Awareness and Training (3.2) Family

Security Requirements and the Technologies That Implement Them

A practitioner reference for Defense Industrial Base contractors · Family 2 of 14 in a 14-part series on the NIST SP 800-171 families · Prepared July 2026

Overview of the Awareness and Training Family

Awareness and Training (3.2) is the smallest family in NIST SP 800-171 Rev 2, but it carries an outsized share of assessment risk: two of its three requirements are weighted at the maximum **5 SPRS points** each, and it is the family most often failed for lack of **records** rather than lack of activity. Contractors frequently run some form of training but cannot produce dated completion evidence, role-based curricula for administrators, or insider-threat content - and an assessor scores what can be demonstrated, not what is asserted. That makes **records, not tooling, the product** of this family: a free program that yields clean completion evidence outperforms an expensive platform with messy records, and the cheapest path to 10 SPRS points runs through documentation discipline rather than procurement.

The family contains **3 security requirements** - **2 Basic** (from FIPS 200) and **1 Derived** (from NIST SP 800-53). The Basic requirements (3.2.1, 3.2.2) address general security awareness and role-based training respectively; the Derived requirement (3.2.3) adds insider-threat awareness. Because the family is people-centric, its "implementing technology" is a security awareness training platform plus a learning management system (LMS) that captures who was assigned what, when they completed it, and what happens when they do not. This is **Family 2 of 14** in a planned series covering all fourteen 800-171 families.

Which revision applies? This guide covers **NIST SP 800-171 Revision 2**, which is the baseline the DoD's CMMC program and DFARS 252.204-7012 currently require. In May 2024 NIST published **Revision 3**, which renumbers this family to 03.02, adds organization-defined training frequencies, and introduces a new requirement on training feedback and updates for social engineering and social mining. Revision 3 has **not** been adopted for CMMC as of this writing - continue to assess against Revision 2 until the DoD formally transitions, and treat Revision 3 as forward-looking.

Requirement wording below is **summarized for readability**. The controlling text is the official publication, **NIST SP 800-171 Rev 2** (security requirements) and **NIST SP 800-171A** (assessment

objectives); consult them for exact language. SPRS point values are per the **DoD Assessment Methodology** (NIST SP 800-171 DoD Assessment Methodology, Rev 2).

The 3 Awareness and Training Requirements and Expected Evidence

The evidence column lists the artifacts an assessor typically expects; most controls need **both** a written policy and a technical artifact. The figure under each control ID is its **SPRS point value** (5, 3, or 1) - the score deducted if the control is not met.

NIST SP 800-171 Rev 2 Awareness and Training (3.2) requirements, SPRS weight, and expected evidence.

Control	Security Requirement	Evidence / Artifacts an Assessor Expects
3.2.1 5 pts	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Awareness and training policy with defined cadence; awareness curriculum / course content outline; LMS completion report by user with dates; new-hire onboarding training records; policy-acknowledgment records; phishing-simulation campaign results
3.2.2 5 pts	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Role-to-training matrix (admins, ISSO, help desk, developers, CUI handlers); role-based course content; completion records per role; professional certifications or vendor training certificates for security staff; records showing training before privileged access is granted
3.2.3 1 pt	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Insider-threat module content showing behavioral indicators covered; completion records; documented reporting channel (hotline, ticket category, named contact); evidence the reporting procedure is communicated to users

2 Basic requirements (3.2.1-3.2.2) and 1 Derived requirement (3.2.3).

POA&M warning: 3.2.1 and 3.2.2 are both **5-point** requirements. Under the CMMC Level 2 scoring rules (32 CFR Part 170), 5-point requirements **cannot be placed on a POA&M** at assessment time - they must be fully implemented before the assessment for a Conditional or Final status to be possible. 3.2.3, weighted at 1 point, is the family's only POA&M-eligible requirement. Training is one of the cheapest 10 points in the entire methodology to secure; there is no reason to arrive at an assessment without it.

Cost-Effective Implementation Paths

Awareness and Training is unusual among the fourteen families: a **$0 implementation can fully satisfy every assessment objective**, because the U.S. government publishes free, DoD-official courseware with completion certificates. Commercial platforms buy convenience and automation - not compliance that the free path lacks. Choose a tier by administrative capacity, not by assessment anxiety:

Three implementation tiers, costed for a 25-person contractor

Tier	Annual cost	Stack and evidence model
$0 government stack	$0	DoD **Cyber Awareness Challenge** (cyber.mil - the same annual course the DoD requires of its own personnel and contractors) for 3.2.1; **CDSE Insider Threat Awareness** eLearning (INT101.16 - free, certificate issued at a 75% passing score) for 3.2.3; CDSE and CISA role-based courses for administrators and ISSOs for 3.2.2. Note that **CDSE does not retain completion records** - each user must save their certificate, and your register plus the saved certificates *are* the assessment evidence. Layer on **Project Spectrum** (projectspectrum.io, DoD's no-cost readiness portal for DIB small businesses) and the DoD CIO's **DIB Cybersecurity-as-a-Service** no-cost resource list. Evidence: completion certificates filed per user plus a roster-reconciliation register (a disciplined spreadsheet is acceptable at this scale).
Lean SMB	~$600–800	**Wizer Boost** ($25/user/yr at the entry 25-user tier on a 3-year term, billed annually - $625/yr for a 25-person shop; volume pricing drops to $8–$20 at higher counts; a genuinely free basic tier also exists) or entry-tier KnowBe4. Automated assignment, reminders, and LMS reporting replace manual reconciliation; optional **GoPhish** (open source; self-host on a small cloud VM for roughly $20–40/month) if phishing simulation is wanted. Worth the spend when manual record-keeping exceeds roughly $600/yr of admin time - typically around 20–30 employees.
Already-on-E5 / GCC High	$0 marginal	Attack Simulation Training and training-assignment tooling you already license (see the licensing callout below) - configure it and export its reports rather than buying a redundant platform.

Phishing simulation is not required. None of the 800-171A assessment objectives for 3.2.1–3.2.3 mandate simulated phishing. Simulation strengthens 3.2.1/3.2.3 evidence (click rates, report rates, remedial-training records) and is genuinely useful - but a cost-constrained organization can defer it

entirely without creating a finding. Do not let a simulation-platform quote delay implementing the training itself.

Commercial platform pricing, for budgeting context: published benchmark data puts KnowBe4 at roughly **$7.50–$30 per user per year** depending on tier, seat count, and contract term, with a **25-seat minimum** that matters to very small shops; Proofpoint and Hoxhunt price comparably at the mid-market. Vendor pricing changes frequently - confirm current quotes before budgeting. The sections below cover the full commercial stack for organizations that choose it.

Implementing Technologies and How to Configure Them

The systems below are the common building blocks for the family. A single awareness platform with an integrated LMS and phishing simulator can carry all three requirements, provided role-based and insider-threat content is explicitly assigned and completion is tracked per user.

Security Awareness Training Platforms (KnowBe4, Proofpoint Security Awareness Training, Hoxhunt, SANS Security Awareness)

- Sync the user population automatically from the directory (Entra ID / Active Directory via SCIM or the vendor's sync agent) so every account holder - including new hires - is enrolled without manual list maintenance. *(3.2.1)*
- Build an annual baseline campaign covering the core topics: phishing and social engineering, password and MFA hygiene, acceptable use, physical security, removable media, and - critically for the DIB - **CUI identification, marking, and handling**. Generic consumer content that never mentions CUI is a common assessor finding. *(3.2.1)*
- Configure enforcement: automated reminders, manager escalation for non-completion, and (via Conditional Access or account-flagging integration) consequences for users who never complete. An assessor will ask what happens when someone does not finish. *(3.2.1)*
- Enable the platform's insider-threat / data-protection modules and assign them to all users, not just security staff. *(3.2.3)*

Microsoft Attack Simulation Training (Defender for Office 365)

Licensing check first: Attack Simulation Training requires **Microsoft Defender for Office 365 Plan 2** - included in Microsoft 365 E5/G5 (and the GCC High E5 bundles common in the DIB) or purchasable as an add-on. It is **not** included in Microsoft 365 Business Premium, which carries only Defender for Office 365 Plan 1 (E3 tenants get only a limited trial subset). Check what you already own before buying a third-party simulator - E5/GCC High tenants frequently pay twice for capability they already license.

- For Microsoft-centric tenants (including GCC High, where availability should be verified for your plan), use Attack Simulation Training to run phishing simulations with automatic just-in-time training assigned to users who click. *(3.2.1, 3.2.3)*
- Schedule recurring simulations (at least quarterly) with varied lure types - credential harvest, attachment, link-in-attachment, OAuth consent - rather than a single annual test. *(3.2.1)*
- Export campaign results and repeat-clicker reports; feed repeat clickers into a documented remedial-training workflow. *(3.2.1)*

Phishing Simulation Programs

- Whether via KnowBe4 PhishER, Proofpoint, Hoxhunt, or the open-source **GoPhish**, treat simulation as a measurement and reinforcement tool: track click rate, credential-entry rate, and **report rate** over time. A rising report rate is the strongest evidence the awareness program works. *(3.2.1, 3.2.3)*
- Deploy a "report phish" button (KnowBe4 Phish Alert, Microsoft Report Message add-in) so recognizing *and reporting* - the literal words of 3.2.3 - has a concrete, logged mechanism. *(3.2.3)*
- Document simulation authorization in policy so campaigns are sanctioned exercises, and coordinate with the help desk before each wave.

Role-Based Training for Administrators, ISSOs, and CUI Handlers

- Maintain a **role-to-training matrix**: for each role (system administrator, ISSO / security officer, help desk, developer, program manager handling CUI), list the required courses, the source, and the cadence. This single document is the backbone of 3.2.2 evidence. *(3.2.2)*
- For administrators, assign technical security training - secure configuration, privileged-account hygiene, audit-log review - through vendor curricula (Microsoft Learn security paths, SANS/GIAC courses, CompTIA Security+ / vendor certifications) or the awareness platform's advanced modules. *(3.2.2)*
- For the ISSO / security lead, document training aligned to the duties in the SSP: incident response coordination, POA&M management, assessment preparation. External evidence (certificates, CPE transcripts, conference attendance) counts if it is recorded. *(3.2.2)*
- Gate privileged access on training: make completion of the admin curriculum a checklist item before an admin account or PAM role is issued, and record it in the access-request ticket. *(3.2.2)*
- Include DoD-specific content where relevant: the DoD CUI awareness course (available publicly from DoD CUI program resources) is free and directly on-point for CUI handlers.

Insider-Threat Awareness Content and Reporting Channel

- Cover the recognized behavioral indicators: unexplained removal or copying of CUI, working odd hours without cause, unexplained affluence, attempts to access data outside job scope, disgruntlement paired with policy violations, and unreported foreign contacts where relevant. CDSE (the DoD Center for Development of Security Excellence) publishes free insider-threat awareness courses that map cleanly to 3.2.3. *(3.2.3)*
- Establish and publicize a reporting channel - a monitored mailbox, help-desk ticket category, or hotline - and name the role that receives reports. Assessment objectives for 3.2.3 test that users know *how* to report, not just what to look for. *(3.2.3)*
- Fold insider-threat scenarios into phishing simulations and annual refreshers so the topic recurs rather than appearing once at onboarding. *(3.2.3)*

LMS and Training-Records Management

- Whatever delivers the training, one system must be the authoritative record: user, course, assignment date, completion date, and score. Awareness platforms include an LMS; organizations with an HR LMS (Workday Learning, Cornerstone, Moodle, TalentLMS) can centralize there via SCORM/xAPI packages. *(3.2.1, 3.2.2, 3.2.3)*
- Export completion reports at least annually and after each campaign, and archive them with the compliance evidence set - do not rely on the vendor portal being available and unchanged at assessment time. *(3.2.1)*
- Reconcile the LMS roster against the directory quarterly: every enabled account in the CUI environment should map to a trained (or newly-assigned) user. Unenrolled service-desk hires are the classic gap. *(3.2.1)*
- Capture policy acknowledgments (acceptable use, CUI handling) electronically - awareness platforms and Microsoft Forms both work - and retain them alongside completion records.

Cadence, Onboarding, and Program Governance

- Write the cadence into the awareness and training policy: initial training **before or promptly upon** system access, an **annual** refresher for all users, role-based training on role assignment and annually thereafter, and ad-hoc updates when threats or policies change. Annual is the de facto assessor expectation even though Rev 2 does not state a number. *(3.2.1, 3.2.2)*
- Wire training assignment into the onboarding workflow (HR system trigger or joiner checklist) so day-one access and day-one training travel together. *(3.2.1)*
- Review and refresh content annually - stale 2019-era content with no mention of MFA fatigue attacks, QR-code phishing, or AI-generated lures undermines the "aware of security risks associated with their activities" objective. *(3.2.1)*

Tools for Extracting Structured Configuration Evidence

Wherever possible, capture evidence as **structured, text-based exports** - JSON, CSV, or API pulls - rather than screenshots. Machine-readable exports are timestamped, show the full record set, and can be ingested directly by a compliance platform.

KnowBe4

- **KnowBe4 Reporting API** (`/v1/training/enrollments`, `/v1/phishing/security_tests`) - per-user enrollment, completion status and dates, and phishing-test results as JSON. *(3.2.1, 3.2.3)*
- **Scheduled report exports** - completion and non-completion reports by group as CSV, emailed on a schedule to the compliance mailbox. *(3.2.1)*

Microsoft 365 / Attack Simulation Training

- **Microsoft Graph** (`/security/attackSimulation/simulations` and `.../report` endpoints) - campaign configuration, per-user click and report actions, and assigned-training completion as JSON. *(3.2.1, 3.2.3)*
- **Graph PowerShell** (`Get-MgUser`) - the authoritative user roster as CSV, for reconciliation against LMS enrollment. *(3.2.1)*
- **Viva Learning / M365 admin reports** - course-completion exports as CSV where Viva Learning delivers content. *(3.2.1, 3.2.2)*

Proofpoint Security Awareness Training

- **Proofpoint SAT API** - training assignments, completions, and phishing-simulation events as JSON; CSV exports from the admin console for point-in-time snapshots. *(3.2.1, 3.2.3)*

LMS Standards and Cross-Platform Records

- **SCORM / xAPI (Tin Can)** - deliver third-party content (CDSE-style courses, custom CUI modules) through your LMS so completions land in one reportable store; xAPI statements are JSON by design. *(3.2.1, 3.2.2)*
- **Moodle / TalentLMS / Cornerstone APIs** - completion and transcript exports as JSON/CSV where an HR LMS is the system of record. *(3.2.2)*
- **Certificate register** - a simple version-controlled CSV of security-staff certifications (holder, credential, issuer, expiry) turns scattered PDFs into checkable evidence. *(3.2.2)*

Reconciliation and Compliance Automation

- **PowerShell / Python join scripts** - join the directory export against the LMS export and emit an exceptions list (enabled users with no current training). Run quarterly; archive the output. *(3.2.1)*

- **OSCAL** (NIST Open Security Controls Assessment Language) - represent the 3.2 implementation statements and assessment results in your SSP as JSON/XML/YAML alongside the other families. *(all AT)*

Practical tip: for every export, record what was run, on which system, and when. A traceable, dated artifact is worth far more than an undated screenshot.

Conclusion

Awareness and Training is the least technical family and among the easiest to fully satisfy - yet its two 5-point Basic requirements make it one of the most expensive to neglect. Stand up one awareness platform synced to the directory, define a role-to-training matrix, add insider-threat content with a named reporting channel, run phishing simulations on a schedule, and export the completion records. Ten SPRS points and a clean family assessment follow from a program most organizations can implement in weeks.

The July 2026 suspension of CMMC Phase 2 paused the third-party certification milestone, not the underlying obligation: NIST SP 800-171, DFARS 252.204-7012, and the Level 2 self-assessment remain fully in force. Implementing this family well is still required today.

Glossary of Acronyms

API	Application Programming Interface
CDSE	Center for Development of Security Excellence
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CPE	Continuing Professional Education
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
FIPS	Federal Information Processing Standard
GCC	Government Community Cloud
ISSO	Information System Security Officer
LMS	Learning Management System

MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OSCAL	Open Security Controls Assessment Language
PAM	Privileged Access Management
POA&M	Plan of Action and Milestones
SAT	Security Awareness Training
SCIM	System for Cross-domain Identity Management
SCORM	Sharable Content Object Reference Model
SPRS	Supplier Performance Risk System
SSP	System Security Plan
xAPI	Experience API (Tin Can API)

About Methodical Security

Methodical Security provides resources and tooling to support Defense Industrial Base organizations through CMMC / NIST SP 800-171 assessments. Its platform, **Certalo**, works at the determination-statement level: it maps your existing documentation to each objective, flags where evidence is thin, and compresses the path to a submission-ready SSP, Assessment Report, and SPRS package. The result turns a one-time compliance scramble into a repeatable process — protecting current revenue and opening new contract eligibility.