# MEETING CMMC WITH ANCHOR

## Analysis of Anchor's Impact on Cybersecurity Maturity Model Certification


### Abstract

DoD is launching a supply-chain risk-management approach to improve the security of its data, as it is processed by its contractors. As a result, all DoD contractors will need to obtain third-party certification documenting they meet requirements for the CMMC maturity level appropriate to be able to process DoD data and sign/extend contracts. Anchor empowers organizations to meet CMMC requirements by providing the automated controls to all data and application types, without changing the workflow within the organizations. In this document, we provide a detailed analysis of the capabilities of Anchor, toward meeting the CMMC compliance.



DAtAnchor Compliance Documents

support@datanchor.io

# 1 Introduction

Cybersecurity Maturity Model Certification (CMMC) dictates the rules around an organization's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) in order for the organization to be able to sign contracts with DoD. FCI is provided by or generated for the government under a contract to develop or deliver a product or service to the government. This information cannot be made public. CUI is information that requires protection and can only be shared subject to specific controls in accordance with federal law and regulations.

The DoD is progressing beyond the past approach of requiring a self-assessment for NIST 800-171 compliance as a part of its contract process. As a part of new supply-chain risk-management approach, all DoD contractors (more than 300,000 in the USA) will need to obtain third-party certification that they meet requirements for the CMMC maturity level appropriate to the work they intend to do for the DoD.

Many organizations do not fully understand NIST controls, which set the foundation for CMMC. Due to the sheer number of controls and terms required for compliance, there is a misconception that the path to compliance is complicated, arduous, and expensive. *This is not true*. This paper provides a high-level overview of the CMMC framework, its key components and addresses some of the important questions around what an organization needs for CMMC. The discussions will be in terms of fundamental cyber security principles and their connections to CMMC. Within these principles, we discuss how the use of the Anchor platform by DAtAnchor provides a *simple, low-maintenance, and affordable* means to keep your organization compliant with CMMC.

In this report, we also provide a checklist on the potential risks and required controls provided by CMMC, which was primarily derived from the NIST Cybersecurity Framework. The checklist helps organization's identify and inventory their information assets, assess the adverse impact to DoD customers and the organization, identify potential protections and processes that secure the assets, and complete a risk-based assessment considering their resources, the consequences of a potential breach and available protections and safeguards. To become compliant, organizations need to remediate vulnerabilities.

Depending on the practices/actions taken by the organizations, CMMC assigns a level for cybersecurity maturity. These levels are shown in the following table from the lowest to the highest.

| |
|---|
| **Level 1 – Basic Cyber Hygiene** |
| **Level 2 – Intermediate Cyber Hygiene** |
| **Level 3 – Good Cyber Hygiene** |
| **Level 4 – Proactive** |
| **Level 5 – Advanced/Progressive** |

The critical objective for DoD contractors will be meeting Level 3, since an organization assessed at Level 3 will have demonstrated Good Cyber Hygiene and effective implementation of controls that meet the security requirements of NIST SP 800-171 [1]. As a result, organizations prove a basic ability to protect and sustain assets and CUI. Once a control is introduced in a level, it becomes required for all levels directly above as well. Hence, for an organization to achieve Level 3, all the practices and processes defined in Levels 1 thru 3 must be achieved. DoD Prime contractors must also follow the appropriate level requirement to their contractors, which will vary depending on the nature of the contractors' work. For instance, a prime contractor with CMMC Level 3 certification could have a subcontractor, with which it shares just FCI; it suffices then that contractor achieves Level 1 certification.

The following table lists the broad technical domains for the CMMC model most of which are originated from FIPS SP 200 [2] security-related areas and the NIST 800-171 control families. On the same table, we also provide a simple description of how Anchor builds the necessary controls in each area toward achieving CMMC/NIST requirements. For simplicity, we classify the domains under four broad categories: **Identification and Assessment of Risks; Protection; Management; and Response & Training**.

| | CMMC/NIST Domain | Anchor Impact | How Anchor helps |
|---|---|---|---|
| **Identification and Assessment of Risks** | 1. Audit and Accountability | *Very High* | Anchor has a high-granular data access monitoring system for all access, even by the third parties and sub-contractors. It can be connected to SIEM tools and creates appropriate warning messaging and throttling mechanisms. |
| | 2. Identification and Authentication | *High* | Anchor adds attribute-based controls to access every piece of data. As a result, authentication is not only enforced by user credentials, but also by physical and logical contexts. This level of robustness eliminates a wide variety of security issues due to captured/weak passwords and authentication attacks. |
| | 3. Security Assessment | *Medium* | Anchor's monitor provides a fully transparent view of the access to data from all applications, devices, locations, and users. By controlling the plaintext access from any unauthorized application, it eliminates attacks from that surface. Thereby, the need for assessment is simplified substantially. |
| | 4. Situational Awareness | *N/A* | While Anchor enhances internal awareness, this term requires external channels including security forums to be utilized in situational awareness. |
| **Protection** | 5. Access Control | *Very High* | Anchor automates and simplifies access controls via its attribute-based approach, shrinking the attack surface due to phishing and other classical attacks to access credentials. It respects other ACLs and enforces the rules via persistent encryption. As a result, Anchor eliminates loss of sensitive data in plaintext from stolen, lost, retired assets or access credentials. The same level of security applies independently of the systems of the third party: Sharing does not mean giving up control. |
| | 6. Media Protection | *Very High* | Combining persistent and transparent encryption, Anchor not only provides perpetual security, but it also enhances efficiencies by eliminating any workflow impediments, typically caused by other security solutions. Further, with classification integrated, Anchor can identify media with necessary CUI markings in the location it is stored and prohibits the access outside of the owner(s). |

| | | | |
|---|---|---|---|
| | 7. Personnel Security | *Very High* | Anchor automatically enforces authorized access via its patent-pending key manager that combines automated governance with encryption. Anchor eliminates terminated employees from taking data in plaintext. Via its instant revocation capability, data exposure remains in ciphertext, even though the terminated employee had access to plaintext with the same device previously. |
| | 8. Physical Protection | *Very High* | Anchor maintains audit logs of all access to data. With the ability to enable edits without third parties being able to capture content, Anchor eliminates the need for the sharer to secure the systems for the third party, isolate, or remediate. All third-party consumption is also monitored. The same level of security applies independently of the systems of the third party: Sharing does not mean giving up control. |
| | 9. System and Communication Protection | *Very High* | Anchor provides the capability of creating internal and external boundaries for access to any data. These boundaries can be physical (based on geography, connectivity, or proximity to devices) or virtual (based on user credentials/groups within Active Directory). Confidentiality and access boundaries for CUI are enforced via FIPS-validated cryptography, as the data is stored at rest, in transit, and even during consumption by an application. Key management and protection are handled via a multi-stage encryption process with the Master Keys are always controlled by the organization over a secure HSM. |
| | 10. System and Information Integrity | *High* | With classification integrated, Anchor can identify sensitive data and the location it is stored. It eliminates the risk of data loss by persistent encryption. Further, via a diligent certification process, Anchor eliminates specific set of malwares and malicious code/applications from leaking data in plaintext. |
| **Management** | 11. Risk Management | *Medium* | Via its integration with data scanning and classification, Anchor can enable risk reports for even encrypted data. Also, Anchor's one-click application certification process simplifies the management of non-vendor-supported products and exposed such products to ciphertext only, depending on the need. |
| | 12. Asset Management | *Low* | While Anchor enables enforcement of the governance rules for CUI, definition of procedures around the handling of CUI is an input to Anchor. |
| | 13. Maintenance | *High* | DAtAnchor maintains all Anchor products and provides regular updates, patches, and enhancement via a simple and secure process. Anchor can provide off-site |

| | | | |
|---|---|---|---|
| | | | maintenance via its compliant AWS/Google Cloud processes, as per the mandates of FedRAMP/NIST. |
| | 14. Configuration Management | *Very High* | Anchor's dashboard enables IT to make new governance rules and initiate them through highly straightforward controls provided. The configurations include protection boundaries, access rules and attributes, and whitelisted applications and processes (outside of which, processes are not allowed to interact plaintext). Monitoring logs are generated and stored in a secured location for the organizational system. |
| **Response and Training** | 15. Awareness and Training | *N/A* | While DAtAnchor does not provide or establish training processes and procedures for organizations, it partners with other organizations to provide that. Reach out to DAtAnchor for training support. Also, the visual tools for system monitoring and SIEM access constitute valuable resources for overall personnel training. |
| | 16. Recovery | *Medium* | Anchor is not a backup solution. However, its monitoring and throttling capabilities help mitigate the attacks on backup data stores, via direct integration. Confidentiality of backup CUI is guaranteed as Anchor security travels with data. |
| | 17. Incident Response | *Medium* | Anchor has a highly-granular data access monitoring system. It can be connected to SIEM tools and creates appropriate warning messaging and throttling mechanisms. While detection, visualization, and reporting are for data centric attacks, network intrusion detection is beyond the scope of Anchor. |

*Table 1: CMMC domains and the impact of the Anchor platform are summarized. The impact is ranked based on a 5-tier scale: Very High, High, Medium, Low, Very Low, as well as N/A for components that are beyond the scope. We also provide a short description of Anchor's contribution toward mitigating the associated risks.*

Next, we dissect each section in the table and provide more details on the requirements and Anchor's contributions.

# 2 Why Anchor™

## 2.1 Background

DAtAnchor, Inc. is based in Columbus, Ohio. The Founder and CEO, Emre Koksal, has a PhD from MIT and is a Professor of Electrical and Computer Engineering at The Ohio State University. In conjunction with his time at MIT Lincoln Labs, Dr. Koksal helped build Sycamore Networks Intelligent Optical Transport Node. He also has several patents/technologies being commercialized by other companies. He is the recipient of Columbus Business First – Inventor of the Year Award in 2020, the National Science Foundation CAREER Award in 2011, HP Labs Innovation Research Award in 2011, and Ohio State University CoE Innovator of the Year Awardee in 2016 and 2020.

DAtAnchor's Board has taken several cybersecurity and technology companies public, such as Barracuda Networks and Infinera, and sold companies to SAP, Dell, Cisco, and Oracle among others. The technology of DAtAnchor is licensed via OSU and has multiple patents pending.

DAtAnchor has received substantial interest from institutional and commercial organizations for Dr. Koksal's Anchor platform. Anchor is currently deployed in a variety of organizations, including large technology and power enterprises, small and mid-sized healthcare and legal organizations, military contractors, and a research university. DAtAnchor established partnerships with major cloud vendors, including Box and Egnyte and is also building out a national MSP network of service providers.

**Business Benefits**

CMMC/NIST compliance made easy
Control and secure sensitive data
Collaborate without risk
Audit compliance in real-time
Automated data governance
Easy to implement and manage
Zero user impact

**Key Features**

Dynamic access revocation
FIPS compliant data encryption
Works with all applications and data
Security travels with data
Direct integration with cloud storage
Encryption enforced automatically
Granular, real-time data monitoring

**Sample Industries**

Manufacturing
Academic Institutions
Government
Healthcare
Legal
Financial Services

**Supported Systems**

Cloud or on-premise
Microsoft Windows optimized
Android and iOS Mobile Apps

## 2.2 Value

Anchor ensures data does not leave your organization without your knowledge and approval. The software makes this possible through its novel encryption methodology where a heartbeat is embedded into all sensitive data, including files, database and IoT payloads. This heartbeat verifies no matter where data travels, where it rests or how it gets there, if data access is not within the boundaries, the consumer will be presented with unreadable ciphertext. These boundaries or access rules are established by the organization and based on an access policy (e.g., Active Directory, HR Department) and/or physical requirements (e.g., IP Range, Wi-Fi, YubiKey, Geo-fencing, Bluetooth, etc.). An initial operation occurs where the selected files are encrypted with the heartbeat embedded in the data, the organization then defines who can access the data when within the set of defined boundaries. Subsequently, if the selected data is accessed outside the boundaries, the data is displayed as ciphertext with fully automated key management.

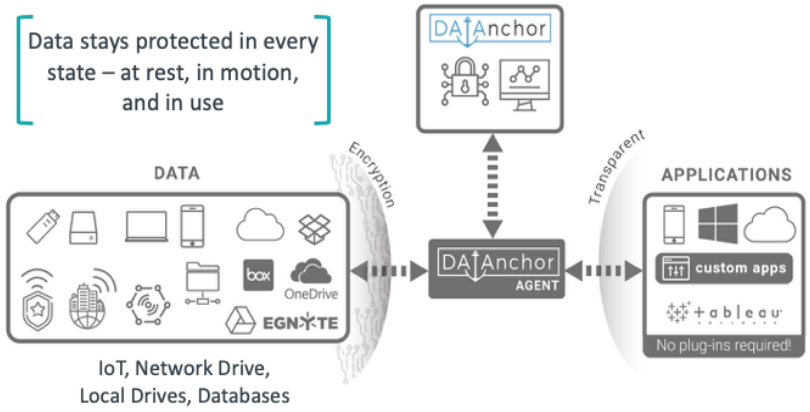


*Figure 1: Anchor is a SaaS-supported end-point solution that provides full control of CUI, no matter where it is consumed. The universal nature of it enables organizations to protect all applications, data types in any store, making it a unique solution to support DoD contractors, including manufacturers to become CMMC compliant, without changing any of their workflow.*

## 2.3 Architecture and Integrations

As illustrated in Figure 1, Anchor is a SaaS-supported end-point solution. It slides seamlessly between applications and data stores to provide FIPS-compliant encryption in place. Anchor's end point agent is an extension of the kernel; as a result, encryption and decryption are built as native operations as natural as simple read and write operations. With Anchor, data need not be stored in a

separate container for protection, nor does it require a separate drive attached. Encryption extends from at rest all the way to in transit and even during consumption by applications.

Anchor's **transparent** encryption ensures that the plaintext is made available, directly to all applications approved by the organization, without requiring and separate plugins: *users are unaware that the data they access is encrypted*. On the other hand, encryption is **persistent** and used to automatically enforce the governance rules at all times: the plaintext exposed to the applications are temporary and they can be revoked manually by the organization or automatically whenever the rules are broken.

Each file is encrypted with a separate key. The rules enforcement engine works in conjunction with the key manager and the access monitor, where file level audit logging takes place. The trio is containerized and readily deployable as a SaaS on cloud or locally on premise. Anchor also provides **third-party collaboration** over the cloud, via its secure applications. Anchor enables organizations to retain full control of their data as subcontractors and third-party collaborators can contribute to a project on all kinds of popular applications, including MS Office, pdfs, images, videos, etc. This zero-asset approach to third party sharing simplifies collaboration on projects significantly, as the prime contractor need not worry about the sub contractors' compliance deficiencies.

### 2.3.1 Applications and Data Stores

Functionality of Anchor can be viewed as a combination of Digital Rights Management (DRM) and the Digital Loss Prevention (DLP). The classical approaches to DRM and DLP are cumbersome, impede workflows, and eliminate sharing by blocking such actions rather than providing the ability to retain control. These solutions are integrated into applications and control user actions directly as they interact with the applications.


*Figure 2: A few examples of popular applications, stores and data management tools, that integrate with the Anchor platform for protection and compliance.*

Unlike its competitors, the Anchor platform is not attached to individual applications or data stores. Anchor is universal and can 'hook up' to all applications to protect files as they are consumed. Popular applications include Office (Word, Excel, PowerPoint, PowerBI, etc.), PDF (Adobe, Phantom), CAD (AutoCAD, Solidworks, Revit, etc.), image viewers, video players, and other possible custom applications.

Further, Anchor's drivers and filters are extensions of the kernel. They are detached from the stores, and as a result, encryption and decryption can be provided to data, kept in any store or drive, including cloud stores, network shares, and local drives along with data management tools. Some popular examples are illustrated in Figure 2. Anchor does not require a separate container or a file system.

### 2.3.2 Industries

The breadth of applications makes the Anchor platform ideal for a broad set of industries. We help protect and control sensitive data for the world's most information-critical industries including:

**Defense Industrial Base:** Protecting classified and CUI is critical to our national security and defense. Department of Defense contractors use Anchor to comply with CMMC.
**Manufacturing:** The companies who build the world we know have experienced rapid digital transformation and deal with increasingly complex supply chains. Anchor protects the intellectual property they depend on from CAD, CAM, BIM, product, process, engineering software and more.
**Healthcare:** Healthcare is about people, and people have a right to privacy. Anchor secures protected health information (PHI) helping healthcare professionals comply with HIPAA and uphold their responsibility to patients without impeding their workflow.
**Financial Services:** "Protecting investors means protecting their data, too." - finra.org Anchor has a high impact helping businesses establish a program to comply with the FINRA cybersecurity checklist.
**Legal Services:** Law firms live and breathe their ability to preserve clients' trust. They are also a prime target for cyber-attacks. Anchor empowers firms to hold private client information with confidence in a world where a single breach can destroy a reputation earned over decades.
**Consulting Services:** Anchor provides a secure collaboration for an organization, their clients, and their partners so each organization maintains absolute control over how, when, and under what circumstances their data is used.

## 2.4 Classify and Anchor

For all stores, Anchor integrates with classifiers and acts on the detected sensitivity level. Unified Anchor platform scans and classifies the data automatically at end points, network shares, and cloud stores and identifies sensitive data, including PII, PHI, or others based on the rules specified by the organization. Sensitive data is transparently encrypted and anchored to the organization, with proper rules, without any manual actions necessary. Integrations with classification engines, including Varonis and Egnyte Protect as well as Anchor's native classification engine have been demonstrated.

## 2.5 Third-Party Sharing

DAtAnchor empowers organizations to share data with third parties, without ever losing control of sensitive data. All actions of third parties are logged and the originating organization can revoke access at any given point in time. DAtAnchor also enables real-time collaboration sessions, where the parties can co-edit documents, with the keys disposed upon termination.

## 2.6 Industrial Internet of Things (IIoT)

DAtAnchor SDK supports deployment into edge IoT devices. To simplify and shorten prototyping and development cycles, we offer a flexible architecture to speed value creation.

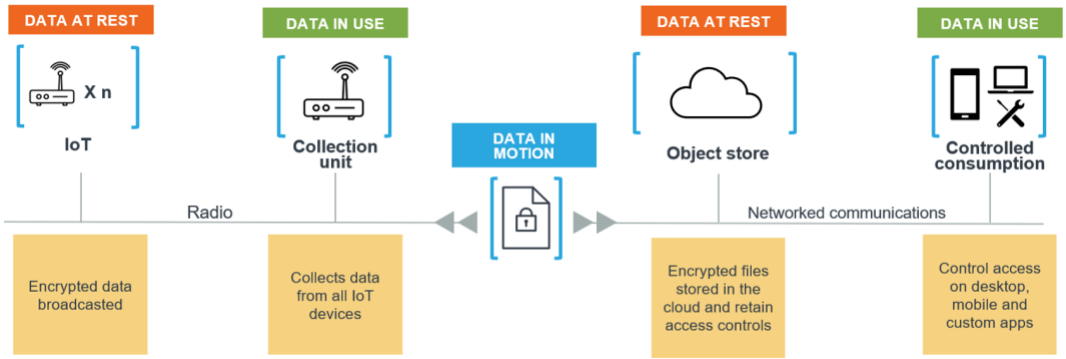


*Figure 3: DAtAnchor's SDK can control platform is enabling a new generation of connected hardware that significantly improves operational effectiveness of operators and assets.*

# 3 Detailed Checklist for CMMC L3 Controls with Anchor

Anchor is a simple and affordable platform that enables CMMC over a wide variety of industries and use cases. The platform is easy to deploy and substantially reduces the overhead associated with compliance. The main components Anchor uses to help organizations comply with CMMC requirements include transparent and persistent encryption, simple management and monitoring dashboard, instant revocation capability, and automated governance.

The table attached to the end of this document provides a detailed analysis of Anchor's capabilities to meet the CMMC. Note: each domain has multiple practices, each with a different requirement. Anchor provides full compliance for 77, while strongly supports 30 others out of a total of 130 practices. The remaining 18 practices are out of the scope of Anchor, leading to an overall CMMC **impact rate of 82.3%** for Anchor. Further, Anchor achieves this with maximal usability and a minor footprint on existing workflows.

# 4 Bibliography


[1] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle and G. Guissanie, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST Special Publication 800-171, 2020.

[2] C. Gutierrez and J. William, "Minimum Security Requirements for Federal Information and Information Systems," FEDERAL INFORMATION PROCESSING STANDARDS, 2006.

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Access Control (AC) | AC.1.001 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | AC.1.001-AC.2.006 requires access to information system by authenticated users and the information to remain within the system, eliminating exfiltration.<br><br>Anchor automates and simplifies the required conditions. It enforces access rules via persistent strong encryption, and adds an attribute-based approach, to further eliminate loss due to information leaving the intended store and access point. As a result, attacks such as phishing and access credential losses are mitigated. Anchor respects other existing ACLs. As a result, Anchor eliminates loss of sensitive data in plaintext from stolen, lost, or retired assets or access credentials. The same level of security applies independently for the systems of the third party: Sharing does not mean giving up control of information. | **Compliant with Anchor™** |
| Access Control (AC) | AC.1.002 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.1.003 | Verify and control/limit connections to and use of external information systems. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.1.004 | Control information posted or processed on publicly accessible information systems. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.005 | Provide privacy and security notices consistent with applicable CUI rules. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.006 | Limit use of organizational portable storage devices on external information systems. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.007 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | AC.2.007-AC.2.010 requires logging and access management for users.<br><br>Anchor verifies access controls during setup and creates proper certificates, associating the device-user pair to the access control rules. Subsequently, it uses Auth0 as a proxy to perform authentication via the authentication system of the organization. | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.008 | Use non-privileged accounts or roles when accessing non-security functions. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.009 | Limit unsuccessful logon attempts. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.010 | Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.011 | Authorize wireless access prior to allowing such connections. | AC.2.011-AC.2.015 is about remote access and monitoring.<br><br>Anchor's association of the user with the attributes makes it an automated zero-trust solution. As a result, Anchor continues to protect data, no matter where it is consumed, including remote stations. Further, real-time monitoring and control for all access, including remote is available from Anchor's dashboard. | **Compliant with Anchor™** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Access Control (AC) | AC.2.013 | Monitor and control remote access sessions. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.015 | Route remote access via managed access control points. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.2.016 | Control the flow of CUI in accordance with approved authorizations. | AC.2.016-AC.3.019 mandates controlling access to CUI and revocation of access outside of specific terms.<br><br>Anchor's key management, enables access to the keys subject to predefined appropriate conditions, including user groups and roles. As a result, flow of CUI in plaintext cannot be diverted maliciously. Any access denial is even logged in real-time, capturing the attempt to execute non-permitted actions. Instant revocation eliminates the loss of data, even for users with prior access to CUI. | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.017 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.018 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.019 | Terminate (automatically) a user session after a defined condition. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.012 | Protect wireless access using authentication and encryption. | AC.3.012-AC.3.022 enforces mobile devices and remote/mobile access to follow similar access control and revocation requirements.<br><br>Anchor's iOS and Android Apps make it possible to extend the controlled encrypted access to CUI from mobile platforms. | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.020 | Control connection of mobile devices. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.014 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.021 | Authorize remote execution of privileged commands and remote access to security- relevant information. | | **Compliant with Anchor™** |
| Access Control (AC) | AC.3.022 | Encrypt CUI on mobile devices and mobile computing platforms. | | **Compliant with Anchor™** |
| Asset Management (AM) | AM.3.036 | Define procedures for the handling of CUI data. | AM.3.036 is the only term under the Asset Management domain. While Anchor enables enforcement of the context rules for CUI, definition of procedures around the handling of CUI is an input to Anchor. | **Anchor™ Supports Compliance** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Audit and Accountability (AU) | AU.2.041 | Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. | AU.2.041-AU.2.044 provides the requirements around logs, their coverage, and enablement of analytics, reporting, and investigations.<br><br>Anchor has a highly-granular data access monitoring system for all access, even by the third parties and sub-contractors. It can be connected to SIEM tools and creates appropriate warning messaging and throttling mechanisms. | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.2.042 | Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.2.043 | Provide system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. | | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.2.044 | Review audit logs. | | **Anchor™ Supports Compliance** |
| Audit and Accountability (AU) | AU.3.045 | Review and update audited events. | AU.3.045-AU.3.052 gives the requirements around how to store and process the audit data.<br><br>Anchor enables a single click to download logs as CSV files for access and storage in other media. The database can be integrated with almost all SIEM tools to facilitate assessment by the auditor and reviewers. Anchor provides access and processing for the logs via its dashboard, access to which is carefully controlled and managed. It can be only accessed by authorized users. | **Anchor™ Supports Compliance** |
| Audit and Accountability (AU) | AU.3.046 | Alert in the event of an audit process failure. | | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.3.048 | Collect audit information (e.g. logs) into one or more central repositories. | | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.3.049 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.3.050 | Limit management of audit logging functionality to a subset of privileged users. | | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.3.051 | Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. | | **Compliant with Anchor™** |
| Audit and Accountability (AU) | AU.3.052 | Provide audit reduction and report generation to support on-demand analysis and reporting. | | **Compliant with Anchor™** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Awareness and Training (AT) | AT.2.056 | Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. | AT.2.056-AT.3.058 mandate the minimum requirements for internal training and awareness.<br><br>While DAtAnchor does not provide or establish training processes and procedures for organizations, it partners with other organizations to provide such. Reach out to DAtAnchor for training support. Also, the visual tools for system monitoring and SIEM access constitute valuable resources for overall personnel training. | **Anchor™ Supports Compliance** |
| Awareness and Training (AT) | AT.2.057 | Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. | | **Anchor™ Supports Compliance** |
| Awareness and Training (AT) | AT.3.058 | Provide security awareness training on recognizing and reporting potential indicators of insider threat. | | **Anchor™ Supports Compliance** |
| Configuration Management (CM) | CM.2.061 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | CM.2.061-CM.3.069 cover the configuration, control, and setup of new applications by the IT or users within the organization. It requires full monitoring and control of all software and hardware to go through an approval process and remain under continual check. It also introduces the notion of blacklisted applications for the organization to revoke them.<br><br>Anchor assists with this process significantly. First, it can provide encrypted control for executables. As a result, application sources remain encrypted with keys controlled by the organization.<br><br>Second, Anchor eliminates any new application or software to have any access to CUI in plaintext, unless explicitly certified and whitelisted by the administration. Even if a process, malware, or application is set up maliciously, Anchor eliminates its exposure to plaintext. That is the default position.<br><br>Lastly, Anchor's dashboard enables IT to make new governance rules and initiate them through highly straightforward controls provided. The configurations include protection boundaries, access rules and attributes, and whitelisted applications and processes (outside of which, processes are not allowed to interact in plaintext). Monitoring logs are generated and stored in a secured location for the organizational system, tracking CUI access by any given application. | **Compliant with Anchor™** |
| Configuration Management (CM) | CM.2.062 | Employ the principle of least functionality by configuring organizational system to provide only essential capabilities. | | **Compliant with Anchor™** |
| Configuration Management (CM) | CM.2.063 | Control and monitor user-installed software. | | **Compliant with Anchor™** |
| Configuration Management (CM) | CM.2.064 | Establish and enforce security configuration settings for information technology products employed in organizational information systems. | | **Compliant with Anchor™** |
| Configuration Management (CM) | CM.2.065 | Track, review, approve/disapprove, and log changes to organizational systems. | | **Compliant with Anchor™** |
| Configuration Management (CM) | CM.2.066 | Analyze the security impact of changes prior to implementation. | | **Compliant with Anchor™** |
| Configuration Management (CM) | CM.3.067 | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the organizational system. | | **Compliant with Anchor™** |
| Configuration Management (CM) | CM.3.068 | Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services. | | **Compliant with Anchor™** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Configuration Management (CM) | CM.3.069 | Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. | | **Compliant with Anchor™** |
| Identification and Authentication (IDA) | IA.1.076 | Identify information system users, processes acting on behalf of users, or devices. | IA.1.076, IA.1.077 is about proper identification and authentication of users to access the systems with CUI.<br><br>Anchor verifies access controls during setup and creates proper certificates, associating the device-user pair to the access control rules. Subsequently, it uses Auth0 as a proxy to perform authentication via the authentication system of the organization. | **Compliant with Anchor™** |
| Identification and Authentication (IDA) | IA.1.077 | Identification and Authentication (IDA) | | **Compliant with Anchor™** |
| Identification and Authentication (IDA) | IA.2.078 | Enforce a minimum password complexity and change of characters when new passwords are created. | IA.2.078-IA.2.082 specify the exchange for authentication, involving user credentials and password management.<br><br>Anchor does not directly impact the protection of passwords or access, but it does ensure CUI remains secure even when user credentials are stolen with various other attributes added in order to access the keys. | **Anchor™ Supports Compliance** |
| Identification and Authentication (IDA) | IA.2.079 | Prohibit password reuse for a specified number of generations. | | **Anchor™ Supports Compliance** |
| Identification and Authentication (IDA) | IA.2.080 | Allow temporary password use for system logons with an immediate change to a permanent password. | | **Anchor™ Supports Compliance** |
| Identification and Authentication (IDA) | IA.2.081 | Store and transmit only cryptographically- protected passwords. | | **Anchor™ Supports Compliance** |
| Identification and Authentication (IDA) | IA.2.082 | Obscure feedback of authentication information. | | **Anchor™ Supports Compliance** |
| Identification and Authentication (IDA) | IA.3.083 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | IA.3.083-IA.3.086 is on authentication mechanisms and their basic settings.<br><br>Anchor adds attribute-based controls to access every piece of data. As a result, authentication is not only enforced by user credentials, but also by physical and logical contexts that act as dynamic multifactors. This level of robustness eliminates a wide variety of security issues due to captured/weak passwords and authentication attacks. | **Compliant with Anchor™** |
| Identification and Authentication (IDA) | IA.3.084 | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. | | **Compliant with Anchor™** |
| Identification and Authentication (IDA) | IA.3.085 | Prevent reuse of identifiers for a defined period. | | **N/A** |
| Identification and Authentication (IDA) | IA.3.086 | Disable identifiers after a defined period of inactivity. | | **N/A** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Incident Response (IR) | IR.2.092 | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | IR.2.092-IR.2.094 require organizations to clearly define incidents and build mechanisms to detect and contain them.<br><br>Anchor empowers the organizations with the tools to detect incidents involving CUI. Anchor has a highly granular data access monitoring system. This system can be connected to SIEM tools and creates appropriate warning messaging and throttling mechanisms.<br><br>Anchor also reduces the reporting overhead significantly but making all audit logs downloadable as spreadsheets for processing by SIEM tools or manually.<br><br>While detection, visualization, and reporting are for data centric attacks, network intrusion detection (e.g., DDoS) is beyond the scope of Anchor. | **Anchor™ Supports Compliance** |
| Incident Response (IR) | IR.2.093 | Detect and report events | | **Anchor™ Supports Compliance** |
| Incident Response (IR) | IR.2.094 | Analyze and triage events to support event resolution and incident declaration | | **Anchor™ Supports Compliance** |
| Incident Response (IR) | IR.2.096 | Develop and implement responses to declared incidents according to pre-define procedures | IR.2.096-IR.3.099 cover the procedures around processing of audit logs.<br><br>Anchor also reduces the reporting overhead significantly by making all audit logs downloadable as spreadsheets for SIEM or manual processing.<br><br>While detection, visualization, and reporting are for data centric attacks, network intrusion detection (e.g., DDoS) is beyond the scope of Anchor. | **Anchor™ Supports Compliance** |
| Incident Response (IR) | IR.2.097 | Perform root cause analysis on incidents to determine underlying causes. | | **Anchor™ Supports Compliance** |
| Incident Response (IR) | IR.3.098 | Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. | | **Compliant with Anchor™** |
| Incident Response (IR) | IR.3.099 | Test the organizational incident response capability. | | **Anchor™ Supports Compliance** |
| Maintenance (MA) | MA.2.111 | Perform maintenance on organizational systems. | MA.2.111-MA.2.114 are pertaining to the maintenance of organization systems, including retention of system security during maintenance.<br><br>DAtAnchor maintains all Anchor products and provides regular updates, patches, and enhancement via a simple and secure processes. Anchor can provide off-site maintenance via compliant AWS/Google Cloud processes, as per the mandates of FedRAMP/NIST. It also provides support to the IT personnel during maintenance activities. | **Compliant with Anchor™** |
| Maintenance (MA) | MA.2.112 | Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. | | **Anchor™ Supports Compliance** |
| Maintenance (MA) | MA.2.113 | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | | **Anchor™ Supports Compliance** |
| Maintenance (MA) | MA.2.114 | Supervise the maintenance activities of personnel without required access authorization. | | **Anchor™ Supports Compliance** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Maintenance (MA) | MA.3.115 | Ensure equipment removed for off-site maintenance is sanitized of any CUI. | By its attribute-based access control, Anchor can simply eliminate any access to the keys encrypting CUI off-site. This can be set up with one-click via the administrative dashboard, provided by Anchor. | **Compliant with Anchor™** |
| Maintenance (MA) | MA.3.116 | Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. | MA.3.116 is the processes associated with the content of test and diagnostic programs. | **N/A** |
| Media Protection (MP) | MP.1.118 | Sanitize or destroy information system media containing CUI before disposal or release for reuse. | MP.1.118-MP.3.125 require organizations to<br><br>Combining persistent and transparent encryption, Anchor not only provides perpetual security, but also enhances efficiencies by eliminating any workflow impediments, typically caused by other security solutions. Further, with classification integrated, Anchor can denote media with necessary CUI markings in the location it is stored and prohibits the access outside of the organizations' preference. Persistent encryption implies security, not only at rest and in transit, but also during consumption. | **Compliant with Anchor™** |
| Media Protection (MP) | MP.2.119 | Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. | | **Compliant with Anchor™** |
| Media Protection (MP) | MP.2.120 | Limit access to CUI on system media to authorized users. | | **Compliant with Anchor™** |
| Media Protection (MP) | MP.2.121 | Control the use of removable media on system components. | | **Compliant with Anchor™** |
| Media Protection (MP) | MP.3.122 | Mark media with necessary CUI markings and distribution limitations. | | **Compliant with Anchor™** |
| Media Protection (MP) | MP.3.123 | Prohibit the use of portable storage devices when such devices have no identifiable owner. | | **Compliant with Anchor™** |
| Media Protection (MP) | MP.3.124 | Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. | | **Compliant with Anchor™** |
| Media Protection (MP) | MP.3.125 | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. | | **Compliant with Anchor™** |

tubesock anchor™

**Note**: This CMMC Level 3 (based on v1.02) and NIST 800-171 controls mapping document contains sample controls only. Please note that some controls are dependent on enterprise policies aligned with the Anchor™ information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which controls are applicable to you, and for developing and maintaining your own System Security Plan. Anchor™ has no responsibility or liability if you choose to include any or all the ample controls set forth in this document in your System Security Plan.

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Personnel Security (PS) | PS.2.127 | Screen individuals prior to authorizing access to organizational systems containing CUI. | PS.2.127 and PS.2.128 mandate organizations to keep CUI safe with access by individuals inside or outside the organization.<br><br>Anchor automatically enforces authorized access via its patent-pending key manager that combines automated governance with encryption. Anchor eliminates terminated employees from taking data in plaintext. Via its instant revocation capability, data exposure remains in ciphertext, even though the terminated employee had access to plaintext with the same device prior. Furthermore, physical location and geography can also be chosen as context rules as well as monitored for personnel and partners in order to eliminate leakage to undesired locations. | **N/A** |
| Personnel Security (PS) | PS.2.128 | Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. | | **Compliant with Anchor™** |
| Physical Protection (PE) | PE.1.131 | Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. | PE.1.131-PE.3.136 require organizations to keep and maintain logs of all activity and physical access to the systems containing CUI. This extends to the third party/subcontractor systems and sites.<br><br>Anchor maintains audit logs of all access to selected data. With the ability to enable edits without third parties being able to capture content, Anchor eliminates the need for the sharer to secure the systems for the third party, isolate, or remediate. All third-party consumption is also monitored. The same level of security applies independently of the systems of the third party: Sharing does not mean giving up control of information. | **Compliant with Anchor™** |
| Physical Protection (PE) | PE.1.132 | Escort visitors and monitor visitor activity. | | **Compliant with Anchor™** |
| Physical Protection (PE) | PE.1.133 | Maintain audit logs of physical access. | | **Compliant with Anchor™** |
| Physical Protection (PE) | PE.1.134 | Control and manage physical access devices. | | **Compliant with Anchor™** |
| Physical Protection (PE) | PE.2.135 | Protect and monitor the physical facility and support infrastructure for organizational systems. | | **Compliant with Anchor™** |
| Physical Protection (PE) | PE.3.136 | Enforce safeguarding measures for CUI at alternate work sites. | | **Compliant with Anchor™** |
| Recovery (RE) | RE.2.137 | Regularly perform and test data back-ups. | RE.2.137-RE.3.139 instructs to create back-ups and secure backed up CUI.<br><br>Anchor is not a backup solution. However, Anchor's monitoring and throttling capabilities help mitigate the attacks on backup data stores, via direct integration. Confidentiality of backup CUI is guaranteed as Anchor security travels with data. | **N/A** |
| Recovery (RE) | RE.2.138 | Protect the confidentiality of backup CUI at storage locations. | | **Compliant with Anchor™** |
| Recovery (RE) | RE.3.139 | Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined. | | **N/A** |

tubesock anchor™

**Note**: This CMMC Level 3 (based on v1.02) and NIST 800-171 controls mapping document contains sample controls only. Please note that some controls are dependent on enterprise policies aligned with the Anchor™ information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which controls are applicable to you, and for developing and maintaining your own System Security Plan. Anchor™ has no responsibility or liability if you choose to include any or all the ample controls set forth in this document in your System Security Plan.

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Risk Management (RM) | RM.2.141 | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. | RM.2.141-RM.3.146 directs organizations to scan, classify, assess the data in their stores for CUI. Once risks are assessed, organizations should remediate vulnerabilities.<br><br>Via its integration with data scanning and classification, Anchor can enable risk reports for all data. It also makes it possible to process and classify even encrypted data.<br><br>Anchor has a highly-granular data access monitoring system for all access, even by the third parties and sub-contractors. It can be connected to SIEM tools and creates appropriate warning messaging and throttling mechanisms. | **Compliant with Anchor™** |
| Risk Management (RM) | RM.2.142 | Scan for vulnerabilities in the organizational system and applications periodically and when new vulnerabilities affecting the system and applications are identified. | | **Anchor™ Supports Compliance** |
| Risk Management (RM) | RM.2.143 | Remediate vulnerabilities in accordance with risk assessments. | | **Anchor™ Supports Compliance** |
| Risk Management (RM) | RM.3.144 | Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria. | | **Anchor™ Supports Compliance** |
| Risk Management (RM) | RM.3.146 | Develop and implement risk mitigation plans. | Anchor supports execution of plans via automated governance engine. | **Anchor™ Supports Compliance** |
| Risk Management (RM) | RM.3.147 | Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk. | Anchor's one-click application certification process simplifies the management of non-vendor-supported products and exposed such products to ciphertext only, depending on the need. | **Anchor™ Supports Compliance** |
| Security Assessment (CA) | CA.2.157 | Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. | CA.2.157, CA.2.158 is about setting up security controls and policies involving environments, system boundaries, etc.<br><br>Anchor is about protecting all CUI within the boundaries and rules specified by the organization. Anchor makes the execution of the plans simple and fully automated. | **Anchor™ Supports Compliance** |
| Security Assessment (CA) | CA.2.158 | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. | In conjunction with Anchor's monitor and rules enforcement, any security control is assessed in real time. | **Anchor™ Supports Compliance** |
| Security Assessment (CA) | CA.2.159 | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. | CA.2.159-CA.3.162 is requiring the organization to execute an assessment plan that includes monitoring, detection, and correction of any vulnerabilities.<br><br>Anchor's monitor provides a fully transparent view of the access to data from all applications, devices, locations, and users. This capability renders the assessment software development trivial. The assessment is in real time and continual. | **Anchor™ Supports Compliance** |

tubesock anchor™

**Note**: This CMMC Level 3 (based on v1.02) and NIST 800-171 controls mapping document contains sample controls only. Please note that some controls are dependent on enterprise policies aligned with the Anchor™ information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which controls are applicable to you, and for developing and maintaining your own System Security Plan. Anchor™ has no responsibility or liability if you choose to include any or all the ample controls set forth in this document in your System Security Plan.

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| Security Assessment (CA) | CA.3.161 | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | CA.2.159-CA.3.162 is requiring the organization to execute an assessment plan that includes monitoring, detection, and correction of any vulnerabilities.<br><br>Anchor's monitor provides a fully transparent view of the access to data from all applications, devices, locations, and users. This capability renders the assessment software development trivial. The assessment is in real time and continual. | **Compliant with Anchor™** |
| Security Assessment (CA) | CA.3.162 | Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk. | | **N/A** |
| Situational Awareness (SA) | SA.3.169 | Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders. | SA.3.169 is enforcing the organizations to remain up to date on the threats and potential attacks, using external forums and other resources available externally.<br><br>While Anchor enhances internal awareness, this term requires external channels including security forums to be utilized for situational awareness. | **N/A** |
| System and Communications Protection (SCP) | SC.1.175 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | The CMMC practices here are not listed in the order they are published under CMMC document. They are ordered in a fashion that makes it possible to break it into two parts as: network centric and data centric requirements.<br><br>The first batch of practices are concerning the network centric approach to protecting communication sessions. It involves management and protection of sessions, control, and monitor network communication, ensure authenticity and integrity of communicated data.<br><br>Anchor is not a network-centric solution and it does not manage communication sessions. However, its rule-based encrypted access ensures data remains encrypted outside the authorized environment and in transit for all communications. | **N/A** |
| System and Communications Protection (SCP) | SC.1.176 | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | | **N/A** |
| System and Communications Protection (SCP) | SC.2.178 | Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. | | **N/A** |
| System and Communications Protection (SCP) | SC.2.179 | Use encrypted sessions for the management of network devices | | **N/A** |
| System and Communications Protection (SCP) | SC.3.184 | Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e. split tunneling). | | **N/A** |
| System and Communications Protection (SCP) | SC.3.186 | Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. | | **N/A** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| System and Communications Protection (SCP) | SC.3.181 | Separate user functionality from system management functionality. | The first batch of practices are concerning the network centric approach to protecting communication sessions. It involves management and protection of sessions, control, and monitor network communication, ensure authenticity and integrity of communicated data.<br><br>Anchor is not a network-centric solution and it does not manage communication sessions. However, its rule-based encrypted access ensures data to remain encrypted outside the authorized environment and in transit for all communications<br><br>. | **N/A** |
| System and Communications Protection (SCP) | SC.3.189 | Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. | | **N/A** |
| System and Communications Protection (SCP) | SC.3.183 | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | | **N/A** |
| System and Communications Protection (SCP) | SC.3.192 | Implement Domain Name System (DNS) filtering services. | | **N/A** |
| System and Communications Protection (SCP) | SC.3.185 | Protect the authenticity of communications sessions. | | **N/A** |
| System and Communications Protection (SCP) | SC.3.182 | Prevent unauthorized and unintended information transfer via shared system resources. | The second batch of practices are concerning the data centric approach to protecting CUI. It involves establishing processes and controls for the security of data at rest, in transit and as it is accessed by the users and applications.<br><br>Anchor provides the capability of creating internal and external boundaries for access to any data. These boundaries can be physical (based on geography, connectivity, or proximity to devices) or virtual (based on user credentials/groups within Active Directory). Confidentiality and access boundaries for CUI are enforced via FIPS-validated cryptography, as the data is stored at rest, in transit, and even during consumption by an application. Key management and protection are handled via a multi-stage encryption process with the Master Keys always controlled by the organization over a secure HSM.<br><br>Control and monitoring of all CUI are ensured even when it is outside the scope of the organization. | **Compliant with Anchor™** |
| System and Communications Protection (SCP) | SC.3.187 | Establish and manage cryptographic keys for cryptography employed in organizational systems. | | **Compliant with Anchor™** |
| System and Communications Protection (SCP) | SC.3.191 | Protect the confidentiality of CUI at rest. | | **Compliant with Anchor™** |
| System and Communications Protection (SCP) | SC.3.193 | Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g. forums, LinkedIn, Facebook, Twitter). | | **Compliant with Anchor™** |
| System and Communications Protection (SCP) | SC.3.177 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | | **Compliant with Anchor™** |

tubesock anchor™

| CMMC Domain | CMMC Practice | CMMC Practice Description | Compliance Explanation with Anchor™ | CMMC Compliance with Anchor™ |
|---|---|---|---|---|
| System and Communications Protection (SCP) | SC.3.188 | Control and monitor the use of mobile code. | Confidentiality and access boundaries for CUI are enforced via FIPS-validated cryptography, as the data is stored at rest, in transit, and even during consumption by an application. Key management and protection are handled via a multi-stage encryption process with the Master Keys always controlled by the organization over a secure HSM.<br><br>Control and monitoring of all CUI is ensured even when it is outside the scope of the organization. | **Compliant with Anchor™** |
| System and Communications Protection (SCP) | SC.3.190 | Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. | | **Compliant with Anchor™** |
| System and Communications Protection (SCP) | SC.3.180 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | | **Compliant with Anchor™** |
| System and Information Integrity (SI) | SI.1.210 | Identify, report, and correct information and information system flaws in a timely manner. | SI.1.210 and SI.2.214 requires monitoring of the system and detection of flaws in real-time.<br><br>Anchor's monitor incorporates the access patterns and creates reports and warning messages. | **Compliant with Anchor™** |
| System and Information Integrity (SI) | SI.2.214 | Monitor information system security alerts and advisories and take action in response. | | **Anchor™ Supports Compliance** |
| System and Information Integrity (SI) | SI.1.211 | Provide protection from malicious code at appropriate locations within organizational information systems. | SI.1.211-SI.1.213 require system scans for files and malicious executables and processes.<br><br>With classification integrated, Anchor can identify sensitive data and the location it is stored. It eradicates the risk of data loss by persistent encryption. Further, via a diligent certification process, Anchor eliminates specific set of malwares and malicious code/applications from leaking data in plaintext. | **Compliant with Anchor™** |
| System and Information Integrity (SI) | SI.1.212 | Update malicious code protection mechanisms when new releases are available. | | **Compliant with Anchor™** |
| System and Information Integrity (SI) | SI.1.213 | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. | | **Compliant with Anchor™** |
| System and Information Integrity (SI) | SI.2.216 | Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | SI.2.216-SI.3.220 require detection of abnormal usage patterns as well as message content injected in the system, including spam and email forgery.<br><br>Anchor does not provide detection for actions through email or user access to the system, unless they access data. | **N/A** |
| System and Information Integrity (SI) | SI.2.217 | Identify unauthorized use of organizational systems. | | **Anchor™ Supports Compliance** |
| System and Information Integrity (SI) | SI.3.218 | Employ spam protection mechanisms at information system access entry and exit points. | | **N/A** |
| System and Information Integrity (SI) | SI.3.219 | Implement email forgery protections. | | **N/A** |
| System and Informational Integrity (SI) | SI.3.220 | Utilize sandboxing to detect or block potentially malicious email. | | **N/A** |

tubesock anchor™

**Note**: This CMMC Level 3 (based on v1.02) and NIST 800-171 controls mapping document contains sample controls only. Please note that some controls are dependent on enterprise policies aligned with the Anchor™ information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which controls are applicable to you, and for developing and maintaining your own System Security Plan. Anchor™ has no responsibility or liability if you choose to include any or all the ample controls set forth in this document in your System Security Plan.