Compliance Decision Making Process
DFARS Edition

Release 2024.1

PUBLIC RELEASE AUTHORIZED

Executive Summary

Compliance with the US Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) requires a proactive approach to be efficient and effective. Proactive compliance can be thought of as having four (4) distinct components:

1. Decisions;
2. Intent;
3. Risk; and
4. Triggers.

The common military planning acronym associated with this is DIRT, which comes from the broader Military Decision Making Process (MDMP). In this document, we co-op concepts from DIRT & MDMP with a cybersecurity compliance-focused Compliance Decision Making Process (CDMP). This document helps define a viable process to tackle compliance-related decision making to minimize risk. Getting to the point of making a sound decision requires multiple supporting steps, which are explained in this document.

Compliance Decisions

There are many compliance-related decisions that organizations face. Decisions are often “forks in the road” where there is a binary option to take one path or the other, but not both. This is where the decisions are expected to be based on compliance intent and risk analysis. Examples of decisions that impact compliance include:

- The organization accepts a contract to store, process and/or transmit Controlled Unclassified Information (CUI) as part of a contract with a third party (e.g., government, prime contractor, partner, etc.).
- Action is taken to restructure supporting business processes to support the broader corporate strategy.
- The organization’s CUI enclave is onsite in its own segmented environment.

Compliance Intent

The compliance intent captures executive leadership’s intent for compliance operations. Decisions should be formed, based on compliance intent. Compliance intent:

- Provides the basis for unity of effort throughout the organization to justify cost/changes necessary to comply.
- Is meant to support the organization’s broader mission and strategy.
- Allows stakeholders to gain insight into what is expected of them, what constraints apply, and most importantly, why the compliance operations are being conducted.

Understanding of Risk

A clear understanding of compliance intent directly influences risk analysis. Understanding the nuances of compliance-related risk can lead to better decision making and that can lead to proper technology alignment, less unexpected change, etc. Examples of understanding risk include:

- The organization must avoid business engagements with third parties that store/process/transmit CUI that are not able to obtain and maintain CMMC L2 certification.
- While Security Protection Data (SPD) is unlikely to be designated as a CUI category by the US National Archives (NARA), the DoD is unlikely to alter its course that SPD must be protected in a manner that limits technology options.
- The majority of False Claims Act (FCA) submissions are made from insiders (often recently separated individuals), so compliance operations must have appropriate evidence of due diligence and due care to demonstrate the organization’s compliance efforts.

Compliance Triggers

Compliance operations are rarely static. Identifying triggers in the compliance landscape can refine risk management analysis and lead to proper decision making that stays inline with compliance intent. Examples of compliance triggers include:

- NIST releases NIST SP 800-171 R3.
- DoD issues a class deviation to remain aligned with NIST SP 800-171 R2.
- 32 CFR § 170.19(c)(2) designates External Service Providers (ESPs) as being considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits CUI or Security Protection Data (SPD).

CDMP Step 1: Awareness of Compliance Obligations

Substeps:

1. Establish a formal project to resource and manage the compliance process.
2. Conduct an initial assessment of the compliance mandate.
3. Determine the compliance intent.
4. Define the initial scope of compliance.
5. Identify applicable stakeholders.
6. Conduct a gap assessment.
7. Issue preliminary requirements guidance (including facts and assumptions) to stakeholders.
8. Monitor for evolving requirements / changes to compliance requirements.

Inputs:

- Source requirements (e.g., specific law, regulation and/or contractual obligation).
- Operational authority to conduct compliance operations within the organization.
- Documented roles and responsibilities.
- Documented stakeholders.

Outputs:

- Project plan (including running estimate for timeline and budget).
- Running Estimate
- Preliminary stakeholder guidance on compliance requirements.

Initial Assessment (internal to compliance team)

The initial assessment helps compliance staff determine:

- Time available from notification of compliance obligation to the compliance deadline.
- The compliance staff's Subject Matter Expertise (SME) with the DFARS requirements (e.g., NIST SP 800-171 & CMMC).
- The reasonable scope of the compliance efforts.
- Which consultants and/or External Service Providers (ESP) require contact and incorporation into the planning process.

Running Estimate (shared with stakeholders)

Running estimates helps stakeholders with understanding the situation, assessing progress and making effective decisions throughout compliance operations. Effective compliance plans and successful executions hinge on current and accurate running estimates with relevant information. A running estimate contains:

- Identify facts (initial).
- Identify assumptions (initial).
- Organizational status, including third-parties that affect compliance efforts (e.g., gap assessment results).
- Organizational / third-party capabilities (initial assessment).
- Organizational / third-party constraints (initial assessment).
- Initial conclusions and preliminary recommendations with associated risk.

CDMP Sept 2: Identify Facts & Assumptions

Substeps:

1. Determine facts that affect compliance operations.
2. Determine assumptions that affect compliance operations.

Inputs:

- Initial Assessment
- Running Estimate

Outputs:

- Facts
- Assumptions

It is imperative to separate facts from assumptions.

Facts

Facts are statements of truth, or statements thought to be true.

For example:

- *The organization stores and processes Controlled Unclassified Information (CUI) as part of a government contract.*
- *NIST SP 800-171 compliance has been a requirement since 1 January 2018.*
- *NIST SP 800 171 R3 was released on 14 May 2024.*
- *The DoD issued a class deviation to delay DFARS implementation of NIST SP 800-171 R3.*
- *Office of Management and Budget (OMB) requires organizations to adopt the most current version of NIST one year after its release.*
- *Per 32 CFR § 170.19(c)(2), an External Service Provider (ESP) will be considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits CUI or Security Protection Data (SPD).*

Assumptions

Assumptions are essentially gaps in knowledge or information that need to be confirmed or denied.

For example:

- *Before NIST SP 800-171 R2 is deprecated in May 2025, the DoD will remove the class deviation for DFARS to transition to NIST SP 800-171 R3.*
- *The DoD may realize that the Defense Industrial Base (DIB) would be under undo financial pressure to adjust its technologies, ESP and business processes to treat SPD as CUI.*

Transitioning assumptions to facts is the goal during planning, as it builds situational understanding and validates planning efforts. Presumptive planning is acceptable, if stakeholders understand the planning is based on assumptions. Compliance staff may continue to plan with assumptions to avoid hindering planning efforts or degrade timelines. For assumptions, planners are expected to use historical data, intuitive analysis and judgment to determine risk.

CDMP Step 3: Define A Problem Statement

Substeps:

1. None

Inputs:

- Initial Assessment
- Running Estimate
- Facts & Assumptions

Outputs:

- Problem Statement

Solving a problem is the driving reason for compliance planning processes. Problem statement development begins with identifying the problem. To identify the problem, it requires compliance staff to determine answers to two questions:

1. *What is the difference between the current state of the operational environment and desired state?; and*
2. *What is preventing the organization from reaching the desired end state?*

The problem statement is a concise statement of the obstacles preventing an organization from achieving a desired end state. The problem statement should include only the significant elements of the problem framing. In this way, the problem statement becomes concise, yet remains relevant to the rest of the problem-solving process.

An example problem statement might be:

How does ACME adjust its business operations and adopt the right technologies to comply with the US Department of Defense's (DoD's) Cybersecurity Maturity Model Certification (CMMC)?

- *The requirements are numerous and constrict the ability of ACME's internal business units to share data with necessary stakeholders.*
- *ACME has three (3) IT and one (1) cybersecurity personnel on staff, so staffing strength is limited.*
- *Not all existing technologies in use at ACME meet the rigorous compliance requirements.*
- *ACME is receiving pressure from its vendors to demonstrate compliance with CMMC, where a failure to demonstrate compliance, or a viable path to compliance, will result in cancelled contracts.*

CDMP Step 4: Determine Constraints

Substeps:

1. Determine resourcing limitations.
2. Determine technical limitations.
3. Determine conflicting business processes.

Inputs:

- Running Estimate
- Facts & Assumptions
- Problem Statement

Outputs:

- Constraints

A constraint is a restriction placed on compliance efforts, generally from either (1) a technical limitation or (2) a conflicting business practice. A constraint dictates an action, inaction or technical limitation that affects compliance efforts.

There is never enough money, people or time for cybersecurity-related compliance operations. Therefore, it is necessary to clearly identify the applicable constraints that affect compliance operations. This includes, but is not limited to:

- Budgetary resources.
- Available personnel with sufficient subject matter expertise.
- Timeline.
- Technical limitations.
- Existing contractual obligations.

Technical Limitations

Technical limitations are going to be specific to the law, regulation and/or contractual obligation. There may be systems, applications and/or processes that are unable to meet configuration requirements.

For example:

- *An old manufacturing computer that uses an unsupported operating system. It is incapable of being patched or run the latest antimalware software.*
- *A firewall that is able to use AES-256 encryption, which is secure, but does not use a FIPS 140-2 validated cryptographic module.*

Conflicting Business Practice

Conflicting business practices may address the ability to control the environment where sensitive / regulated data is stored, processed and/or transmitted. Conflicting business practices generally lead to expanded compliance scopes.

For example:

- *Sensitive / regulated data is emailed via the corporate email system.*
- *Lack of visitor control through the manufacturing building.*
- *Remote / work from anywhere workforce.*
- *The use of contractors to perform work on projects with sensitive / regulated data.*

Step 5: Identify Possible Courses of Action (COA)

Substeps:

1. Analyze compliance intent.
2. Analyze facts, assumptions and constraints.
3. Determine decision points / triggers.

Inputs:

- Running Estimate
- Facts & Assumptions
- Problem Statement
- Constraints

Outputs:

- COAs

The US military defines a Course of Action (COA) as a “broad potential solution to an identified problem.” In all honesty, determining courses of action is based on making a Scientific Wild Ass Guess (SWAG), which essentially is an educated guess that is derived from available facts and assumptions. This does not make the process of determining COAs wrong by relying on SWAG, but it is something that decision makers must fully understand since risk can never be eliminated from the equation when there is a certain level of uncertainty that must be accounted for.

In the development of COAs is often helped by creating a unique COA for each of these questions:

1. *What scenario reflects the most advantageous outcome?*
2. *What scenario reflects the most disadvantageous outcome?*
3. *What scenarios are plausible that should not be discounted?*

Part of COA development involves clearly defining both the advantages and disadvantages of each scenario.

Advantages

Listing advantages of a particular COA are important for decision makers, but it is important for those developing the COAs to avoid skewing the benefits to meet a preferred narrative. While it is impossible to completely eliminate bias, it is crucial to be as objective as possible in the analysis of advantages.

For example:

- *No requirement to change ACME’s technology and/or third-parties.*
- *Ability to drastically reduce the scope of compliance.*

Disadvantages

Listing disadvantages of a particular COA are important for decision makers, but it is important for those developing the COAs to avoid skewing the negatives to meet a preferred narrative. While it is impossible to completely eliminate bias, it is crucial to be as objective as possible in the analysis of disadvantages.

For example:

- *Significant cost and time delay to change ACME’s technology and/or third-parties.*
- *Expansion of the scope of compliance.*

EXAMPLE
Defining Facts, Assumptions & COAs

Problem Statement

Per the CMMC Proposed Final Rule (32 CFR), an External Service Provider (ESP) will be considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits (S/P/T) CUI or Security Protection Data (SPD). Per DFARS 252.204-7012(b)(2)(ii)(D), if ACME intends to use a Cloud Service Provider (CSP) to S/P/T any Covered Defense Information (CDI) in performance of its contract, ACME must ensure its CSP are either FedRAMP certified of meet security requirements equivalent to the FedRAMP moderate baseline.

How does ACME adjust its business operations and adopt the right technologies to comply with the US Department of Defense's (DoD's) Cybersecurity Maturity Model Certification (CMMC) for SPA & SPD?

- The requirements are numerous and constrict the ability of ACME's internal business units to share data with necessary stakeholders.
- ACME has three (3) IT and one (1) cybersecurity personnel on staff, so staffing strength is limited.
- Not all existing technologies in use at ACME meet the rigorous compliance requirements.
- ACME is receiving pressure from its vendors to demonstrate compliance with CMMC, where a failure to demonstrate compliance, or a viable path to compliance, will result in cancelled contracts.
- An ACME executive will be required to make an annual affirmation in Supplier Performance Risk System (SPRS).

Facts

- ACME S/P/T CUI as part of a government contract.
- NIST SP 800-171 compliance has been a requirement since 1 January 2018.
- NIST SP 800 171 R3 was released on 14 May 2024.
- The DoD issued a class deviation to delay DFARS implementation of NIST SP 800-171 R3.
- Office of Management and Budget (OMB) Circular A-130 requires organizations to adopt the most current version of NIST one year after its release.[1]
- Per 32 CFR § 170.19(c)(2), an External Service Provider (ESP) will be considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits CUI or Security Protection Data (SPD).
- ACME currently does not treat SPD in the same manner as CUI.
- ACME's current ESPs and CSPs are not:
    - CMMC L2 certified;
    - FedRAMP moderate certified; or
    - FedRAMP moderate equivalent.
- Until the CMMC Final Rule is published, ACME's current compliance requirements for DFARS 252.204-7012 is to document ACME's CUI environment in a System Security Plan (SSP) and track deficiencies per a Plan of Action & Milestones (POA&M).

Assumptions

- Before NIST SP 800-171 R2 is deprecated in May 2025 (per OMB A-130), the DoD will remove the class deviation for DFARS to transition to NIST SP 800-171 R3.
- Before NIST SP 800-171 R3 is enforced, the DoD will release "CMMC 3.0" to address changes from NIST SP 800-171 R3.
- The current technology in use at ACME to S/P/T SPD may not be compliant with the CMMC Final Rule.
- The DoD may realize that the Defense Industrial Base (DIB) would be under undo financial pressure to adjust its technologies, ESP and business processes to treat SPD as CUI.

Constraints

- Available ESP and CSP that are capable of S/P/T SPD, per the CMMC Proposed Final Rule.
- Budget constraints to re-engineer the CUI environment for (1) new technologies or (2) new third-parties to
- Obtaining FedRAMP certification is not easy. FedRAMP certification generally requires a sponsor (e.g., government client). Approaching FedRAMP certification without a sponsor requires the CSP to through the Joint Authorization Board (JAB) process. The CSP would have to work with a FedRAMP CPAO to get the CSP's evaluated as being in a FedRAMP

[1] OMB A-130 - https://csrc.nist.gov/csrc/media/Presentations/2021/omb-circular-a-130-implementation-and-updates-to-s/images-media/Federal_Cybersecurity_Privacy_Forum_2Dec2021_NIST_SP800-53update.pdf

ready state and then petition the FedRAMP JAB to accept the CSP's authorization package. Given that the JAB process only selects around 12 packages per year, this reduces the odds of unsponsored FedRAMP certification for most CSP.

Courses of Action (COA)

COA 1: Do nothing and wait for guidance.

COA Description: ACME continues addressing applicable NIST SP 800-171 R2 and CMMC 2.0 requirements and does not make any technology / service provider changes until it absolutely has to. With CMMC being an utter shit show, once the CMMC Final Rule is published there will likely be several years grace period to then become compliant.

Advantages:

- Short-term minimization of cost / change.

Disadvantages:

- Potential loss of market share to ACME's competitors that are able to earn a CMMC certification before ACME.

COA 2: Perform a technology/service provider migration.

COA Description: ACME takes the proposed rule at face value, which necessitates changes to how SPA & SPD are treated. This requires new technology investment and potentially new business relationships with third-party vendors.

Advantages:

- Potential marketing win against ACME's competitors who choose to do nothing.
- A potentially more secure environment to protect SPA / SPD.

Disadvantages:

- Limited options for technology solutions and/or compliant CSP/ESP.
- Significant changes to business processes and technology architecture.
- Cost associated with breaking existing contracts / service agreements.
- Effort could be for nothing if the CMMC Final Rule loosens requirements.

COA 3: Stick it out with existing technologies / service providers.

COA Description: ACME takes a guarded "wait and see" approach to the CMMC Final Rule, where ACME will make a reasonable effort to work with existing technologies and CSP/ESP to address changes.

Advantages:

- Short-term minimization of cost / change.
- No short-term costs associated with breaking existing contracts / service agreements.
- ACME's existing technology providers and CSP/ESP will have a vested interest in rapidly evolving their offerings to keep ACME as a client.

Disadvantages:

- Potential loss of market share to ACME's competitors that are able to earn a CMMC certification before ACME.