2024

Funding and Scoping for CMMC 2.0

CRITICAL PRISM DEFENSE LLC
HTTPS://CRITICALPRISMDEFENSE.COM

23 FEBRUARY 2024

Revised edition to update information from CMMC 1.0 to version 2.0

Contents

Table of Figures

Introduction

Companies are currently considering how to fund cybersecurity projects. In the wake of the COVID-19 pandemic, companies are now evaluating how they might fund initiatives necessary to move their businesses towards compliance with the Cybersecurity Maturity Model Certification (CMMC). There are a few ways to fund these initiatives, but many key items have the potential to impact the amount of funding needed to prepare your organization for certification. The important part is to

understand where your compliance program is today, so you can better visualize how to get it to where it needs to be.

Whether your company plans to meet the CMMC objectives or to stop doing business with the Federal Government, keep in mind that cybersecurity is an important part of maintaining your business health and ensuring resilience in the future. The number of small businesses failing due to cyber-related risks is rapidly increasing. When businesses suffer a cyber-attack and cannot afford the cost to recover, they often go bankrupt. If you believe that you can just purchase insurance to cover those expenses, think again. Insurance companies have increased premiums around 32% just this past year, and many of them are requiring an audit for compliance with a cybersecurity framework.

In addition to the new federal regulations being pushed out by the Defense Federal Acquisition Regulations (DFARS), many states have laws requiring levels of protection for different types of information. If your business operates in those states or does business with people or businesses in those states, you still have the state laws and regulations to follow. Other federal governments have also enacted cybersecurity protection measures for their citizens (such as GDPR). Not doing so can also leave you open to lawsuits in the event of a breach or incident.

Data protection is commonly referred to as a cybersecurity requirement, but it is the entire business that uses data, and the entire business that must work together to properly protect information to avoid lawsuits, loss of intellectual property, reduce insurance costs, reduce the risks of a data breach, reduce risk of financial loss, provide clients some level of assurance their information is protected, protect your company brand, enable trust in your business, protection of your company's reputation and most of all – to do what is ethically correct.

This paper is not to provide your organization with legal guidance or legal representation, nor does it claim to be an authoritative source. This is to assist your organization with navigation through a compliance journey and to provide ideas on options to make your own business and risk decisions. The numbers presented are considered rough orders of magnitude (ROM) for estimating costs to assist your organization with planning, not to be considered an actual cost or expected cost.

Phases for compliance

The general, a company should consider five phases in their approach to cyber security compliance (Figure 1: Compliance Journey):

1. Scope. We must understand the Scope that the compliance requirements apply to. This can include activities such as mapping data flows or user workflows, controlling their Scope wherever possible.
2. Gap Assessment. Perform a Gap Assessment to measure your current compliance posture for the Scope identified in comparison to your compliance requirements. The results of unmet compliance requirements will be entered into a Plan of Actions and Milestones (POA&M).
3. Cross Walk. Perform a Compliance Crosswalk during the Gap Assessment to see what controls, policies, processes, procedures, and practices you have already implemented from other compliance requirements for your Scope.
4. Remediation. Implementation of identified remediation strategies identified during the Gap Assessment and Cross Walk that was entered into the POA&M.
5. Formal Assessment. Receiving the Formal Assessment from an authorized assessment team for the certification you are applying for.

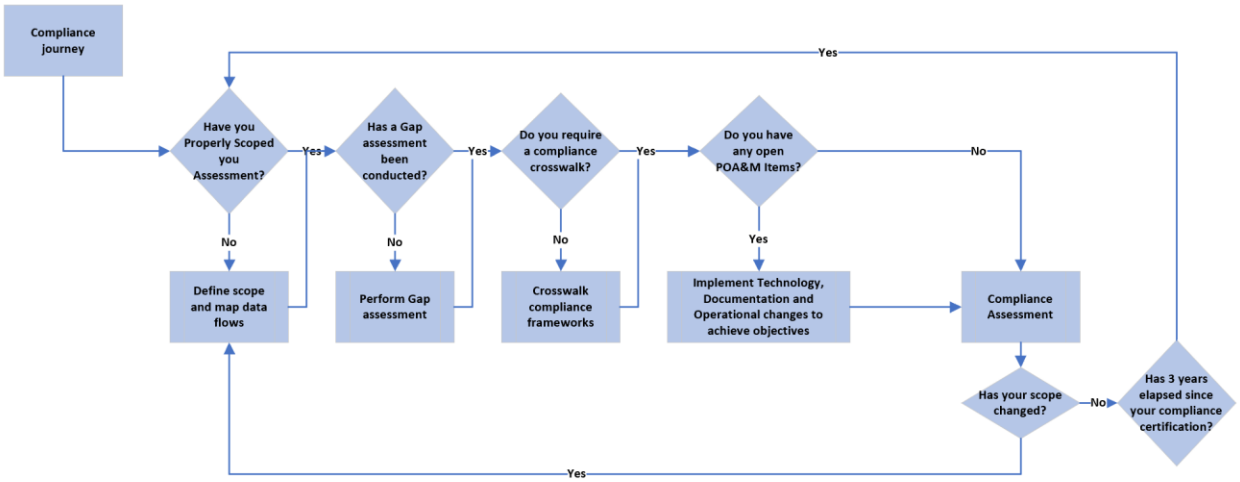

Figure 1: Compliance Journey

What are my costs?

Scope

You will need to define the Scope of your organization that the regulation applies to. This means understanding the type of information you receive, the security requirements for that data, who receives it, where it goes, how it is stored, how it is processed, and finally where you may need to share it with others outside of your organization. When you understand how the sensitive data flows through your organization, you can then map out all the people, technologies and products that touch that information (in transit, at rest, or by processing the information). This becomes your Scope.

1. Peter is our business manager. He uses his laptop to access the government procurement bids website and download documents that contain Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Peter stores this information on his local computer and will post it to the file share for the bid team to access. The bid team takes the contract, creates a requirements document, and uploads it into the requirements tool. Each member of the bid team will generate their responses for the proposal and develop technical documents for it. All the documents go into the requirements tool. Peter then takes all the documents out of the requirements tool and sends it over to the costing team to enter into their Enterprise Resource Planning (ERP) tool to develop the costs for the work. Peter will then email out the proposal response to the government. The data from each location is backed up into the enterprise backup tool, which is in the cloud. Peter can access his email from his company cell phone when working remotely.

When you develop a proposal as a response to a Request for Proposal (RFP) from the government, you will typically "Scope" the work. Your organization will fabricate 10 screws that meet the desired specifications and deliver them within one week to a specified address at a cost of $15.00 for the screws and $2.50 for shipping. What if they change that address and now it will cost you an additional $2.50 to ship them? That is a change in Scope, is it not? Your then agreed upon price should be $15.00 for screws and $5.00 for shipping.

When the Scope changes, the terms will change as well. If your organization implemented NIST SP800-171 controls to a specific Scope of your organization and organizational systems, but now a new contract is requiring you to expand that Scope, shouldn't there be an equitable adjustment there? Using the same scenario, you will need to manufacture 10 screws (all the same requirements) and now they want 10 nuts to fit those screws. The nuts and screws are created using different computers and manufactured on different equipment, so your Scope has changed (Figure 2: Change in Scope). You now need to apply organizational practices and implement technical solutions to ensure compliance is achieved.

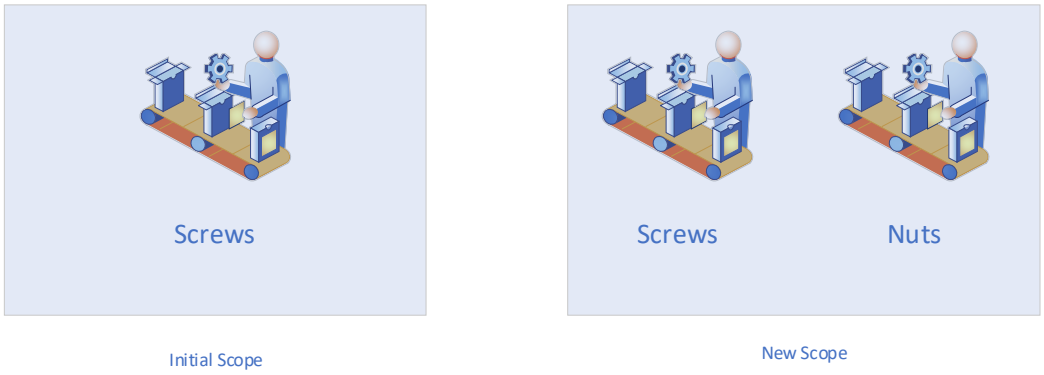

Figure 2: Change in Scope

Another method of scoping uses your organizational structure. You can split out into business units to shrink the Scope down and start separating your technology and people into those groups. If there are shared resources at the enterprise level, the compliance requirements would flow up to the enterprise level. This may dictate having multiple instances of that resource or adopting the most restrictive compliance requirements to that asset (Figure 3: Scope for your business units).

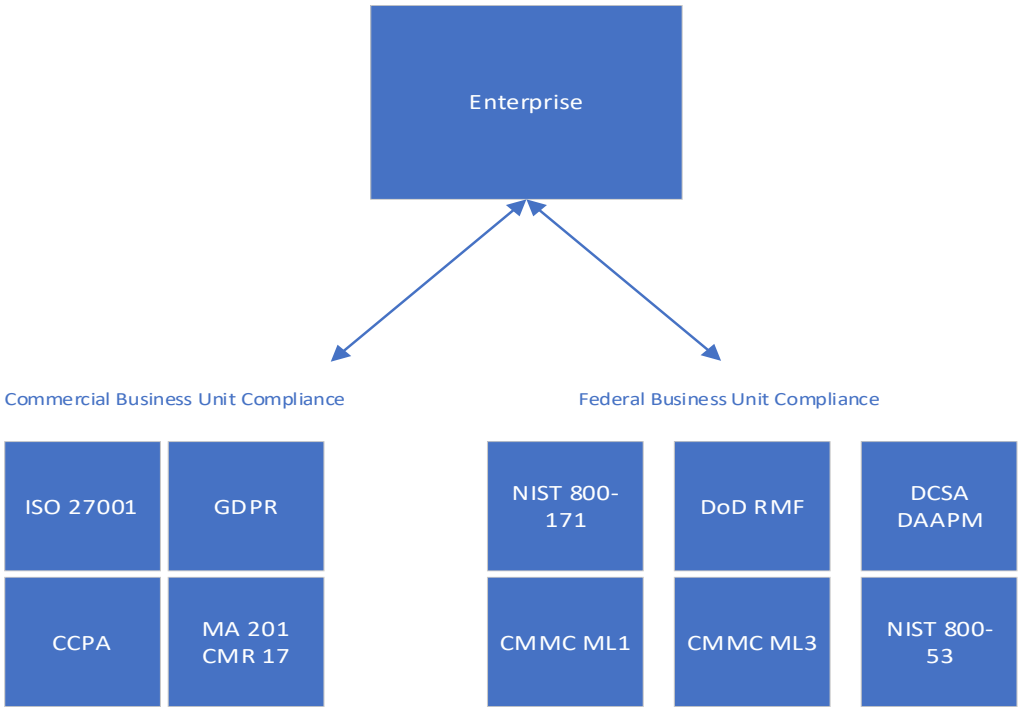

Figure 3: Scope for your business units

Scoping will vary based on your organization, and some of these activities should be conducted at reoccurring intervals through processes. Many organizations may do this through their ISO 9001 internal audit process; others may do this through their contract's compliance process.

Understand your requirements in contracts. We will focus solely on ones related to CMMC, but it should be conducted across all your contract requirements in general.

Contract	FAR 52.204-21	DFARS 252.204-7012	DFARS 252.204-7019	DFARS 252.204-7020	DFARS 252.204-7021	DFARS 252.239-2010
ABC	X	X				
XYZ	X	X	X	X		X
123	X					

Figure 4: Contract Requirements Review

Make it a point to review information you have for each of your contracts, in order to determine what information is considered FCI or CUI, as well as to map out how the data flows between systems and users. The locations, technology, and people that the information flows through will be the Scope of your CMMC compliance program.

Review the data flows to see which ones are unnecessary or can be eliminated by restricting access to necessary pieces of information. Your organization may decide to completely change its data flow to reduce the Scope overall. Instead of the government or prime contractor emailing you information, you may agree that you will review the CUI information in their systems over the internet, so your organization is reduced to a ML1 assessment instead of a ML3.

Scoping your assessment boundary should be one of the first steps you take, as it will drive all other costs, estimates and assumptions going forward. A representative from each part of the organization that handles FCI or CUI should be involved. If you do not know who that is yet, then identifying these components will be a part of the scoping process. Use a whiteboard and draw out how your data flows into your organization from the origin (government, prime contractor, collaborator). Identify who uses it, as well as what resources that data is stored in, processed in, or transmitted over. Do not forget how the data flows out of your organization!

Assume it will be a team of 2 people for 40 hours each (over a period of time) for a micro business. For small businesses, it may be 5-10, and for a medium nosiness it may be 10-20. You will also need to calculate a level of complexity, because not all organizations deal with large amounts of sensitive data. Alternatively, their Scope may be so limited (paper copies, or primarily use a prime contractor information system for the information) that there should not be a lot of work involved.

Micro: 2 * 40 * 200 * .5 = $8,000.00
Small: 5 * 40 * 200 *1.0 = $40,000.00
Medium: 10 * 40 * 200 * 2.0 = $160,000.00

CMMC Gap Assessment

Once the Scope is identified, you can assess that Scope against the regulation. This is a Gap Assessment. For example:

1. Do the file server, email server, bid team computers, ERP tool, requirements tool, and bid team members meet requirement AC.L2-3.1.19, which requires encrypted CUI on mobile devices and mobile computing platforms? [a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified; [b] encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.
    a. If yes to both [a] and [b], mark as compliant.
    b. If not, what solution will you pursue to meet this requirement and what is the cost to implement this?
        i. The required remediation should go into a Plan of Actions and Milestones (POA&M) document.

This is a compliance assessment of your organization and systems to identify where there may be "gaps" in what is currently in place to meet the compliance requirements. Gap Assessments should be performed by someone experienced with assessing technology and business processes. To complete a comprehensive assessment, you may need to engage a third party. This is a cost that you should absolutely prepare for, as it is the best way to avoid costly design mistakes or a false sense of compliance. The cost of a Gap Assessment can be difficult to pass on to an organization requesting you to be compliant. You can also conduct a Gap Assessment using in-house staff; however, they should be independent of the processes and practices they are assessing, in order to avoid a conflict of interest, and need to have the proper experience to fully understand the written requirements. It is for this reason that most people hire an independent third party.

Now that you have a Scope, look at it and see if it adheres to your target maturity level. Are all the necessary practices in place? If not, then this is your organization's compliance gap. These gap items should go into a Plan of Action and Milestones (POA&M) for your organization to start gathering information, such as costs, schedules, and impacts. This will allow you to make decisions or to collaborate on alternatives. Decisions may be to modify your Scope again, or to outsource a service. Your organization may also decide to increase overhead costs to recuperate costs for the items in the POA&M.

The Gap Assessment can vary depending on what you want reviewed. I believe a Gap Assessment can be done at various levels to fit the needs of the OSC. Your organization may not want a very complex and expensive review to start with, because you are not sure how ready your organization may be for CMMC.

1. Quick review to assess maturity and understanding of an organization.
2. Review of documentation and objective evidence.
3. In depth review of documentation and objective evidence, provide feedback to OSC of identified gaps.
4. Provide a POA&M to the OSC with products, solutions, and services to remediate gaps
5. Mock CMMC Assessment.

For a quick assessment, a good consultant can quickly identify how ready your organization will be to move forward with other phases in a few hours' time. The output should be recommendations on how you can press forward, if the right personnel are in place, and if they should investigate outsourcing

functions to an MSP or MSSP. You may want to leverage in-house personnel experienced with auditing in general (financial, quality) to see how ready your organization may be for CMMC. There may be some challenges using internal personnel, as they may need to learn about what they are being asked to assess, but it is not something that should stop you from trying.

Quick Assessment: 8 Hours * $200 = $1,600.00

The second phase for a Gap Assessment is to review documentation. Ask for everything, see what you receive. Do a quick cross reference to see if you received supporting documentation for CMMC objectives (whether the documentation is sufficient or not is not really part of this phase). If you are able to receive all of that, then you can infer your organization has a level of maturity, as well as a basic understanding of CMMC and how to comply with objectives. This can be done fairly quickly as well.

Documentation review: 20 Hours * $200 = $4,000.00

Accruing a highly in-depth look at your policies, procedures, and practices is a must for preparing for CMMC. This is the first thing the CMMC assessment team will review for your organization. The person doing this review should be very familiar with auditing and reviewing objective evidence to meet an objective. A technical writer, auditor, risk manager, attorney, or other roles may work if you plan on using internal personnel. It should not be someone on the team preparing all of this information. One key item to look at, other than meeting an objective, is whether your organization documentation is saying what it does, and your organization does what it says.

Objectives * Time to review each objective * Labor cost
320 * .2 * $200 = $12,800.00

Implementation estimates will all depend on your Scope and what Gaps you may have. The gaps may simply require a documentation update, or they may require you to replace all of your outdated hardware and software used for processing, storing, or transmitting CUI. Using some strategies, you may be able to limit your Scope, or protect the information in a different way. These estimates can be a percentage of your IT budget, a percentage of your annual revenue, or estimated out per employee. We will use the employee cost estimate, since it is the number, we are using to identify micro, small, and medium businesses in this paper. This would be an annual cost (not one time) so costs are spread across years, not all at once.

2% of Annual revenue
10% of IT Budget
$1,200 per employee

Micro: 25 * $1,200.00 = $30,000.00
Small: 50 * $1,200.00 = $60,000.00
Medium: 250 * $1,200.00 = $300,000.00

For a CMMC Mock assessment, the costs would be the same as a full assessment.

Crosswalk

This is a sub-task to a Gap Assessment, and may not be applicable to your organization. An initiative like this leverages your existing policies and compliance frameworks to see if those items directly "cross" over to a CMMC objective. Your company may already be compliant with PCI/DSS, NIST Special Publication 800-171, NIST Special Publication 800-53, ISO 27001, or FedRAMP. The controls, business processes, and artifacts you have in place to support compliance with those other frameworks can help you with compliance with CMMC. At CMMC Level 2 there are 110 necessary practices, of which are all mapped back to NIST 800-171. This means that to achieve CMMC compliance, you can leverage how you have already implemented the NIST 800-171 controls. What you have created and implemented for those regulatory compliance objectives may map over to CMMC with or without the need to do additional leg work. This should be incorporated into your Gap Assessment, as it may result in an overall reduction in hours and costs associated with becoming CMMC compliant.

If your organization is already ISO 27001 compliant, then you do not need to create a completely new compliance program. Your ISO 27001 program is likely to cover some of the practices and objectives in CMMC. The practices may need to be enhanced or updated to include specifics in the CMMC objectives. These modification needs would be identified in the Crosswalk and placed into your POA&M for the Gap Assessment.

The Crosswalk can be conducted alongside your gap assessment phases. If your organization already has an ISO 27001 certification or something similar, this can be leveraged to show that your organization may already meet some objectives. This would include mapping an ISO 27001 compliance objective to a CMMC objective, then identifying if it is wholly or partially able to meet the CMMC objective. This can be completed in 2 parts: mapping the objectives to each other, then checking to see if they are sufficient for meeting CMMC objectives. The mapping exercise alone may be an 8-hour task for an individual. Using open and free tools can be helpful but should not be a definitive or authoritative source as to whether they directly map to each other or not.

Mapping: 8 Hours * current compliance frameworks * $200 =
In-depth crosswalk: 320 objectives * current compliance frameworks * .10 * 200 =

Micro: (8 * 1 *200) + (320 *1 *.10 *200) = $8,000.00
Small: (8 * 2 *200) + (320 *2 *.10 *200) = $16,000.00
Medium: (8 * 3 *200) + (320 *3 *.10 *200) = $24,000.00

CMMC Assessment

The Cybersecurity Maturity Model Assessment process, which is conducted by a Provisional Assessor (PA) or a CMMC Certified Assessor (CCA), relies heavily on the Organization Seeking Certification (OSC) determining the Scope of the assessment. This means that if you define the Scope as a single computer, that is all the CMMC Third-Party Assessor Organization (C3PAO) will pass over to the CCA or PA for them to Scope the cost of the work. The CCA/PA will work with the OSC to gather the appropriate documentation to conduct the assessment, then to receive a verification from the OSC that the Scope is accurate. If you didn't identify the Scope correctly (e.g. you are processing FCI or CUI in your email system but didn't identify it), the CCA/PA will not look at your email system. Does this mean you should tell the C3PAO and CCA/PA that you only store, transmit or process FCI/CUI in a small Scope when you know it is being used in other systems? That is your business risk decision, but I highly recommend against it.

Once the assessment kicks off and the Scope, cost, timeframe, etc. are all agreed upon between the OSC and the lead assessor, you are locked into that agreement. If the OSC changes the Scope on the fly, it is a change in Scope for the assessor and the assessment process will need to start over again. If during the assessment there are CMMC objectives you do not comply with, then you have 90 days to correct them and to schedule an assessment to look over those corrected deficiencies. This may be at an additional cost to your organization.

Remember that you will need a full assessment every 3 years. If the Scope of where you need to transmit, store, or process CUI changes when a new contract is awarded, or when you need to use other tools/services to work with FCI/CUI, you will need to get another assessment to include those changes. This should not be a full assessment; it should just be for what changed since the last assessment (keyword "should"). These costs will need to be anticipated and figured into your budget somewhere. Your business will need to figure out how it plans to recuperate these costs.

Let us make some assumptions about how we estimate costs. We will not take into consideration the fact that this is new, and so some businesses may want a priority set for a CMMC assessment, or they may want it expedited for one reason or another. We are not taking into consideration that the C3PAOs may not have all of their tools, processes, or staffing in place to increase efficiency. The market is also limited, so there is not a lot of competition to lower costs.

- We will assume that the target is a CMMC Level 2 Assessment
  - 59 Objectives for CMMC Maturity Level 1
  - 320 Objectives for CMMC Maturity Level 2 (plus ML1)
- We will assume 2 pieces of objective evidence are gathered for each objective
  - Either reviewed, interviewed, or tested
- It will take 15 minutes per objective for each piece of evidence to be gathered
- The Labor cost for the PA/CCA/CCP will be on a scale of $175/hr to $225/hr
  - We will use $200/hr
- The level of complexity of your systems and organization will influence costs
  - 2.0 Very Complex (virtualized, multiple cloud hosted services, enclaves, multiple locations across the world)
  - 0.1 Very Simple (single computer, no external services)

(CMMC Objectives * 2) * .25 [15 minutes] * $200 [Hourly Rate] * Complexity =

Micro: (320 * 2) * .25 * 200 * .50 = $16,000.00
Small: (320 * 2) *.25 * 200 * 1.2 = $38,400.00
Medium: (320 * 2) *.25 * 200 * 2.0 = $64,000.00

CMMC Scope Changes

Using the same formula, you can also generate an estimate for a Scope Change. The Scope Change could be moving from a CMMC Level 1 to level 2. This would increase your objectives from 59 to 320 (delta of 261 objectives) [(261*2)*.25 *200 * 1.2 = $31,320.00]. The Scope Change could be to include another piece of equipment into your Scope, or a business system. Since those types of Scope Changes are very targeted the complexity would be much lower (not all assets need to be reviewed, just ones that changed the Scope) [261 * 2) *.25 *200 *.2= $5,220.00].

Delta Scope Change

- Micro: (261 * 2) * .25 * 200 * .50 = $10,800.00
- Small: (261 * 2) *.25 * 200 * 1.2 = $15,660.00
- Medium: (261* 2) *.25 * 200 * 2.0 = $52,200.00

Add new product to scope

- Micro: (320 * 2) * .25 * 200 * .2 = $6,400.00
- Small: (320 * 2) *.25 * 200 * .4 = $12,800.00
- Medium: (320 * 2) *.25 * 200 * .6 = $19,200.00

Remediation

After a Gap Assessment and/or a Crosswalk, you will need to implement the objectives identified in your Plan of Action and Milestones (POA&M). If your business is already patching, but does not have a documented policy, process, procedure, or practice for patching, your organization will need to complete the documentation. Your company may not have a vulnerability management program, and will therefore need to purchase and integrate a tool. For controls and practices not yet in place, a business can evaluate the best way to meet that requirement. In some cases, a business can choose to work with a third party to implement a given control. For instance, a business might hire a security guard to manage physical security and sign-ins into their facilities; you may hire a third party to handle physical security on weekends, while your in-house staff handles it on weekdays. Your organization may decide to implement these items themselves, outsource the work to a Managed Security Services Provider (MSSP), outsource to a Managed Services Provider (MSP), implement a shared responsibilities model, or have a third-party help with deploying necessary technologies and teaching your staff how to use them. Process maturity and documentation are what most organizations will struggle with in striving for CMMC compliance.

The next step is to take all the POA&M items and understand the costs and timeframes necessary to implement them. The total cost here is what our discussion will revolve around. For example, now that you have found out becoming compliant with this regulation will cost your organization $30,000, how do you proceed in such a way that ensures you can bill this back to the client?

The cost for Remediation will be very different across organizations. If your organization does not have a cybersecurity program now, it will cost much more to implement than an organization that already has one (assuming the Scope is exactly the same). If your organization waits until the last minute to implement cybersecurity practices, it will cost more than it would if they were applied progressively over several months or years. Remember, the government assumes your organization has the DFARS 252.204-7012 clauses flowed down to your organization, and that the NIST SP800-171 controls have been applied to your organization. Therefore, they believe that there should not be an enormous workload to make your organization compliant with CMMC. Now is the time to be strategic, and to plan how you will achieve CMMC compliance over time.

This cost is extremely difficult to estimate because every organization is different, (technology, people, scope, maturity, complexity, contracts, etc…). If you are asking a third party to assist you with this, the costs can be all over the board, depending on their level of maturity. If you only ask for an endpoint detection and response service, they may price it out per user or per install. They may want to include everything in your organization rather than your applicable Scope. If you have not set a Scope, your organization cannot assume they can figure that out for you. In the end, you may opt for including everything because it takes too much time to define the Scope. Ultimately, these costs will add up, and your executives will think that security and compliance costs way too much (instead of $1,200 per employee it now costs $1,500 per employee).

If you use the costs identified by the Office of the Under Secretary of Defense for Acquisition & Sustainment that was listed in Figure 6: DFARS Case 2019-D041 Cost Estimate, the costs do not exactly add up. Why is that? Well, the assumptions for these costs were based on the belief that the contractors already had the FAR 52.204-21 and DFARS 252.204-7012 clause in current contracts, and those contractors have already stated they are in compliance with it.

If you had a contract and you have replied that you are compliant with NIST SP800-171—either through a CDRL delivery to your contracting officer, or by submitting your score into the Supplier Performance Risk Assessment (SPRS) tool—you may be on your own to pay for the application of those controls to your environment. For example, the estimate for meeting a majority of the NIST 800-171 controls could be $150,000 for your organization, and to implement the remainder of the CMMC Level 2 practices is $60,000 in the Figure 6: DFARS Case 2019-D041 Cost Estimate. You can charge the $60,000 back to the government in one way or another, but the $150,000 is now on your organization to fund. The only caveat to that is if your Scope has changed from when you first applied those controls to what your Scope may be today. Be prepared with backup to justify that change in Scope in your proposal, or for justification on rate changes when bidding on the contract (or for an annual change in rate).

Keep in mind that the costs in Figure 5: Estimates for CMMC Compliance in an Organization Seeking Certification (OSC) do not include estimates for items such as per diem and travel for third parties or estimate for your organization to prepare for an assessment if a recommended phase has not been completed.

Phase	Micro Business (<25)	Small business (>25 & <250)	Medium Business (>250 & <1500)
Scoping	$8,000.00	$40,000.00	$160,000.00
GAP Assessment	$33,800.00 + Assessment	$33,800.00 + Assessment	$33,800.00 + Assessment
Crosswalk	$8,000.00	$16,000.00	$24,000.00
Remediation/Implementation	$30,000.00	$60,000.00	$300,000.00
CMMC Assessment	$35,250.00	$84,600.00	$141,000.00
CMMC Scope Change	$6,400.00 - $10,800.00	$12,800.00 - $15,660.00	$19,200.00 - $52,200.00
CMMC 3 Year Assessment	$35,250.00	$84,600.00	$141,000.00
First Year ROM	**$35,250.00 - $115,050.00**	**$84,600.00 - $234,400.00**	**$141,000.00 - $658,800.00**

Figure 5: Estimates for CMMC Compliance in an Organization Seeking Certification (OSC)

CMMC cert	Average nonrecurring engineering costs	Recurring engineering costs	Average assessment costs	Total annual assessment cost
Level 1	$0	$0	$1,000	$1,000
Level 2	407	20,154	7,489	28,050
Level 3	1,311	41,666	17,032	60,009
Level 4	46,917	301,514	23,355	371,786
Level 5	61,511	384,666	36,697	482,874

Figure 6: DFARS Case 2019-D041 Cost Estimate

Methods of Passing Compliance Costs

The method you choose to use for passing costs over to a client must be consistent with the Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulations Supplement (DFARS) and Cost Accounting Standard (CAS). The information in this section provides examples on how CMMC can get rolled into one of the standard methods. Remembering that CMMC is not a cyber issue, it also involves procurement, contracts, finance and others.

Labor Rates

Your base labor rates should be in line with the Bureau of Labor Statistics for each specific occupation. You may have some adjustments that put an individual towards the higher end or the lower end of the rate curve (such as security clearance, education, or critical skill). In addition, during the Gap Assessment you may require specialized skill sets for specialized systems, like your ERP.

Indirect charging

The hourly rate you pay your employee is not the same rate you bill your clients for labor work, right? What is figured into that rate? This is a very simple example of how this works out.

Employee hourly rate: $100.00
Benefits: 35% ($35.00)
Overhead Expenses: 25% ($25.00)
Profit: 15% ($15.00)
Compliance Requirements: 25% ($25.00)
Billed to Customer: $200.00 an hour

Now, looking at the bigger picture, if you are bidding on a contract, and you believe it will take 300 hours to complete that work (direct billing to that contract) and it will cost your organization $15,000 to meet the objectives of CMMC, you can spread that cost through your labor rate for this contract.

Employee hourly rate: $100.00 * 300 = $30,000.00
Benefits: 35% ($35.00) * 300 = $10,500.00
Overhead Expenses: 25% ($25.00) * 300 = $7,500.00
Profit: 15% ($15.00) * 300 = $4,500.00
Compliance Requirements: 25% ($25.00) * 300 = $7,500.00
Total Cost: $60,000 in labor

- Note that the compliance cost in this figure is less than the cost estimated to meet the CMMC objectives

However, in this scenario you have not recuperated your costs for compliance and have had to pull $7,500 from your profit margin to cover the costs for compliance. You will need to adjust your indirect cost for this contract for compliance from 25% to 50% to cover this cost, or you have other contracts in the queue that you may be awarded. You may decide that you will want to pull funds out of profits for now to be more competitive in the bid and hope that future contracts are awarded to cover your expenses.

Employee hourly rate: $100.00 * 300 = $30,000.00
Benefits: 35% ($35.00) * 300 = $10,500.00

Overhead Expenses: 25% ($25.00) * 300 = $7,500.00
Profit: 15% ($15.00) * 300 = $4,500.00
Compliance Requirements: 50% ($50.00) * 300 = $15,000.00
Total Cost: $67,500 in labor

Direct Billing

Direct billing is when you bill the client "directly" for those costs. You will need to have some supporting documentation to support the cost. It may be a quote from a vendor, your Plan of Actions and Milestones (POA&M) that shows the objective, what needs to be completed and your estimated costs, a basis from actual costs of a similar project your company has done, maybe a basis of actual costs from a peer, or maybe it is just an engineering estimate.

Employee hourly rate: $100.00 * 300 = $30,000.00
Benefits: 35% ($35.00) * 300 = $10,500.00
Overhead Expenses: 25% ($25.00) * 300 = $7,500.00
Profit: 15% ($15.00) * 300 = $4,500.00
Total Cost: $52,500.00 in labor
Compliance Cost: $15,000.00

Direct Charging

You may wish to have your existing personnel charge hours for the compliance efforts directly to the contract. Your system administrator or compliance manager would then bill hours directly to the project that requires the compliance work. Your estimate was $1,000.00 in labor, but the labor rate is different than the machinist making the screws. You will need to include the rate as another labor category in your proposal.

Compliance Analyst (individual performing the compliance work)
Employee hourly rate: $100.00 * 85 = $8,500.00
Benefits: 35% ($35.00) * 85 = $2,975.00
Overhead Expenses: 25% ($25.00) * 85 = $2,125.00
Profit: 15% ($15.00) * 85 = $1,275.00
Subtotal Cost in Labor: $14,875.00

Machinist
Employee hourly rate: $100.00 * 300 = $30,000.00
Benefits: 35% ($35.00) * 300 = $10,500.00
Overhead Expenses: 25% ($25.00) * 300 = $7,500.00
Profit: 15% ($15.00) * 300 = $4,500.00
Subtotal Cost: $52,500.00 in labor

Labor Totals: $67,375.00

Summary

Estimating is a way to anticipate costs for a project. This is done with some, but not all, knowledge of the project. If you need to know the complete costs for a project, you will likely need to spend more money up front to get a true estimate of the work. The estimates in this document are shown just to provide the reader with information about an approach which may help them figure out what their costs could be, as well as to provide them with a strategy to recuperate those costs through a contract with the federal government.

If your company is unsure of whether they will continue to do business with the DoD, or prime contractors that levy the FAR and DFARS requirements on your organization, you should run through some of the exercises here to provide a medium to high level of confidence about the possible costs associated with continuing that line of business. Using this whitepaper as a guide to walk you through these steps is a great start, but the costs estimated here are based on calculations that are far from perfect. They are not a one-size-fits-all method.

Many of the costs identified in here will become recurring costs in some sort of cycle. You will have CMMC assessments every 3 years (at least), and your hardware/software has a lifecycle as well. Think about when you buy a car; you still must pay excise taxes (in most states), car insurance, your license renewal fees, maintenance for the car, or repairs to the car if something breaks unexpectedly. You may replace the vehicle altogether when repairs get too expensive (because parts are no longer getting produced), the vehicle is no longer reliable, or your needs for a vehicle change (you now need more seats or storage space).

If you receive estimates from third parties to assist in CMMC in one capacity or another, use their estimates to question yourself:

Did we properly Scope the requirement?

Does the third party really understand what we need?

Is the third party knowledgeable, and do they have trained/certified staff to support CMMC for the technology we need it applied to?

Will the third party support me through the CMMC assessment?

Will the third party cover any expenses for objectives not met?

Does the third party have professional liability insurance to cover my loss of business if they misguided my organization?

References

Articles on CMMC Costs

CMMC Audit - https://www.cmmcaudit.org/cmmc-allowable-cost-discussion/

How Much Will CMMC Certification Cost My Business? | Pivot Point Security

CMMC Related Sites

CMMC FAQ OUSD - https://www.acq.osd.mil/cmmc/faq.html

DFARS case with Federal Government Estimates on CMMC Costs

Federal Register: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)

DISA Supplier Performance Risk System

https://www.sprs.csd.disa.mil/

Labor costs

https://www.bls.gov/oes/

IPNS SIN 132-51 Rates - https://www.gsaadvantage.gov/ref_text/GS35F050GA/0UY0LL.3QODND_GS-35F-050GA_GS35F050GAIPNS1.PDF#:~:text=not%20present%20%20%20SIN%20%20%20GSA,%20%20195.66%20%2010%20more%20rows%20

GSA CALC Cyber - https://calc.gsa.gov/?q=cyber%7C

Other relevant links

Compliance Crosswalk Tool: https://cch.commoncontrolshub.com/

General Data Protection Regulation https://gdpr.eu/ https://www.youtube.com/watch?v=4OJbnkPGt9M

State Laws relevant to Data Breaches

Connecticut Public Act No. 21-119 https://www.cga.ct.gov/2021/act/Pa/pdf/2021PA-00119-R00HB-06607-PA.PDF

Massachusetts 201 CMR 17 https://www.mass.gov/regulations/201-CMR-17-standards-for-the-protection-of-personal-information-of-residents-of-the

California CCPA https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Summary of Data Security Laws
https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx

Federal Government References

Cost Accounting Standards https://www.acquisition.gov/far/52.230-2

Federal Acquisition Regulations https://www.acquisition.gov/browse/index/far

Defense Federal Acquisitions Regulations Supplement https://www.acquisition.gov/dfars

Defense Pricing and Contracting https://www.acq.osd.mil/dpap/dars/class_deviations.html