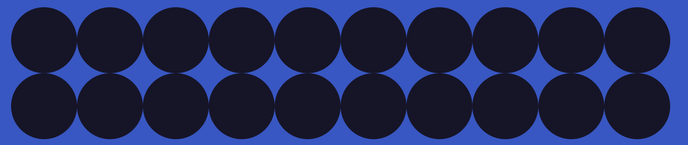
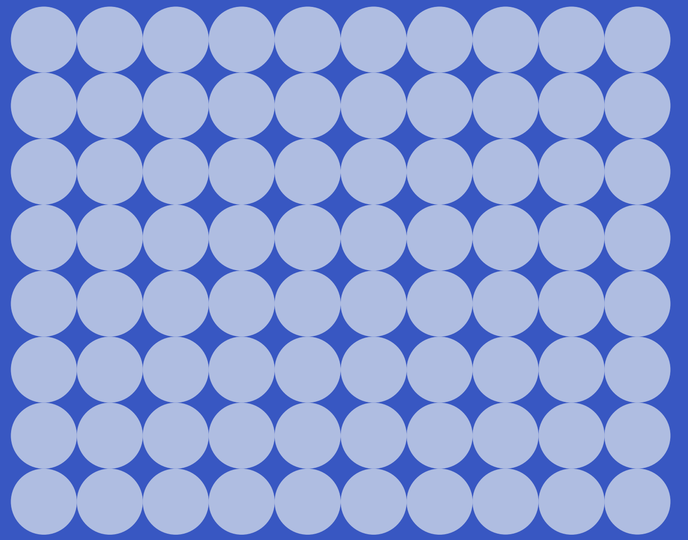
C3 INTEGRATED SOLUTIONS

YOUR CMMC RESPONSIBILITY



OURS



C3 COMMAND

Breaking down C3's Shared Responsibility Philosophy

Introduction

C3 Integrated Solutions is a specialized services provider that designs, implements, and manages IT & compliance solutions purpose-built for the U.S. Defense Industrial Base.

Our most comprehensive CMMC solution, C3 Command, has been explicitly constructed to meet the technical, operational, and administrative requirements of CMMC compliance.

In developing C3 Command, we wanted to provide defense contractors with an end-to-end solution, optimized for speed and CMMC compliance assurance, that:

01. **Encompassed the entire compliance boundary** so that contractors didn't have to figure out the gaps
02. **Eliminated the need to manage multiple service providers** and their corresponding shared responsibility matrices
03. **Dramatically reduced the time and effort** required from internal employees

These three objectives led us to embrace a much more comprehensive approach to shared responsibility than is otherwise available in the market, or even our other services and solutions.

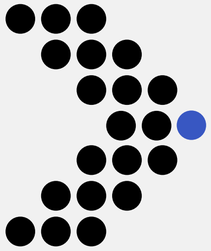
In this document, we explain C3 Command's proactive approach to shared responsibility and provide a high-level overview of our commitment to take responsibility for meeting **~80% of your company's CMMC Level 2 assessment objectives.**

> The Shared Responsibility philosophy outlined in this document is exclusive to C3 Command, C3's most comprehensive solution. Not all companies will be eligible to participate in C3 Command.

C3’s Shared Responsibility Philosophy

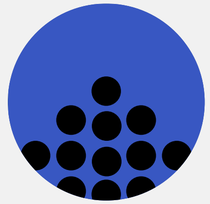
Exclusive to C3 Command, the C3 Shared Responsibility Model is our approach to leadership, responsibility, and ownership in your CMMC compliance journey.

It’s anchored around **three core principles:**



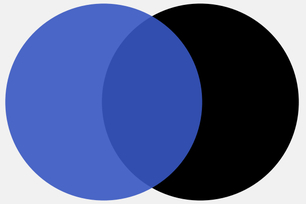
01.

WE LEAD CMMC COMPLIANCE EFFORTS; WE DON’T JUST “ASSIST” THEM.



02.

OUR SOLUTION SHOULD ADDRESS YOUR ENTIRE COMPLIANCE BOUNDARY, NOT JUST A PORTION OF IT.



03.

OUR RESPONSIBILITY EXTENDS BEYOND IT TO INCLUDE DOCUMENTATION, POLICIES, AND EVIDENCE.

By designing C3 Command around this philosophy, we’ve not only considered how to take you through your first assessment successfully, but also how to make it easy for you to maintain compliance year after year.

320 responsibilities

C3's customer responsibility matrix is designed to communicate roles and responsibilities associated with the cybersecurity requirements outlined in NIST Special Publication 800-171 Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and as required to meet Level 2 compliance for the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) program.

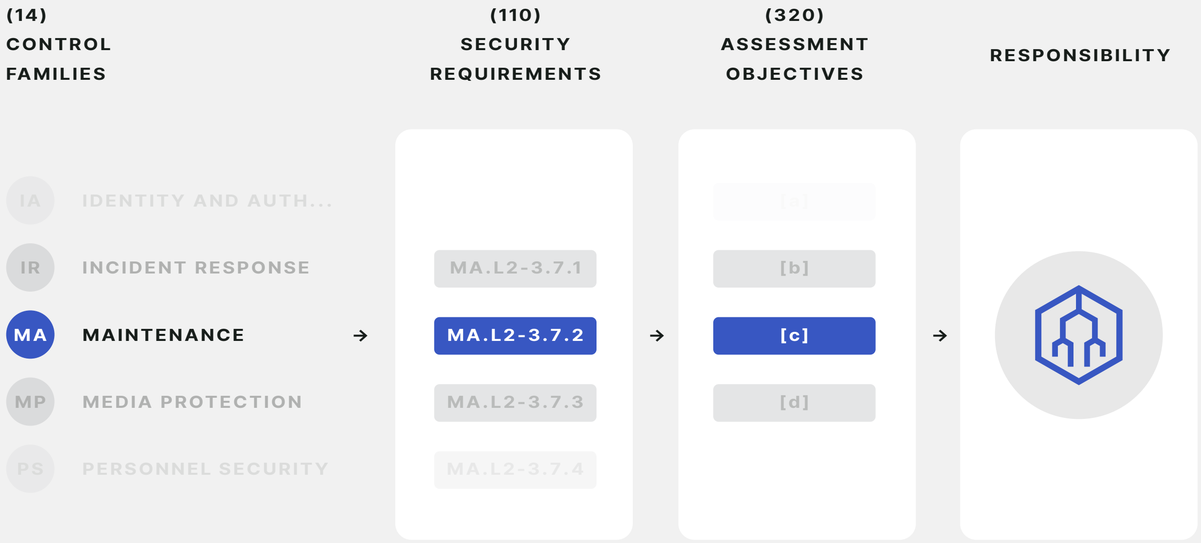
The Requirements

NIST SP 800-171 breaks down its requirements into 110 security requirements (sometimes known as "cybersecurity practices" or "controls") across 14 Security Requirement Families (often referred to as "control families" or "domains").

A companion document, NIST Special Publication 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*, breaks the 110 controls down more granularly into 320 specific assessment objectives against which your organization will be measured during the assessment.

C3 has elected to map our Customer Responsibility Matrix to the more detailed 320 assessment objectives.

We've found that even within the same control, responsibility can and often should shift from assessment objective to assessment objective.



The responsibility breakdown

NOTE: While responsibility for meeting a specific assessment objective may fall to a third party, ultimately, the Organization Seeking Certification (OSC) ultimately owns their own compliance and is accountable for validating that work.

For C3 Command, assessment objective responsibility will fall into one of three categories:

C3 INTEGRATED SOLUTIONS

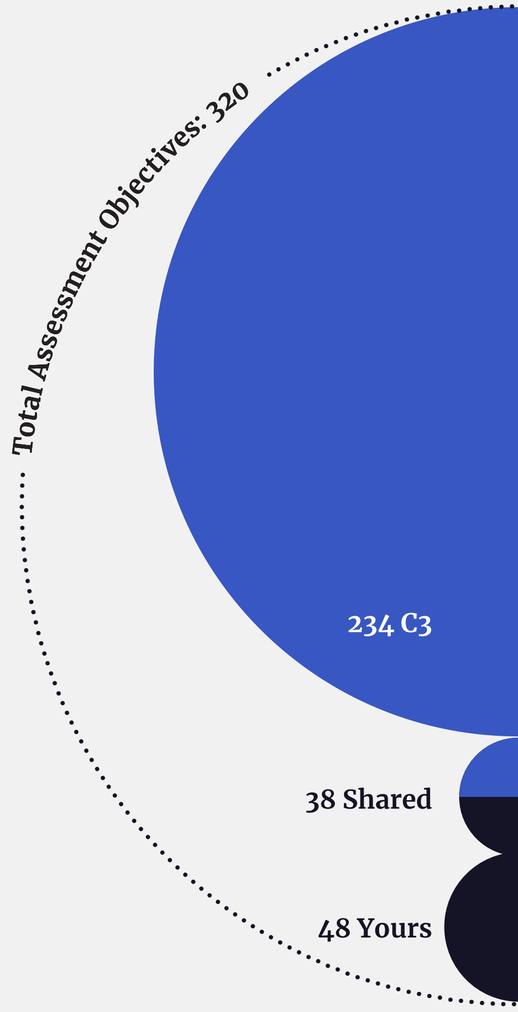
C3 is solely responsible for meeting this objective (though we may need your confirmation or support). In our model, C3 is solely responsible for 234 (73%).

SHARED

We share responsibility for meeting this objective. You and C3 are jointly responsible for 38 (12%).

CLIENT

The client is solely responsible for meeting this objective (though the C3 team typically consults to support you). In C3's shared responsibility matrix, you are solely responsible for 48 (15%).



What falls in your responsibility?

25 RELATE TO PHYSICAL OBJECTS & PREMISES

12 INVOLVE IDENTIFYING SOMETHING

11 RELATE TO INTERNAL PROCESSES

Of the 48 assessment objectives that fall solely under the client's responsibility, some patterns emerge:

- **25 out of the 48 relate to *physical* objects and premises.** C3 isn't responsible for physical objects in your possession. This means that you'll always be responsible for protecting and handling paper CUI and portable storage drives (Media Protection), as well as physical access to your systems and your physical premises, such as escorting visitors and monitoring physical access (Physical Protection and Configuration Management).
- **12 of the remaining 23 involve *identifying* something.** You know your business in ways that we never could. As a result, these tasks fall under your responsibility because we'll need you to identify the software you need to use, the external sites and systems you need to access, the mobile devices you're using that need to handle CUI, the customers you need to report incidents to, etc.
- **Of the remaining 11,** some relate to internal processes around posting to publicly accessible systems or incident response, while others involve authorizations, permissions, custom software development, or defining parameters unique to your business processes.

Generally, those same guidelines also apply to shared responsibilities. For example, C3 runs background checks on all its employees (Personnel Security), and ensures they are given role-based security training (Awareness and Training). But you are responsible for screening your own people and ensuring they are adequately trained. That's why we share responsibilities in those domains.

Adopting the RACI model

At its most detailed level, the C3 Customer Responsibility Matrix (CRM) associated with the C3 Command adopts a RACI (responsible, accountable, consulted, and informed) model.

Achieving CMMC compliance requires a combination of technology, design, and specialists in IT, security, and compliance.

- **SYSTEMS ARCHITECT** designs the architecture
- **SYSTEMS INTEGRATOR** implements the architecture to specifications
- **MANAGED SERVICES PROVIDER** manages, maintains, and updates the system
- **SECURITY PROFESSIONAL** monitors for and mitigates cybersecurity risks
- **COMPLIANCE PROFESSIONAL** orchestrates and validates compliance efforts

With C3 Command, C3 performs all of these roles, a critical advantage since very few defense contractors have all of these specialists on staff.

RACI categories are defined as follows:

R

RESPONSIBLE
This is the party doing the actual work.

A

ACCOUNTABLE
This is the party that owns the work's outcome.

C

CONSULTED
This party is sought after for advice and validation by the responsible party.

I

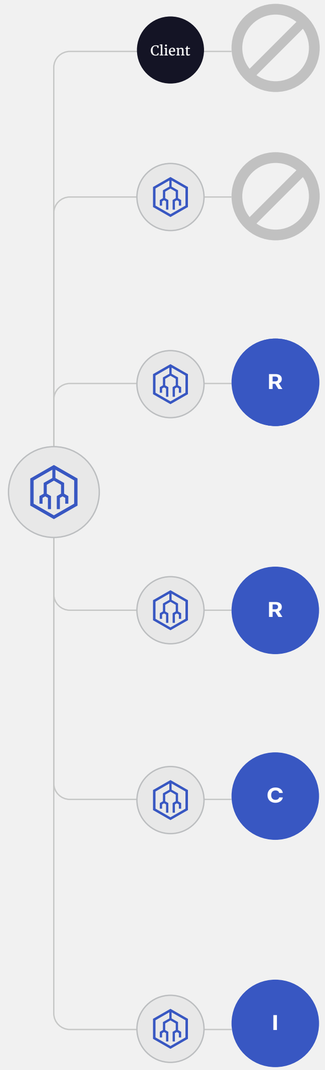
INFORMED
This is an interested party who observes the work or is notified of the outcome.

The RACI model in practice

In this diagram, you can see how we've extended RACI to ensure clear ownership among our own teams so that no assessment objective will slip through the cracks.

SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.	3.14.4[a]	Malicious code protection mechanisms are updated when new releases are available

With C3 Command, we orchestrate all this for you, but you can imagine how complicated it would be to maintain a master responsibility matrix when you use multiple providers to support your CMMC compliance efforts!



CLIENT

The client has **NO RESPONSIBILITY** in achieving this assessment objective.

SYSTEMS INTEGRATOR

The Systems Integrator has **NO RESPONSIBILITY** in achieving this assessment objective.

SYSTEMS ARCHITECT

The Systems Architect is **RESPONSIBLE** for updating malicious code protection configurations when enhancements and new releases are available.

MANAGED SERVICES PROVIDER

The Managed Services Provider is **RESPONSIBLE** for ensuring malicious code protection mechanisms remain up to date.

SECURITY PROFESSIONAL

The Security Professional is **CONSULTED** regarding malicious code protection configurations when enhancements and new releases are available.

COMPLIANCE PROFESSIONAL

The Compliance Professional is **INFORMED** when malicious code protection mechanisms receive a material update.

Pass the assessment. Period.

As you evaluate partners for your CMMC journey, we hope that this document has helped provide you an understanding of the deep consideration and technical depth that has gone into C3 Command.

C3 Command has been designed to meet one specific goal: The successful achievement of CMMC Level 2 certification. Since C3 Command takes into consideration your entire compliance boundary and takes responsibility for and/or supports non-IT requirements such as documentation, evidence gathering, and policy development and management, our Customer Responsibility Matrix for C3 Command is the only one you will ever need.

As you engage with us, we'll welcome the opportunity to walk through our Customer Responsibility Matrix with you. It's a tangible example of our commitment to helping you achieve certification and CMMC certification requirements and ensures that nothing is left to miscommunication or chance.

We hope to have the opportunity to partner on your CMMC compliance journey.