processing CUI. It is estimated that 20k DIB's will need to achieve this level of certification.

Level 4
REVIEWED

Historically, compliance frameworks have mainly focused on protective and reactive controls. While they haven't necessarily been 'easy' to achieve (particularly for SMEs), the standard of security they mandate has rarely crossed over into 'advanced'.

CMMC level 4 bucks this trend by going beyond cyber hygiene and requiring contractors to take a proactive security approach. This includes requirements to proactively search for, track, identify, and block cyber threats, including those initiated by Advanced Persistent Threat (APT) groups.

Level 5
OPTIMIZING

Given that level 4 already broke new ground, CMMC level 5 goes far beyond anything required of DoD contractors in the past. Level 5 — which requires contractors to build and maintain a fully mature security function across all 43 CMMC capabilities — will undoubtedly be reserved for only the most important, sensitive, and high-profile DoD contracts.

For contractors required to achieve level 5 certification, the CMMC standard is no joke. It could take years to reach full CMMC compliance across all 43 capabilities, plus a substantial investment of time and resources. It is estimated that 3,500 DIB's will be required to meet levels 4 and 5 certifications.

How Will CMMC Readiness Be Assessed?

Up to now, DoD contractors have been allowed to self-assess their cybersecurity compliance against the NIST 800-171 framework. Unfortunately, as a DOD audit of 10 contractors in 2019 discovered, the self-assessment model wasn't working. In the auditors' own words:

"DoD contractors did not consistently implement DoD mandated system security controls for safeguarding Defense information. [...] As a result, the DoD does not know the amount of DoD information managed by contractors and cannot determine whether contractors are protecting unclassified DoD information from unauthorized disclosure."

What's going to take the place of the old self-assessment model? The Cybersecurity Maturity Model Certification Accreditation Body (CMMC AB).

The CMMC AB is the body set up to implement and administer the CMMC standard. In doing this, the body will assure the DoD that organizations holding or bidding on defense contracts meet the cybersecurity standards required.

To do this, the CMMC AB will train and appoint Certified 3rd-Party Assessor Organizations (C3PAOs). These CMMC C3PAOs will conduct physical, on-site audits for all current and prospective DoD contractors to ensure they meet each contract's CMMC requirements.

How To Self-Assess Readiness Against CMMC Requirements

Naturally, the first step to becoming compliant is to assess your readiness against the relevant CMMC level. The best way to do this is by conducting a gap analysis. In particular, your gap analysis should focus on the systems and processes your organization uses to store, process, and transmit CUI.

CMMC systems are divided into two categories: human systems and technical systems. Both need to be analyzed carefully to ensure they meet the requirements of the relevant CMMC level.

There are two ways to do this:
» Manually, using physical assessments, investigations, and analyses; and,
» Automatically, using scanning technologies.

As you'd expect, manual assessments are more appropriate for human systems, which automatic assessments are more suited to technical systems.

For human systems, consider funding an impartial assessment by an external party. It's easier for external CMMC assessors to provide a realistic evaluation of your existing systems, which should help to avoid unpleasant surprises when the real audit is completed.

Technical non-compliance issues can be challenging and time-consuming to find manually and can easily fall out of compliance at any time with normal use. For this reason, an automated CMMC software solution is more appropriate for assessing the readiness of technical systems. It's also faster and more thorough than a human audit.

Prepare for CMMC with CimTrak

The timeline to meet CMMC requirements is tight. Version 1.0 of the CMMC framework has already been released, and even organizations that currently hold DoD contracts will need to reach full compliance within just 2-3 years. While that may sound like ample time to adjust, it poses a significant challenge—particularly for organizations that hold sensitive or high-profile DoD contracts.

CimTrak is an IT integrity, security, and compliance tool that helps organizations quickly improve their cybersecurity maturity. CimTrak continuously monitors your environment and detects changes to assets, files, and accounts. When specified changes occur, CimTrak raises an alert and a report, making it easy to identify security issues in hardware and software assets. Crucially, CimTrak's functionality maps directly to many of the control objectives of CMMC version 1.

ADDITIONAL RESOURCES

» CMMC Solution Brief
» CimTrak Compliance Module
» NIST Solution Brief
» How to Prepare for a CMMC Audit
» Top 10 Things to Know About CMMC
» CMMC: Cybersecurity Standards for DoD

CIMTRAK

Innovative, next-generation, file and system integrity monitoring software, securing your infrastructure.
Get compliant and stay that way.

PART 2

How to reach CMMC Compliance

CMMC is the new security framework for DoD contractors. The DoD created the framework to ensure defense contractors have adequate controls in place to protect Controlled Unclassified Information (CUI).

Version 1.0 of the CMMC framework was published in January 2020 and will be phased in gradually for all defense contractors over the next 2-3 years. So, what is CMMC compliance all about?

What is CMMC Compliance?

Unlike the old self-assessment system based on NIST 800-171, achieving CMMC compliance requires contractors to undergo a physical audit from a CMMC C3PAO (Certified 3rd Party Assessor Organization).

Why the change?

The DoD was compelled to create CMMC after a 2019 audit of 10 DoD contractors found that contractors *"...did not consistently implement DoD mandated system security controls for safeguarding Defense information."* This lack of genuine compliance was felt in the real world when several prominent DoD contractors suffered high-profile breaches.

While CMMC requires DoD contractors to reach a higher level of cybersecurity maturity than previous frameworks, that's not to say it's completely different. The first two (of five) CMMC certification levels are heavily based on NIST 800-171. So, DoD contractors that don't process highly sensitive information should already have many of the controls in place — so long as they have assessed their readiness thoroughly.

How To Reach CMMC Compliance

Over the next few years, achieving compliance with CMMC version 1 will be a top priority for defense contractors. While it may be years before the framework is implemented fully, that isn't a lot of time to implement all of the security measures required for compliance. The caveat to understand is that a CMMC certification is based on passing 100% of the requirements. Anything short of that will prevent a prime or sub-contractor to bid and be awarded a contract.

Fortunately, reaching compliance doesn't have to be complicated. We've outline six steps that can achieve compliance ahead of the CMMC certification deadline.

Step 1
GET STARTED STRAIGHT AWAY

CMMC is already a requirement for some of the new DoD contracts and will be phased in for all contracts within the next 2-3 years. If your organization plans to bid on new DoD contracts, you could potentially need to reach CMMC compliance in a matter of weeks or months depending upon the DoD contract.

So, the first thing to realize about CMMC is: **start now** now if you plan on bidding on DoD contracts. CMMC is by far the most stringent security maturity model released to date, so reaching compliance will be far from easy — particularly if your organization needs to reach CMMC level 3 or higher.

Unlike the old NIST self-assessment model, 'rushing through' a compliance initiative isn't going to work with CMMC. Your organization must build a mature cybersecurity function across up to 43 security capabilities to reach full compliance. Unless your cybersecurity program is already highly mature, this is probably not something you can achieve overnight.

The official line from the CMMC Accreditation Body (CMMC AB) is that contractors should prepare for their audit at least six months in advance. Realistically, however, many contractors are likely to need at least a year to prepare fully, and possibly much longer.

Step 2

DETERMINE YOUR CUI ENVIRONMENT

One critical point to keep in mind about CMMC compliance is that it doesn't necessarily cover all of your systems, assets, and processes. It only covers those that are directly or indirectly involved with the storage, processing, or transmission of Controlled Unclassified Information (CUI). Cumulatively, all of your systems that meet these criteria form your 'CUI environment.'

So, how do you determine what your CUI environment covers? If your organization is a DoD contractor, your DoD contracting official will decide. If you're a subcontractor, your prime contractor will decide on behalf of the DoD. With that said, in practice, you can determine the scope of your CUI environment either using an internal assessment or by working with a professional service provider. While the latter certainly adds cost, it may be the safer option.

Step 3

ASSESS YOUR READINESS AGAINST THE CMMC FRAMEWORK

The first step to complying with CMMC requirements is to complete a readiness assessment and gap analysis. After all, you can't create an action plan without knowing where you currently stand. Since protecting CUI is the primary purpose of CMMC, your assessment should focus on how and where CUI is stored, processed, and transmitted.

For human systems, you may find it beneficial to have an impartial assessment completed by an external CMMC assessor. This approach is more realistic than conducting your assessment in-house, which mitigates the possibility of unpleasant surprises when it comes to the real CMMC audit.

For technical systems, an automated scanning solution drastically reduces the labor required to identify gaps and removes the risk of human error. Technical gaps can be tough to find manually and can easily be reintroduced without anybody noticing. Technologies like File Integrity Management (FIM) solutions avoid these issues by continually scanning your CUI environment for changes and raising an alert when detecting a non-compliance issue.

Step 4

IDENTIFY STEPS TO COMPLY WITH CMMC CONTROLS

Once you have identified where your gaps lie, the next step is to identify the steps needed to reach CMMC compliance. During this process, you should also estimate the time and cost needed to resolve each gap.

At this point, you'll begin to see how the CMMC framework changes the cost/benefit analysis of working for the DoD. CMMC mandates an ambitious level of cyber maturity. However, if your existing cybersecurity program is relatively mature — and the contracts you're bidding on don't involve highly sensitive information — it's likely achieving compliance with CMMC controls won't be too arduous. On the other hand, if your program falls substantially short of where it needs to be, the case may not be so clear.

There's no doubt that achieving compliance will be more challenging than it was in the past. Some estimates place the cost of reaching compliance with CMMC level 3 at up to $250,000 — or even more.

Step 5

CREATE A CMMC COMPLIANCE ROADMAP

The next step is to create a remediation roadmap based on the priorities and costs you've calculated. Once again, the key here is to get moving as quickly as possible.

Bear in mind that — at level 5 — CMMC includes 171 practices and 85 processes, spread across 43 security capabilities. While most contractors won't need to comply with all of these, level 3 still consists of 130 practices and 51 processes. Reaching compliance with all of these requirements is a significant endeavor, no matter how mature your cybersecurity program is.

Reaching full compliance with CMMC — particularly levels three and above — could easily take years even for organizations with reasonably mature cybersecurity programs. So, while most contractors can expect at least a couple of years' grace before CMMC becomes a binding requirement, there isn't any time to waste.

Step 6

ASSESS YOUR READINESS AGAINST THE CMMC FRAMEWORK

Many organizations think of compliance as a point-in-time issue. At a given interval — often once per year — they have to prove compliance against a set list of requirements. However, while CMMC audits are indeed a point-in-time assessment, that doesn't mean DoD contractors can let things slip between audits. There are two reasons for this:

1. Having to reestablish compliance across hundreds of requirements is far more arduous than simply maintaining compliance; and,
2. If a contractor is breached and then found to be non-compliant, they run the risk of losing contracts.

To avoid these issues, contractors should take pains to monitor and maintain compliance between audits. Unfortunately, with technical controls in particular, it's easy to fall out of compliance during normal operations. This is because technical systems often have thousands of configuration settings, making human monitoring almost impossible. For this reason, automated CMMC software solutions like FIMs are a more realistic approach to maintaining compliance in technical systems.

How CimTrak Helps with CMMC Levels

Detailed Audit Reports and Forensic Evidence

Determine what systems and devices strayed from a known and trusted state by managing and controlling configuration and the change process associated to authorized behavior — all in real-time.

Continuous Monitoring

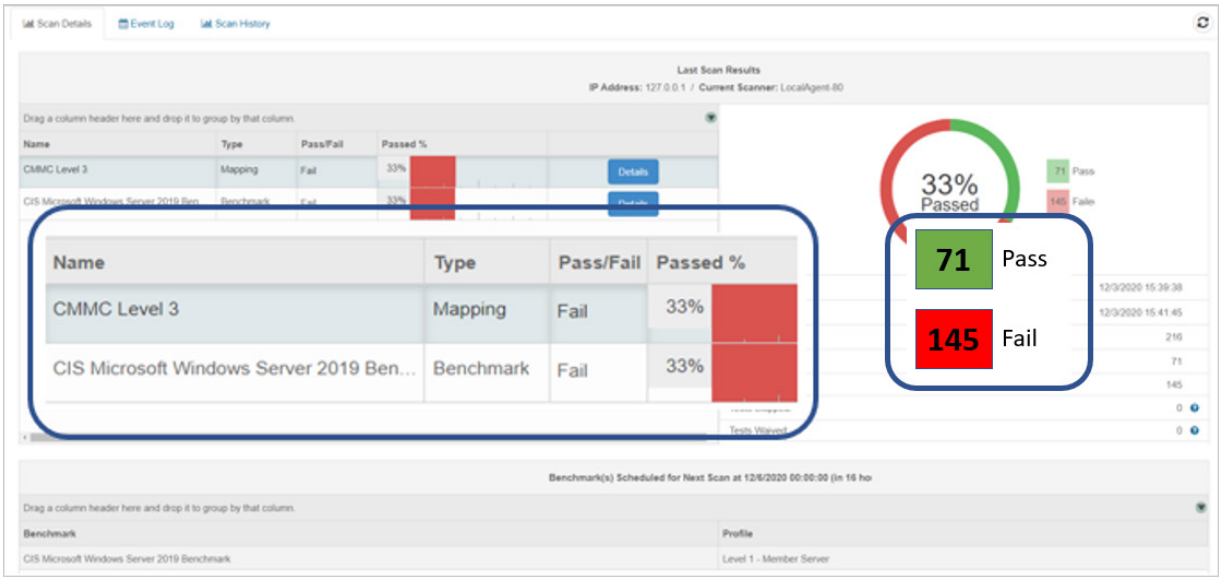
Don't settle on waiting 206 days to determine if there has been a breach. CimTrak's mean time to identify (MTTI) malicious and unwanted changes is measured in minutes as opposed to the industry average of 206 days.

Remediation/Roll-back Functionality

Automatically or manually roll-back and restore systems that have drifted from a known and expected state driving the mean time to contain (MTTC) from an industry average of 73 days to minutes.

Alerting

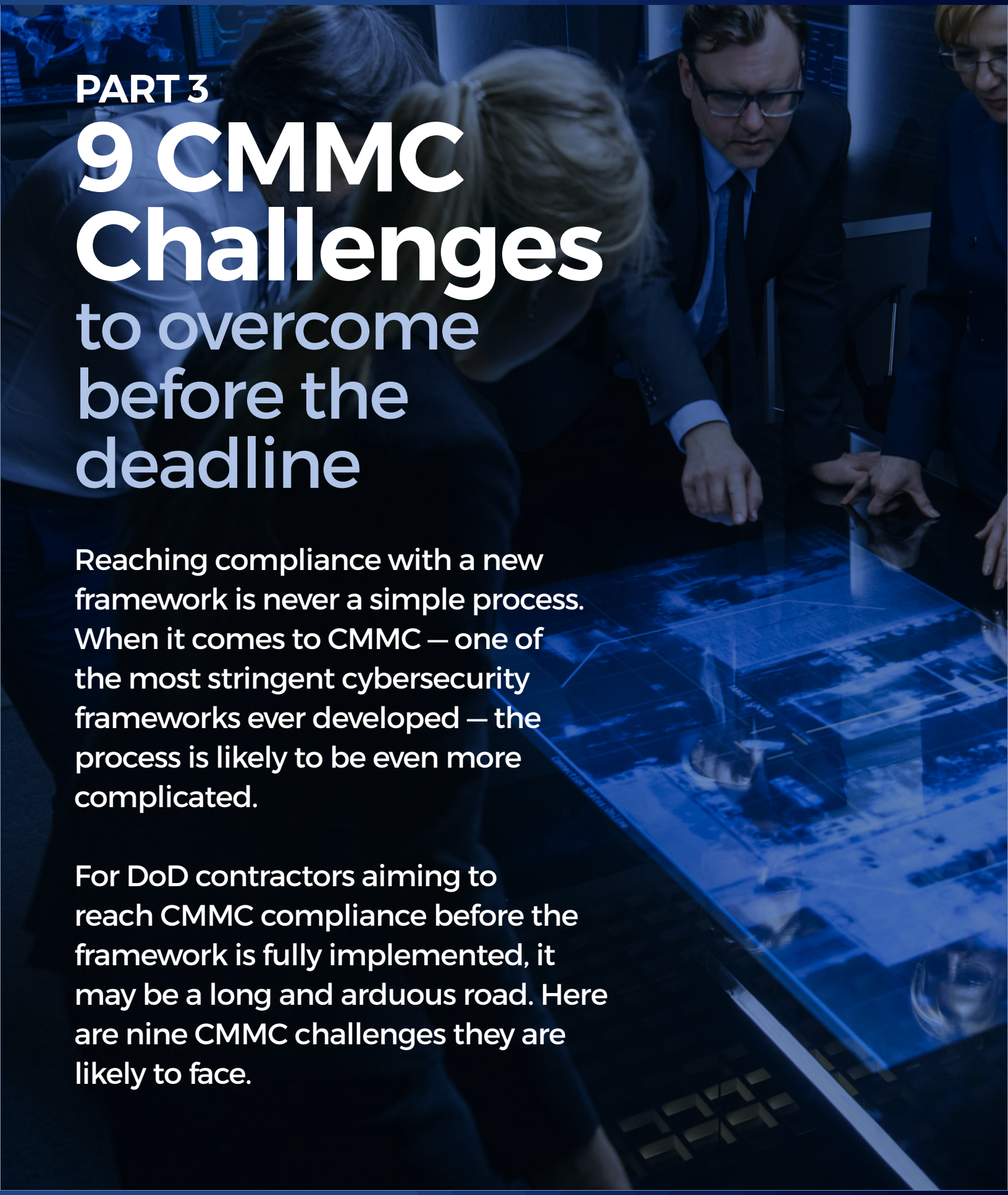
Integrated with ITSM and SIEM technologies creating a closed-loop environment of change management to reconcile and curate expected and approved changes. Reduce the noise +94% to only what is unknow, unwanted, unexpected and/or malicious in nature.



CimTrak's ability to provide a pass/fail rate, along with remediation steps needed to ensure compliance allows for minimal auditing concerns.

ADDITIONAL RESOURCES

- » CMMC Solution Brief
- » CimTrak Compliance Module
- » NIST Solution Brief
- » How to Prepare for a CMMC Audit
- » Top 10 Things to Know About CMMC
- » CMMC: Cybersecurity Standards for DoD



PART 3

9 CMMC Challenges to overcome before the deadline

Reaching compliance with a new framework is never a simple process. When it comes to CMMC — one of the most stringent cybersecurity frameworks ever developed — the process is likely to be even more complicated.

For DoD contractors aiming to reach CMMC compliance before the framework is fully implemented, it may be a long and arduous road. Here are nine CMMC challenges they are likely to face.

Challenge 1

REACHING COMPLIANCE BEFORE THE DEADLINE

For most current DoD contractors, it will likely be a year or two before CMMC is fully implemented. That means — if you already hold one or more DoD contracts — you have approximately that long to prepare.

However, as anyone in the cybersecurity world knows, making significant changes to a security program often takes years. Given that CMMC will require most DoD contractors to make substantial improvements to their existing programs, there's no time to lose.

Challenge 2

REACHING COMPLIANCE BEFORE YOU BID

If you're a prospective DoD contractor, the timescales associated with CMMC could be much shorter. Within a few months, new DoD contracts will begin to require bidders to meet a stated level of CMMC compliance. The rule is simple: no certification, no contract.

Reaching CMMC compliance is a significant process to go through just to be able to submit a bid. There is no guarantee that an organization will successfully obtain a contract once it reaches compliance, making CMMC a substantial hurdle to becoming a DoD contractor.

Challenge 3

ASSESS YOUR READINESS AGAINST THE CMMC FRAMEWORK

In 2019, the DoD audited 10 contractors with contracts worth over $1 million to determine whether they were genuinely compliant with NIST SP 800-171. Results of the audit made two things clear:

1. 9/10 of the contractors didn't have the proper controls in place to protect Controlled Unclassified Information (CUI)
2. Self-assessment doesn't work

As a result, CMMC will not rely on contractors to self assess. Instead, all current and prospective contractors will need to pay a certified assessor to inspect their operations.

Naturally, these assessments will incur a cost. According to the DoD, the assessment cost will "not be prohibitive," and successful contractors will be able to expense part of the assessment cost. Nonetheless, the need to pay and prepare for each audit will become entrenched as a cost of doing business with the DoD.

Challenge 4

COST OF BECOMING COMPLIANT

As any organization with compliance commitments knows, the assessment cost is not the main problem. The cost of preparing for each assessment is usually much greater.

For many current and prospective DoD contractors, becoming CMMC compliant isn't going to be fast or simple. From changes to processes and personnel to the cost of new systems or expert consultancy, it's not likely to be cheap, either.

Corbin Evans, director of regulatory policy at the National Defense Industrial Association, claims the cost of reaching level three compliance could be in the region of $250,000.

Challenge 5

Preparing for a CMMC assessment

Cost isn't the only challenge when it comes to compliance. There's also a significant amount of work to be done to prepare for a CMMC assessment. After all, being compliant isn't enough — you have to be able to prove it.

While the specifics of the CMMC assessment process aren't yet known, it's a reasonable assumption that contractors will need to provide documentation and real-world evidence that all of the requirements are met. Naturally, setting up and maintaining the systems required to produce this evidence will take additional time and resources.

Challenge 6

ASSESS YOUR READINESS AGAINST THE CMMC FRAMEWORK

CMMC compliance has already begun to be implemented. Certification requirements were included as a requirement in the Request for Proposals (RFP) for a handful of contracts in late 2020. These contracts are expected to impact approximately 150 contractors for each contract resulting in a total of almost 1,500 contractors needing to comply immediately with one of the five levels.

Faced with the prospect of becoming CMMC compliant within a very short time, only contractors with mature, well-established cybersecurity programs will have any chance of meeting the requirements of these contracts.

Challenge 7

COMPLIANCE MAY BE HARDER THAN YOU THINK

According to Tier 1 Cyber research, many DoD contractors have a false sense of their cybersecurity preparedness. To make matters worse, only 12% trust their vendors to handle cybersecurity effectively.

With CMMC being the most stringent cybersecurity standard yet — and prime contractors taking on responsibility for subcontractors' compliance — reaching full compliance could be an uphill struggle for many contractors.

Challenge 8

CMMC MAY EXTEND BEYOND THE DoD

While CMMC is exclusive to DoD contracts for the immediate future, there is a history of other government departments and agencies adopting similar standards. DISA STIGs is a current example of this trend, with the most recent being the Cybersecurity and Infrastructure Security Agency (CISA) directive requiring all federal civilian agencies to implement a Vulnerability Disclosure Policy (VDP) — a trailblazed by the DoD and U.S. military.

What does this mean for organizations doing business with federal civilian agencies? Right now, nothing. However, given the history, don't be surprised if CMMC is extended to cover some civilian agencies within a few years.

Challenge 9

IDENTIFYING COMPLIANCE GAPS

One of the greatest challenges for organizations aiming to become CMMC compliant is determining where their gaps lie. While internal and external assessments can be a valuable tool to identify areas of non-compliance — particularly those related to human systems and processes — they are only point-in-time assessments. It's easy for routine changes and updates to cause previously compliant systems to fall back out of compliance.

CimTrak Simplifies CMMC Compliance Gaps

Detailed Audit Reports and Forensic Evidence

Determine what systems and devices strayed from a known and trusted state by managing and controlling configuration and the change process associated to authorized behavior — all in real-time.

Continuous Monitoring

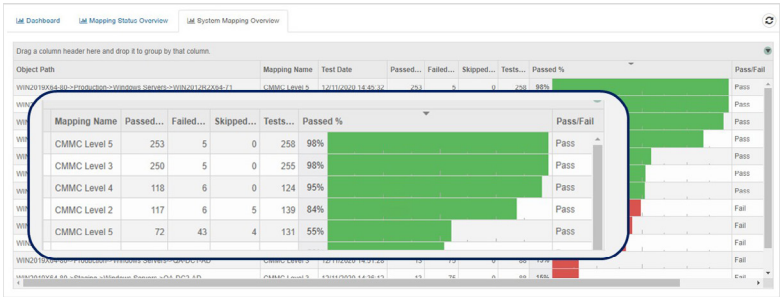
Don't settle on waiting 206 days to determine if there has been a breach. CimTrak's mean time to identify (MTTI) malicious and unwanted changes is measured in minutes as opposed to the industry average of 206 days.

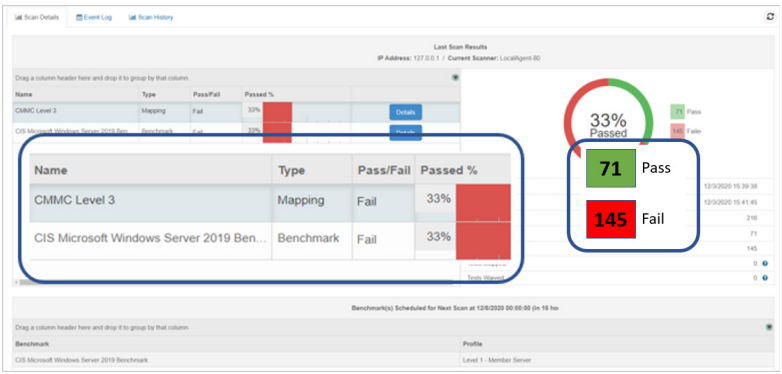
Remediation/Roll-back Functionality

Automatically or manually roll-back and restore systems that have drifted from a known and expected state driving the mean time to contain (MTTC) from an industry average of 73 days to minutes.

Alerting

Integrated with ITSM and SIEM technologies creating a closed-loop environment of change management to reconcile and curate expected and approved changes. Reduce the noise +94% to only what is unknow, unwanted, unexpected and/or malicious in nature.





Given CimTrak's patented real-time change detection capability, immediate notification and remediation options are available to ensure that any potential threat, both internal and external, does not permeate throughout the organizations. CimTrak's mean time to detect (MTTD) malicious and unwanted changes is measured in minutes as opposed to the industry average of 206 days.

CimTrak's ability to provide a pass/fail rate, along with remediation steps needed to ensure compliance allows for minimal auditing concerns.

ADDITIONAL RESOURCES

- » CMMC Solution Brief
- » CimTrak Compliance Module
- » NIST Solution Brief
- » How to Prepare for a CMMC Audit
- » Top 10 Things to Know About CMMC
- » CMMC: Cybersecurity Standards for DoD

CIMTRAK

Innovative, next-generation, file and system integrity monitoring software, securing your infrastructure.
Get compliant and stay that way.

PART 4

Fast track your CMMC Certification

After announcing the new standard in 2019, the DoD published CMMC version 1 in January 2020. Now, defense contractors are scrambling to achieve CMMC certification as quickly as possible to make sure they don't lose out on DoD contracts.

Learn how you can fast track your organization's certification process to make sure you're ready before the CMMC certification deadline.

What is CMMC Certification?

Achieving certification with CMMC version 1.0 requires DoD contractors to evidence compliance across up to 171 practices and 85 processes spread across 43 cybersecurity capabilities. These requirements are spread across five CMMC levels:

1. Performed

Basic cyber controls that any organization should maintain as a minimum standard. DoD contractors that work with mildly sensitive information such as Federal Contract Information (FCI) will need to be CMMC level 1 certified.

2. Documented

Intermediate controls that most organizations should maintain. Contractors that routinely work with FCI and possibly more sensitive information such as Controlled Unclassified Information (CUI) will need to be level 2 certified. Together, CMMC levels 1 and 2 are in line with the requirements of NIST 800-171. As a result, most existing DoD contractors should have little difficulty reaching these levels — so long as they haven't cut corners on the current self-assessment model.

3. Managed

CMMC level 3 requires a level of cyber maturity that goes beyond what most organizations have in place. To reach certification, contractors will need to evidence a significant maturity standard across all 110 NIST controls plus an additional 20 controls. The majority of DoD contractors that hold or process CUI will need to achieve level 3 certification.

4. Reviewed

By the time they reach CMMC level 4 certification, contractors will demonstrate a significantly higher cyber maturity level than most organizations. Level 4 requires contractors to adopt a proactive approach to identifying, tracking, and blocking cyber threats, including those conducted by Advanced Persistent Threat (APT) groups.

5. Optimizing

CMMC level 5 is by far the toughest cybersecurity maturity standard ever required for government contractors. The level — which requires contractors to evidence a fully mature cybersecurity function across all 171 practices, 85 processes, and 43 capabilities — will be reserved for only the most sensitive and high-profile defense contracts. At the current time, CMMC is only a requirement for DoD contracts. However, it has already been suggested that — if successful — other government agencies may adopt CMMC in the future.

How to Get CMMC Certification Quickly

If most existing contractors have at a year or two to prepare, what's the rush?

CMMC is arguably the toughest IT security maturity model ever devised. It's undoubtedly the most challenging compliance requirement ever mandated for defense contractors. If you're even passingly involved with cybersecurity at your organization, you'll know improving maturity is far from easy.

Simply, if your organization is a current or aspiring DoD contractor, you should start preparing for CMMC now. Here are the steps you'll need to take to reach certification quickly:

1. Understand what level you need to comply with

Most DoD contracts don't yet include CMMC requirements, so you may not know which certification level you need to reach. If you're an existing contractor, reach out to your contracting official, or ask your prime contractor to do so if you're a subcontractor. New contractors can easily determine the certification level they need to achieve, as the DoD will publish most new defense contracts with clear CMMC requirements.

2. Determine which systems are in scope

It's important to realize CMMC compliance doesn't apply to all your assets — just those directly or indirectly involved with the storage, processing, or transmission of CUI. These systems form your 'CUI environment.' If you're unsure how to scope your CUI environment, check with your contracting official, prime contractor, or seek help from a professional service provider.

3. Assess your readiness against the appropriate CMMC level

To do this, complete a thorough assessment and gap analysis of your CUI environment. For human systems, it may be useful to arrange an impartial audit, as this will provide a more realistic readiness assessment than an internal exercise. For technical systems, consider using an automated compliance scanning technology such as a System and Integrity Monitoring solution to identify non-compliance gaps quickly.

4. Create and enact a plan to reach compliance

Once you know where your gaps lie, create a clear roadmap to achieve compliance ahead of the CMMC certification deadline. Keep in mind that achieving full compliance could easily take month or years — particularly for higher CMMC levels — so you'll want to get started as soon as possible. Remember to build time buffers into your roadmap to account for any delays.

5. Get assessed by a CMMC Assessor

Unlike the previous model, where contractors self-assessed their readiness against NIST 800-171, achieving CMMC certification requires a physical audit. These audits will be conducted by a Certified 3rd Party Assessor Organization (C3PAO). If your organization is successful in winning defense contracts, part of this assessment cost is reclaimable.

6. Ensure ongoing compliance

As with all security maturity models, one of the most challenging aspects of certification will be maintaining compliance between audits. For technical controls, in particular, it's easy for systems and processes to lapse and drift into non-compliance during normal use. To avoid this, consider using an integrity management solution to continually scan your CUI environment and identify and repair noncompliance issues wherever they arise.

What is the CMMC Timeline?

The DoD has set an aggressive timeline for CMMC, with the understandable intention of protecting CUI as quickly as possible. While this may be good from a security standpoint, it puts significant pressure on current and prospective defense contractors to bring their security programs in line with CMMC requirements.

In June 2020, the DoD added the CMMC requirement to the RFI process. From September, CMMC requirements will actively appear in the RFP process for new contracts, and from October, new contractors must be certified by a CMMC C3PAO (Certified 3rd Party Assessment Organization).

Has that got you worried? If your organization is an existing DoD contractor, you do get a little more leeway. The currently published CMMC timeline looks like this:

» Mid-2020: C3PAOs start applying for accreditation
» Late 2020: 20 DoD contracts are selected for early CMMC certification
» Late 2020: Some new DoD contracts require bidders to be CMMC certified
» 2021-2025: New RFPs gradually start to require certification

As you can see, the DoD is planning for full CMMC implementation within the next five years. That means defense contractors could have anywhere from a few months to a couple years, based on the release of the DoD contract, to reach compliance and be certified by a C3PAO.

Of course, this timeline was developed in the pre-COVID-19 era. The pandemic has already affected some aspects of the rollout — notably the need for on-site assessments — and there is no doubt it will continue to do so. Given that the certification will roll out gradually over several years, however, it seems unlikely that the overall timeline will be substantially affected.

CMMC Software: Prepare for CMMC with CimTrak

The timeline to meet CMMC requirements is tight. Version 1.0 of the CMMC framework has already been released, and even organizations that currently hold DoD contracts will need to reach full compliance within just 2-3 years. While that may sound like ample time to adjust, it poses a significant challenge — particularly for organizations that hold sensitive or high-profile DoD contracts.

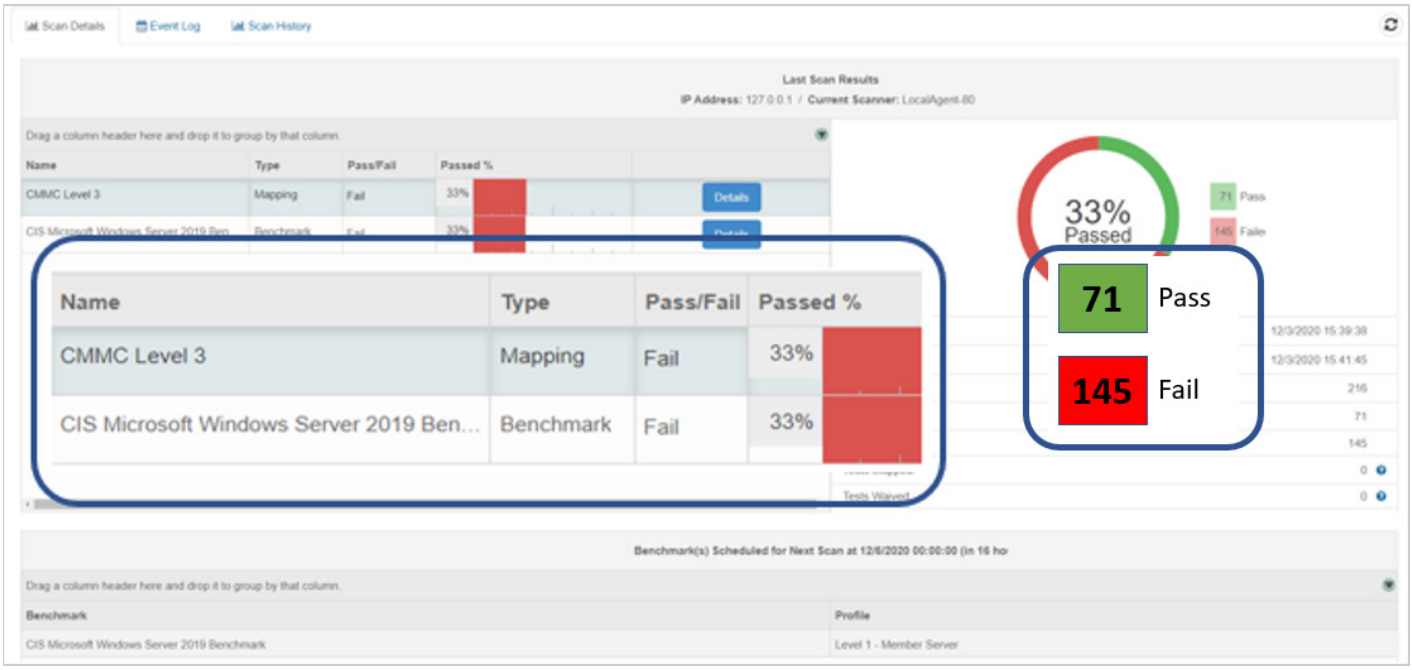
CimTrak is an IT integrity, security, and compliance tool that helps organizations quickly improve their cybersecurity maturity. CimTrak continuously monitors your environment and detects changes to assets, files, and accounts. When specified changes occur, CimTrak raises an alert and a report, making it easy to identify security issues in hardware and software assets.

CimTrak helps meet the demands across all levels of Compliance

CimTrak is able to help simplify compliance with:

» Automated Benchmark Scanning
» Configuration & Change Management
» Real-time Change Detection
» Remediation & Roll-back Capabilities
» Advanced Audit Trail & Reporting

Given CimTrak's patented real-time change detection capability, immediate notification and remediation options are available to ensure that any potential threat, both internal and external, does not permeate throughout the organizations. CimTrak's mean time to identify (MTTI) malicious and unwanted changes is measured in minutes as opposed to the industry average of 206 days.



CimTrak's ability to provide a pass/fail rate, along with remediation steps needed to ensure compliance allows for minimal auditing concerns.

ADDITIONAL RESOURCES

- » CMMC Solution Brief
- » CimTrak Compliance Module
- » NIST Solution Brief
- » How to Prepare for a CMMC Audit
- » Top 10 Things to Know About CMMC
- » CMMC: Cybersecurity Standards for DoD

CIMTRAK

Innovative, next-generation, file and system integrity monitoring software, securing your infrastructure.
Get compliant and stay that way.

Cyber Maturity Model Certification (CMMC) Crosswalk To CimTrak

Access Control (AC)		Asset Management (AM)		Audit & Accountability (AU)		Configuration Management (CM)		Incident Response (IR)		Recovery (RE)		Risk Management (RM)		Security Assessment (CA)		System & Communication Protection (SC)		System & Information Integrity (SI)		Additional 20 Controls Required by CMMC (non 800-171 controls)	
No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak
1.001	✓	3.036		2.041	✓	2.061	✓	2.092		2.137		2.141		2.157		1.175		1.210	✓	AM.3.036	
1.002	✓	4.226	✓	2.042	✓	2.062	✓	2.093		2.138	✓	2.142	✓	2.158		1.176		1.211	✓	AU.2.044	
1.003				2.043		2.063	✓	2.094		3.139		2.143	✓	2.159		2.178		1.212	✓	AU.3.048	
1.004				2.044		2.064	✓	2.096		5.140		3.144		3.161	✓	2.179	✓	1.213	✓	IR.2.093	✓
2.005	✓			3.045		2.065	✓	2.097				3.146		3.162		3.177		2.214	✓	IR.2.094	✓
2.006				3.046		2.066	✓	3.098				3.147		4.163		3.180		2.216	✓	IR.2.095	✓
2.007				3.048	✓	3.067	✓	3.099				4.149		4.164		3.181	✓	2.217	✓	IR.2.097	✓
2.008				3.049		3.068	✓	4.100				4.150		4.227		3.182		3.218		RE.2.137	
2.009				3.050		3.069	✓	4.101				4.151				3.183		3.219		RE.2.139	
2.010				3.051	✓	4.073	✓	5.102				4.148				3.184		3.220		RM.3.144	
2.011				3.052	✓	5.074	✓	5.106	✓			5.152				3.185		4.221	✓	RM.3.146	
2.012				4.053				5.108				5.155				3.186		5.222	✓	RM.3.147	
2.013				4.054				5.110								3.187		5.223	✓	CA.3.162	
2.014				5.055												3.188				SA.3.169	✓
2.015																3.189				SC.2.179	✓
2.016																3.190				SC.3.192	
3.017	✓															3.191	✓			SC.3.193	
3.018	✓															3.192				SI.3.218	
3.019																3.193				SI.3.219	
3.020																4.197				SI.3.220	
3.021																4.228					
3.022																4.199					
4.023																4.202					
4.025	✓															4.229					
4.032	✓															5.198					
5.024																5.230	✓				
																5.208					

✓ CimTrak Provides a Solution

The chart above is a crosswalk for all CimTrak products if they provide a control, automated scan or enable a process, procedure or policy to assist with the evidence collection to meet the objective of a defined domain, category, control, standard, component or assessment factor.

Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server
MySQL PARAMETERS MONITORED, Default rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, and others