RADICL™

CMMC Big Ticket Items Preparation Guide

Becoming CMMC compliant is an investment in time, technology, people, and process. The extent of unexpected and unbudgeted investment can vary greatly based on your current NIST 800-171 adherence and sophistication of IT operations. This document identifies the most significant "big ticket" investment items, those that typically require the most significant outlay of resources. For each we provide key considerations as you evaluate options. We also share how RADICL can accelerate and simplify CMMC compliance with our cost effective and predictably priced Managed Compliance Adherence (MCA) offering along with our broader Cybersecurity-as-a-Service (CSaaS) suite.

Big Ticket Item	Overview	Key Considerations	With RADICL™ MCA
Self- Assessment Process	Readiness requires executing self-assessments to identify gaps in IT/security infrastructure, operational processes, and documentation.	Interpreting the intent of all 110 controls and 320 objectives is a complex and daunting initiative for organizations lacking internal CMMC expertise. The readiness self-assessment is best overseen by someone independent of your IT team or MSP. This independence helps ensure objectivity and accuracy of findings. If you engage a third party to help oversee the self-assessment ensure they are appropriately qualified. They should minimally be a Registered Practitioner Organization (RPO) and ideally have a Certified CMMC Assessor (CCA) on staff.	Our CCA-led compliance team expertly guides and supports your assessment process. Our COMPLY module provides guided workflow, evidence capture, documentation management, and posture visibility.
Remediation Process	Gaps identified in the self-assessment will need to be addressed to bring IT/security infrastructure, operations, and documentation in line with CMMC requirements.	The remediation process will require program and project management to align resources, priority, and schedule to ensure on-time C3PAO assessment readiness.	We program and project manage your readiness process. Our CCA-led team and COMPLY module organizes and drives the remediation process with expert and business aligned guidance. We ensure your internal team and/or MSP know precisely what needs to be done to close identified gaps.

		Remediations continue after CMMC has been achieved. Changes to IT infrastructure and operations may introduce new gaps. The assessment to remediation process should be ongoing to ensure continued compliancy.	When changes in the IT environment occur, we can initiate targeted re-assessments and remediations as needed.
Business System Infrastructure	All IT infrastructure that stores, processes, or transfers CUI must meet CMMC requirements. This minimally includes file storage, file sharing, and email.	Microsoft O365 shops will need to upgrade to GCC or GCC-High based on the type of CUI being handled. Google Workspace shops typically need to upgrade licensing to Google's Assured Workloads and implement very specific configurations. Some smaller organizations, or those that carve out a smaller enclave of in-scope users, choose to leverage a tool like Preveil to handle storing, processing, and transmitting CUI.	If additional technologies are required, we will provide recommendations that meet CMMC requirements and best align with budgetary and operational needs.
IT Support	Configuring and managing network, cloud, endpoint, email, and data management infrastructure to CMMC standards requires IT expertise and capacity. The level of resources required will vary based on the size and complexity of your IT environment and current NIST 800-171 posture.	If you have an internal IT team, you may need to augment them with an MSP or consultant. There are many who focus on and specialize in CMMC readiness. If you have an existing full-service MSP, they should be able to help execute the majority of needed work. However, this work may be out of scope and you'll need to plan for additional costs. You will want to verify your MSP has experience configuring and managing GCC/GCC-High or Google Workspace environments in conformance with NIST 800-171R2.	We can introduce trusted partners who can provide staff augmentation, who also have deep CMMC experience. We will reduce the overall level of internal/external IT effort and costs by providing detailed remediation guidance for bringing systems and infrastructure into compliancy. To ensure trustworthy readiness, we will drive a reassessment process to validate the quality and completeness of work. This avoids more costly rework and possible contract disruption due to a failed C3PAO assessment.
Documentation Development	Over 45 individual documents, policies and procedures need to be developed in preparation for a CMMC assessment.	For most organizations, this is estimated to take around 200 hours of effort. Third-party RPOs can assist with this development.	To facilitate internal documentation development, we provide templates and guidance for CMMC Level 1 and 2.

			If you prefer to outsource documentation development, our team of experts can do so on your behalf and tailor them to your specific organizational and operational needs. We provide in-platform documentation management ensuring easy management and fast 3P assessment.
24x7 Monitoring and Incident Response	CMMC requires 24x7 monitoring and incident response.	Most SMBs need to engage a Managed Security Service Provider (MSSP) or Managed Detection & Response (MDR) response to serve this requirement.	With RADICL Managed Detection & Response (MDR), these requirements are met while also minimizing the likelihood of experiencing a high impact cybersecurity incident (e.g., ransomware).
Anti-Virus	CMMC requires all endpoints have anti-virus installed and maintained/updated.	You'll need to purchase and deploy anti-virus, or ideally EDR technology, on all endpoints.	With RADICL MDR for Endpoints this requirement is met with best-in-class, expertly managed EDR technology.
Risk-Based Vulnerability Management	CMMC requires a risk-based vulnerability management program.	You'll need to purchase, maintain, and operate a vulnerability management product or ensure your MSP is doing so on your behalf. Ideally you have segregation of duties between who is responsible for assessing vulnerabilities and who is responsible for patching. Having the same entity (i.e., your MSP) do both creates independence and objectivity risk.	With RADICL Managed Attack Surface (MAS) this requirement is met with risk-based vulnerability prioritization and expert-driven remediations.
Security Awareness Training	CMMC requires role-based Security Awareness Training.	You'll need to purchase, maintain, and operate a security training awareness product, or have your MSP do so on your behalf. You'll need to ensure your training program meets CMMC specific requirements.	With RADICL Managed Security Awareness this requirement is met with CMMC-specific training and general training that includes phishing simulations.
Third-Party Assessment	In order to be CMMC Certified, an assessment must be performed by a Certified Third-Party Assessment Organization (C3PAO).	Due to the limited number of authorized C3PAOs, there is a backlog forming, so contracting with a C3PAO early in the readiness process is important.	We can introduce trusted C3PAOs who understand RADICL's offering, helping facilitate fast and successful assessments.