The Training Mandate

Building Compliant Awareness and Training Programs Under CMMC Level 2

By David W. Koran, Registered Practitioner Advanced
David Koran & Associates, Inc.

April 2026

1. Regulatory Framework for Training

The Awareness and Training (AT) family within NIST SP 800-171 Rev. 2 establishes the baseline requirement that organizations handling Controlled Unclassified Information (CUI) must ensure their workforce is both informed and competent. While it contains only three controls at CMMC Level 2, the AT family has an outsized operational impact: it is the mechanism through which every other control family is operationalized at the human level. A contractor may deploy the most advanced technical controls available, but if the personnel who interact with CUI do not understand their responsibilities, those controls will not achieve their intended effect.

AT.L2-3.2.1: Role-Based Security Training

AT.L2-3.2.1 requires that organizations provide security awareness training to information system users, including managers, senior executives, and contractors, that is consistent with the policies, procedures, and agreements relevant to their roles. The operative phrase is *consistent with their roles*. CMMC does not permit a single, generic training module delivered uniformly across the entire organization. The training must be differentiated based on the level of access, the nature of interaction with CUI, and the specific responsibilities of the individual.

For contract eligibility, this control carries direct consequences. Under DFARS 252.204-7012, contractors must provide adequate security for covered defense information. The CMMC Assessment Guide (v2.13) maps AT.L2-3.2.1 to the expectation that an organization can demonstrate role-specific training content, delivery records, and evidence that personnel in distinct roles received distinct instruction. A contractor that presents a single awareness video for all employees will not satisfy the assessment criteria.

AT.L2-3.2.2: Basic Security Awareness

AT.L2-3.2.2 requires that the organization ensure all users of organizational information systems are aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. Where AT.L2-3.2.1 demands role specificity, AT.L2-3.2.2 establishes the floor: every individual with access to organizationalsystems must receive foundational training. This includes topics such as recognizing malware and virus threats, identifying social engineering and phishing attempts, understanding acceptable use policies, and knowing the procedures for reporting security incidents. Baseline awareness must also address physical security behaviors that apply across all roles: how to challenge unknown or unescorted individuals in the facility, how to handle visitor situations, and the requirement to remove CUI from plain view before visitors or unauthorized personnel enter an area. On the shop floor, this means securing travelers, work orders, engineering drawings, and any other CUI-bearing documents that may be visible at workstations or inspection areas. In the office, it means clearing desks, monitors, and whiteboards of CUI before uncleared personnel are present. These are not role-specific behaviors. They apply to every employee at every level of the organization.

AT.L2-3.2.3: Insider Threat Awareness

AT.L2-3.2.3 requires the organization to provide security awareness training on recognizing and reporting potential indicators of insider threat. This control addresses a distinct risk category that is separate from external attack vectors. Personnel must be trained to identify behavioral indicators, understand the reporting channels available to them, and recognize that insider threat awareness is a shared organizational responsibility, not solely the domain of security or management.

Together, these three controls form a layered training architecture. AT.L2-3.2.2 ensures universal baseline awareness, AT.L2-3.2.1 adds specificity based on function, and AT.L2-3.2.3 addresses the insider threat dimension. The practical result is that organizations must develop a general training program delivered to the entire workforce, supplemental role-specific training modules targeting defined groups, and dedicated insider threat content that applies across all roles.

Institutionalizing these practices means embedding training into the operating rhythm of the organization. It is not sufficient to deliver training once during onboarding and treat the obligation as fulfilled. The training program must be documented in policy, supported by defined procedures, and subject to periodic review and updating. This is what separates a mature compliance posture from one that will be scrutinized during a formal assessment.

2. Strategic Alignment: Consultant and HR Collaboration

Effective CMMC training programs require coordination between two distinct competencies: the technical subject matter expertise of the CMMC consultant and the administrative delivery and record-keeping infrastructure of the Human Resources department. When these functions operate in isolation, the result is either technically accurate content that is never properly tracked or well-documented training that fails to address the actual security requirements.

The Design Phase: Defining Scope and Ownership

The CMMC consultant is responsible for defining the technical scope and content of the training program. This includes identifying which controls from NIST SP 800-171 are relevant to each role, developing content that addresses those controls at an appropriate depth, and ensuring the training materials are current with the latest revision of the CMMC Assessment Guide. In organizations with established training departments, the consultant serves as a technical advisor: validating content accuracy, reviewing training materials for regulatory alignment, and ensuring the curriculum maps to what an Assessor will evaluate. The consultant does not necessarily deliver every session, but the consultant must confirm that the content is technically correct and complete.

For smaller contractors that do not maintain dedicated training staff, the engagement model is often more direct. In these environments, the consultant may design the entire training program, develop the course materials, and deliver the instruction to employees. This is a common operational reality in the Defense Industrial Base, where many contractors are small and mid-sized manufacturers without the internal resources to build a security training program from the ground up. The consultant's role in these cases extends from program architecture through classroom delivery.

Regardless of the delivery model, Human Resources owns the administrative infrastructure: scheduling, tracking, retention of training records, and integration with the onboarding process. HR manages the annual refresh cycle, ensures that personnel who have not completed required training are identified and escalated, and maintains the artifact trail that will be examined during a C3PAO assessment. The division of responsibility should be documented in the organization's training policy, with the CMMC consultant identified as the technical authority and HR identified as the administrative authority.

MFA Scenario Training for Office Personnel

Office personnel who access CUI behind Multi-Factor Authentication (MFA) represent a common training scenario for defense contractors. These individuals typically interact with CUI through email, shared file systems, or cloud-based collaboration platforms that are protected by MFA as part of the organization's Identification and Authentication (IA) controls. Training for this group must cover the correct use of MFA tokens or authenticator applications, the prohibition against sharing authentication credentials, the procedures for reporting a lost or compromised second factor, and the rationale for MFA in protecting CUI from unauthorized access.

The training should also address the intersection of MFA with remote access scenarios. Personnel working from home or traveling must understand that MFA requirements do not change based on location, that VPN connections to the organization's network require the same authentication rigor, and that using personal devices to bypass MFA controls constitutes a policy violation. These scenarios are directly relevant to controls within the Access Control (AC) and Identification and Authentication (IA) families.

Aerospace and Shop Floor: Media Protection Integration

The manufacturingenvironmentin the Defense Industrial Base presents training requirements that differ fundamentally from the office setting. In a typical aerospace machine shop, CNC machinery may receive machining instructions via USB drives or other portable storage media. These files may contain technical data classified as CUI, including engineering drawings, toolpath data, and inspection parameters. The physical movement of these media devices between workstations, between secure and nonsecure areas, and between shifts creates a distinct set of risks.

Training for shop floor personnel must address the Media Protection (MP) control family. Employees must understand which storage devices are authorized for use, the procedures for sanitizing media before reuse or disposal, the requirements for labeling CUI media, and the prohibition against removing media from the designated secure perimeter without authorization. The training must be practical and tailored to the physical environment. Abstract discussions of cybersecurity policy are insufficient for personnel whose primary interaction with CUI is through a USB drive inserted into a CNC controller.

The consultant should work with shop floor supervisors to develop scenario-based training that mirrors actual workflows. For example: an employee finds an unlabeled USB drive on a workstation. What is the correct procedure? A machinist needs to transfer a toolpath file from a secure terminal to a CNC machine. What steps must be followed? These scenarios ground the training in operational reality and produce measurable comprehension.

3. Role-Based Training Tiers

The following table summarizes the differentiated training requirements for the four principal role categories within a typical defense contractor. Each tier addresses the specific risks, control families, and operational scenarios relevant to the group.

Role Tier	Primary Focus Areas	Key Control Families	Training Delivery Method
Shop/Floor Workers	Physical security of CUI media, proper labeling and marking, media sanitization, secure handling of portable storage devices, insider threat indicators in the physical environment	Media Protection (MP), Physical Protection (PE), Awareness and Training (AT)	Hands-on scenario exercises, practical demonstrations at workstation, supervised media handling drills
Office Personnel	CUI handling in digital formats, phishing recognition, remote access protocols, MFA compliance, acceptable use of organizational systems, insider threat reporting	Access Control (AC), Identification and Authentication (IA), Awareness and Training (AT)	Online modules with scenario-based testing, annual refresher sessions, simulated phishing exercises
Privileged Users (IT/Admins)	System integrity monitoring, audit log review, incident response procedures, configuration management, account management, insider threat detection through technical indicators	Audit and Accountability (AU), Incident Response (IR), Configuration Management (CM), System and Information Integrity (SI)	Technical workshops, tabletop incident response exercises, hands-on lab environments, peer review sessions
Executive Management	Resource allocation for compliance, risk management, contractual obligations under DFARS, business impact of noncompliance, oversight of CMMC readiness	Risk Assessment (RA), Security Assessment (CA), Awareness and Training (AT)	Briefings with quantified risk data, business case presentations, strategic planning sessions

The critical distinction across these tiers is specificity. Shop floor workers do not need instruction on audit log analysis, and IT administrators do not need training on CNC media handling. Each group must receive content that is directly relevant to the risks they face in their specific operational context. This differentiation is what AT.L2-3.2.1 requires, and it is what a C3PAO Assessor will verify.

Executive management training warrants particular attention. Senior leaders are responsible for allocating the resources that make compliance possible: budget for security tools, staffing for IT and compliance functions, and time for personnel to complete required training. If leadership does not understand the contractual and operational consequences of noncompliance, the organization's compliance posture will be structurally underfunded. Training for this group should present CMMC requirementsin terms of contract risk, competitive positioning, and the financial exposure associated with failure to achieve or maintain certification.

Dual-Environment Personnel: Testing and Inspection

Not all personnel fit neatly into a single training tier. Testing and inspection department staff are a common example: their duties frequently span both the office and the shop floor. These individuals may use office workstations to access CUI through MFA-protected systems, review digital inspection records, or generate quality reports. They may also work directly on the manufacturing floor, handling physical media, verifying parts against CUI-bearing engineering drawings, and operating inspection equipment at workstations adjacent to CNC machinery.

Personnel in these dual-environmentroles require training that covers both the office-based and shop floor curricula. They must understand MFA compliance, phishing recognition, and digital CUI handling, and they must also understand media protection, physical labeling requirements, and the procedures for securing CUI within the manufacturing environment. The training program must account for these overlapping responsibilities rather than defaulting to one tier or the other. The organization should identify which roles operate across both environments during the training design phase and ensure those individuals receive the combined curriculum.

Universal Training Requirements Across All Tiers

Certain training topics cut across every role tier and must be addressed in the general awareness curriculum that all employees receive. Malware and virus awareness is one such topic. Every individual who uses an organizational system must understand how malicious software is delivered, what the indicators of compromise look like, and what steps to take if they suspect an infection. This applies equally to an executive reading

email, an office worker downloading a file, and a shop floor operator inserting a USB drive.

Facility security and visitor management represent another universal requirement. Every employee, regardless of role, must know how to challenge an unknown individual who is in a secure area without visible escort or identification. The training must make clear that this is an organizational expectation, not a personal judgment call. Personnel must also be trained on proper visitor procedures: verifying that visitors have been authorized and logged, ensuring visitors are escorted at all times within areas where CUI may be present, and securing CUI before a visitor enters the space.

The requirement to remove CUI from plain view during visitor situations deserves specific emphasis because it applies in both the office and the manufacturing environment. In the office, this means clearing documents from desks, closing files on monitors, and erasing whiteboards. On the shop floor, the exposure is often more pervasive and less obvious: travelers, route cards, inspection sheets, and engineering drawings may be posted at workstations, clipped to machines, or sitting on inspection tables throughout the production area. Employees must be trained to recognize that these documents constitute CUI in plain view and to secure them before any unauthorized individual enters the area. This is a practical, operational discipline that must be rehearsed and reinforced, not merely acknowledged in a training slide.

4. Competency Testing and Records Management

Delivering training is only half of the obligation. The organization must also be able to demonstrate that the training was effective and that personnel achieved a measurable level of understanding. The CMMC Assessment Guide identifies "Test" as one of the assessment methods available to a C3PAO, and the organization's own competency testing program should mirror this expectation.

Exam Structure and Design

Competency testing should use objective, scenario-based questions that assess whether the individual can apply the training content to realistic situations. Multiple-choice questions that test rote memorization of policy language do not demonstrate comprehension. Instead, questions should present a scenario and ask the individual to identify the correct response. For example: a shop floor employee discovers that a USB drive containing CUI has been left on an unsecured workbench. Which of the following

actions should the employee take first? This format validates understanding at the application level, not merely at the recall level.

The minimum passing score should be defined in the organization's training policy and applied consistently. Industry practice for security awareness training typically sets the threshold at 80 percent. Individuals who fail to meet the passing score must be required to retake the training and retest within a defined timeframe. The policy should also specify the consequences for repeated failure, which may include restrictions on access to CUI until competency is demonstrated.

HR Recording and Artifact Trail

The records management component of the training program is as important as the content itself. During a C3PAO assessment, the Assessor will examine training records to verify that every individual within scope received the appropriate training, passed the competency test, and completed these requirements within the required timeframe. Incomplete or disorganized records create an immediate compliance gap.

At a minimum, the organization must maintain the following for each individual: the date training was completed, the specific version of the training material used, the test score achieved, the date of the next required refresher, and the signature or electronic acknowledgment of the individual confirming completion. These records should be maintained in a centralized system that HR can access and produce on demand. Spreadsheets stored on individual workstations or paper records in unlocked filing cabinets do not meet the standard for verifiable, auditable documentation.

Version control of training materials is an additional requirement that organizations frequently overlook. When training content is updated to reflect changes in policy or regulatory guidance, the organization must be able to demonstrate which version of the material each individual received. This is particularly important during periods of transition, such as when NIST SP 800-171 is revised or when organizational procedures change. The artifact trail must connect each individual's training record to a specific, dated version of the content.

5. C3PAO Assessment Expectations

Understanding how a C3PAO Assessor will evaluate the training program is essential for building one that will withstand scrutiny. The CMMC Assessment Guide prescribes three assessment methods: Interview, Examine, and Test. For the AT control family, all three are typically employed.

Interview

The Assessor will interview personnel across the organization to determine whether they understand their security responsibilities. These interviews are not limited to the IT department or the compliance team. An Assessor may speak with a shop floor machinist, an administrative assistant, or a project manager. The purpose is to determine whether the training has been internalized, not merely completed. If a machinist cannot explain the procedures for handling CUI media, or if an office worker cannot describe the process for reporting a suspected phishing email, the Assessor has evidence that the training program is not effective.

Examine

The Assessor will examine the documentary evidence of the training program. This includes the training policy, the training materials, the records of completion, the test results, and any other artifacts the organization produces. The Assessor is looking for completeness, consistency, and currency. Are all personnel within scope accounted for in the training records? Do the training materials address the specific controls relevant to each role? Are the records current, or are there individuals whose last training date is more than twelve months old?

Test

The Assessor may independentlytest the knowledge of personnel to validate the organization's own competency testing results. This is where the distinction between rote compliance and genuine understanding becomes critical. An organization that has delivered thorough, role-specific training and tested for comprehension at the application level will produce personnel who can answer an Assessor's questions confidently and accurately. An organization that has treated training as an administrative obligation will produce personnel who struggle to connect the content of their training to their daily responsibilities.

The overarching objective from the C3PAO perspective is to determine whether the training program is ingrained in the organizational culture. This is not a subjective judgment. It is evidenced by the specificity of the training content, the rigor of the testing methodology, the completeness of the records, and the demonstrated knowledge of the personnel. Organizations that approach training as a compliance formality will find that the assessment exposes the gap between documentation and practice.

6. Lifecycle and Onboarding

A compliant training program must address two temporal dimensions: the ongoing requirement for periodic refresher training and the immediate requirement for training newly onboarded personnel.

Refresher Training Frequency

NIST SP 800-171 and the CMMC Assessment Guide expect that security awareness and role-based training be refreshed on at least an annual basis. This means that every individual within scope must complete the full training cycle, including competency testing, at least once every twelve months. Organizations should establish a fixed annual training period rather than tracking individual anniversary dates, as the latter approach

creates administrative complexity and increases the risk that individuals fall through scheduling gaps.

In addition to the scheduled annual cycle, the organization should define triggers for supplemental training. These triggers should include material changes to security policy, the introduction of new information systems or processes that affect CUI handling, significant security incidents that reveal training gaps, and changes to the regulatory or contractual requirements that govern the organization's obligations. The training policy should specify these triggers explicitly so that supplemental training is delivered based on defined criteria, not ad hoc judgment.

Onboarding New Personnel

Newly hired or newly assigned personnel represent a compliance vulnerability until they have completed the required training. The organization's training policy must define a maximum timeframe for completing initial training, and that timeframe must be operationally realistic while minimizing the period of exposure. A common practice is to require that all initial security awareness and role-based training be completed within the first five business days of employment or assignment to a role involving CUI.

During the period between an individual's start date and the completion of training, the organization must implement compensating measures to prevent unauthorized or uninformed access to CUI. These measures may include restricting the individual's system access until training is completed, requiring that the individual work under direct supervision of trained personnel, or limiting the individual's physical access to secure areas. The specific compensating measures should be documented in the training policy and applied consistently.

The onboarding process should also be integrated with the organization's account management and access control procedures. HR should coordinate with IT to ensure that system access provisioning is contingent on the completion of required training. This creates a procedural interlock that prevents the creation of a compliance gap: an individual cannot access CUI until the training record demonstrates that the prerequisite has been satisfied.

Conclusion

The Awareness and Training requirements under CMMC Level 2 are not administrative formalities. They are the mechanism through which an organization ensures that every individual who interacts with Controlled Unclassified Information understands the risks, knows the procedures, and can demonstrate competency. A training program that

is generic, undocumented, or disconnected from the operational realities of the workforce will not satisfy the expectations of a C3PAO assessment.

Building a compliant program requires deliberate collaboration between the technical expertise of the CMMC consultant and the administrative infrastructure of Human Resources. It requires differentiated content that reflects the distinct risks faced by shop floor workers, office personnel, privileged users, and executive leadership. It requires competency testing that validates understanding at the application level, not merely at the level of attendance. And it requires a records management practice that can produce complete, current, and verifiable documentation on demand.

Organizations that invest in this process will find that the training program serves as more than a compliance artifact. It becomes the foundation for a security culture that is resilient, informed, and capable of withstanding both the scrutiny of a formal assessment and the operational pressures of the defense contracting environment.

About the Author

David W. Koran is a CMMC Registered Practitioner and the Managing Partner of David Koran & Associates, a consulting firm specializing in CMMC readiness and implementation for Defense Industrial Base contractors. He is an Associate Member of the American Bar Association Section of Public Contract Law. His practice focuses on translating regulatory requirements into operational compliance programs for contractors and the legal professionals who advise them.