CYBERSHEATH

AIM for Compliance: A Practical Playbook for CMMC Readiness

From Ongoing Operations to Audit-Ready Evidence

Manage: Sustaining and Demonstrating Long-Term Compliance

Meeting NIST SP 800-171 requirements and CMMC requirements is an important achievement. But what follows—sustaining that compliant state—is where organizations truly separate themselves.

The Manage phase of the AIM framework is about transforming compliance requirements into day-to-day operational practice, building the habits, ownership, and governance structures that ensure you remain operationally resilient and assessment-ready every day.

Compliance is not a project with an end date. It's a long-term operational commitment requiring continuous execution, evidence collection, and adjustment as your environment evolves. The Manage phase ensures that your documented controls consistently align with how you actually operate.

STAGE 1

Establishing Ownership and Accountability

The first requirement for sustaining compliance is clarifying who owns what. A recurring compliance task without an owner is a task that will eventually be forgotten. Ownership ensures consistency, accountability, and a clear chain of responsibility when processes change or issues arise.

Ownership extends across four operational domains:

Security Operations

Security practitioners carry out much of the hands-on, recurring work that demonstrates compliance. This includes reviewing logs, monitoring alerts, executing incident response procedures, and maintaining visibility across your environment. Their actions generate the operational evidence that assessors expect to review.

Technology and IT

Technical teams support compliance by maintaining configuration baselines, applying patches, updating systems, enforcing secure settings, and governing changes. Their operational discipline ensures that controls stay aligned with requirements even as the environment shifts.

Compliance and Governance

Compliance manager maintain the overarching structure: policies, control documentation, periodic assessments, evidence repositories, the SSP, and the POAM. Their responsibility is to maintain the integrity of your compliance program and ensure it reflects how the business functions.

Personnel and Physical Security

HR and facilities teams support personnel screening, onboarding, offboarding, and physical safeguards. Consistent execution of these functions ensures that the "people" side of compliance remains aligned with security and compliance requirements.

Effective management requires that every recurring task—log reviews, access audits, policy reviews, training cycles, incident simulations—has a named owner, a defined output, and a predictable cadence.

STAGE 2

Building Repeatable Cadence and Operational Rhythm

Compliance falters when tasks become ad hoc or dependent on memory. To remain continuously compliant, organizations must adopt a predictable operational rhythm. This rhythm transforms one-time tasks into repeatable processes executed on schedule.

A strong compliance calendar typically includes:

- Regular log reviews
- Recurring access reviews
- Scheduled vulnerability scans
- Annual tabletop exercises
- Policy and procedure reviews
- Periodic self-assessments
- Monthly or quarterly governance meetings
- Continuous evidence collection

These activities should occur with such consistency that they become part of the organization's operational DNA. When assessors ask, "How do you know this happens every week, month, or year?" you can point not only to procedures but to the evidence demonstrating consistent execution.

A documented cadence provides structure; assigned ownership provides accountability; repeatability provides confidence. While many activities follow a fixed schedule, others should be performed in response to significant organizational, technical, or regulatory changes.

STAGE 3

Treating Organizational and Technical Change as Compliance Events

Many compliance failures occur not because a control was never implemented, but because the business changed—and the compliance program did not change with it.

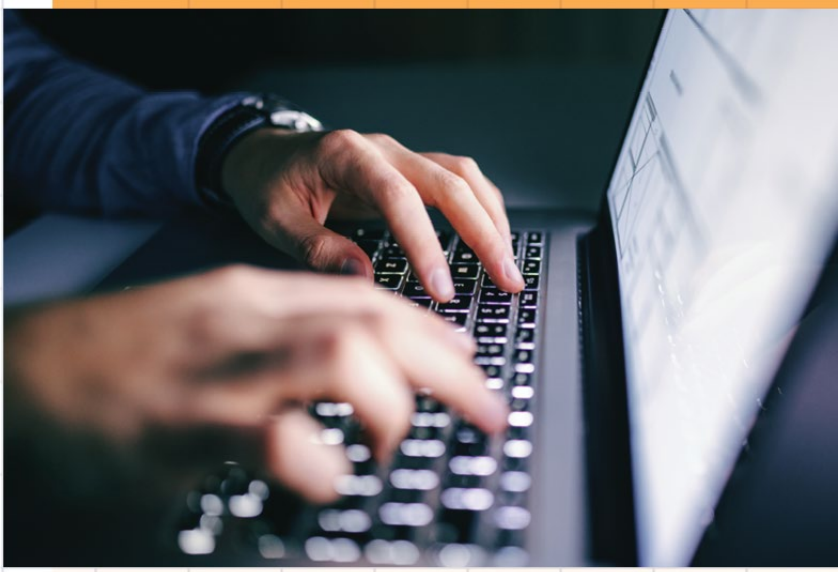
Any shift that affects your environment, workforce, systems, boundaries, or data flows should be treated as a compliance-impacting event. These include:

- Staff turnover or loss of institutional knowledge
- Cloud migrations, new platforms, or major upgrades
- Expansion of CUI use cases due to new contracts
- Adjustments to system boundaries or scope
- Organizational changes such as mergers or divestitures
- Introduction of new business processes involving CUI

When these changes happen, the compliance program must immediately respond by evaluating their compliance impact and, where necessary, reevaluating scope, revisiting CUI flows, updating the SSP, adjusting procedures, and collecting new evidence. The key question becomes: Would this change alter the story I tell an assessor?

If the answer is yes, the change must be managed accordingly.

The Manage phase builds the operational discipline to identify these shifts early, assess their compliance impact, and respond consistently.



STAGE 4

Maintaining Robust Evidence and Demonstrable Compliance

CMMC assessors evaluate objective evidence, not intentions. The Manage phase ensures that every applicable security practice produces clear, recent, and relevant evidence that aligns with your documented controls.

Evidence should naturally emerge from the work you do, including:

- System-generated logs
- Tickets and change approvals
- Records of access reviews
- Training confirmations
- Incident reports
- Meeting minutes
- Audit logs
- Assessment notes

Fresh evidence is essential. Even if a control is well-documented and technically implemented, assessors will expect to see recent evidence that the control is operating as intended. Many

requirements in NIST 800-171 specify operational verbs such as “monitor,” “maintain,” “review,” or “assess,” each of which implies repeatability and documentation.

Strong evidence management ensures that, at any moment, you can demonstrate not only that controls are implemented and operating effectively.

STAGE 5

Using the POAM as a Continuous Management Tool

In the Manage phase, the POAM becomes more than a remediation document—it becomes an operational dashboard. It is the mechanism through which you track deficiencies, exceptions, future requirements, and the status of corrective actions.

A well-maintained POAM supports:

- Tracking of identified gaps until closure
- Planning for upcoming changes
- Documenting risk-based decisions
- Identifying areas impacted by new NIST revisions
- Coordinating actions across teams
- Providing clear audit-ready visibility

Rather than reacting to findings, organizations with strong management programs use the POAM proactively, logging emerging issues before they become audit failures and tracking progress toward resolution.

STAGE 6

Recognizing What Successful Compliance Management Looks Like

A mature Manage program is defined not by perfection, but by predictability and alignment. Successful organizations share several characteristics:

- Controls are not only implemented—they operate consistently.
- Documentation reflects reality, not aspiration.
- Boundaries, scope, and CUI flows are well understood.
- Evidence is stored, current, and easy to retrieve.
- Owners understand their responsibilities and follow defined rhythms.

- Compliance activities remain intact during staffing changes, growth, or technological evolution.

In this state, the organization is consistently prepared for assessments. You no longer prepare hurriedly for assessments because the evidence, execution, and documentation are already aligned.

STAGE 7

Preparing for C3PAO Assessment and Sustaining Certification

As your Manage program matures, the next major milestone becomes external validation through a C3PAO assessment. The strength of your operational discipline directly influences the ease and success of this process.

Selecting a C3PAO

Not all assessors bring the same experience or perspective. Strong candidates understand defense industry operations, have experience with environments similar to yours, and demonstrate a consistent and well-supported understanding of the CMMC Assessment Process and applicable requirements. Engaging in early discussions and walking through sample requirements helps ensure alignment.

Understanding the Assessment Process

Although each C3PAO may have its own approach, assessments generally follow a consistent pattern:

- **Pre-Assessment Activities:** Before the formal assessment begins, the C3PAO coordinates scope, reviews required documentation, confirms assessment logistics, and ensures the organization is prepared for the scheduled assessment.
- **Evidence Collection and Review:** Assessors verify documentation, interview personnel, and validate evidence against assessment objectives.

- **Interview Phase:** This structured period involves objective-by-objective review, comparing your SSP narrative to operational execution. Demonstrations and evidence requests are common.
- **Trending and Evaluation:** Throughout the assessment, assessors evaluate each assessment objective, identify any deficiencies, and may request clarification or additional existing evidence before finalizing their findings.
- **Outbrief and Final Report:** Results are delivered, and deficiencies are documented. In some cases, organizations that meet specific criteria may receive conditional Level 2 certification, requiring closure of eligible POAM items within 180 days.

After Certification

Certification remains valid for three years, but this period requires ongoing adherence to assessed practices. Organizations are expected to maintain compliance throughout the certification period and complete required annual affirmations. Depending on contractual requirements, updates to SPRS or other reporting mechanisms may also be required. Significant scope changes may trigger reassessment.

Compliance as Strategic Business Risk Management

Maintaining certification is not simply about satisfying auditors. It protects contract eligibility and represents a critical business function tied to revenue and competitive advantage. Gaps must be treated as operational risks with formal governance, structured remediation, and executive oversight.

Staying Ahead of Evolving Standards

As organizations begin planning for adoption of NIST SP 800-171 Rev. 3, they should begin assessing future requirements today. The strongest programs anticipate regulatory shifts rather than scrambling to adjust. Continuous alignment with emerging standards keeps organizations ready for the next evolution of CMMC.

Closing Perspective: Managing Compliance for the Long Term

The Manage phase transforms compliance from a point-in-time activity into a disciplined operational function. It ensures that the work done during implementation becomes sustainable and demonstrable. With ownership, cadence, evidence, and governance in place, your organization is prepared not only for today's requirements but for tomorrow's challenges.

Organizations that master this phase remain secure, audit-ready, and aligned with contractual expectations—every day, not just during assessments.

CyberSheath works with defense industrial base (DIB) organizations at every stage of the CMMC journey. If you're looking to formalize your ongoing compliance program or prepare for an upcoming C3PAO assessment, our team is ready to help you get—and stay—audit ready. Contact us today to get started.