

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.	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.		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.1.004	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. 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. 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™	

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™
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. 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. Anchor's iOS and Android Apps make it possible to extend the controlled encrypted access to CUI from mobile platforms.
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

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™
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.	<p>AU.2.041-AU.2.044 provides the requirements around logs, their coverage, and enablement of analytics, reporting, and investigations.</p> <p>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.</p>	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.	<p>AU.3.045-AU.3.052 gives the requirements around how to store and process the audit data.</p> <p>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.</p>	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™

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™
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.	<p>AT.2.056-AT.3.058 mandate the minimum requirements for internal training and awareness.</p> <p>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.</p>	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.	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	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™

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™
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.	Compliant with Anchor™
Identification and Authentication (IDA)	IA.1.077	Identification and Authentication (IDA)	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.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. 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. 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

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™
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.	Anchor™ Supports Compliance
Incident Response (IR)	IR.2.093	Detect and report events	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.	Anchor™ Supports Compliance
Incident Response (IR)	IR.2.094	Analyze and triage events to support event resolution and incident declaration	Anchor also reduces the reporting overhead significantly but making all audit logs downloadable as spreadsheets for processing by SIEM tools or manually. 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.2.096	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. Anchor also reduces the reporting overhead significantly by making all audit logs downloadable as spreadsheets for SIEM or manual processing. 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. 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

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™
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.	<p>MP.1.118-MP.3.125 require organizations to</p> <p>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.</p>	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™

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.	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.	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.	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.	<p>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.</p> <p>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.</p>	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.
Recovery (RE)	RE.2.138	Protect the confidentiality of backup CUI at storage locations.	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.	Compliant with Anchor™
Recovery (RE)	RE.3.139	Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined.		N/A

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.	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.	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.	Anchor™ Supports Compliance
Risk Management (RM)	RM.2.143	Remediate vulnerabilities in accordance with risk assessments.	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.	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. 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. 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

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.	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.		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.
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. 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. 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. 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

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™
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.	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. 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.	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.		Control and monitoring of all CUI are ensured even when it is outside the scope of the organization.

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™
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. 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.	Compliant with Anchor™
System and Information Integrity (SI)	SI.2.214	Monitor information system security alerts and advisories and take action in response.	Anchor's monitor incorporates the access patterns and creates reports and warning messages.	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.	Compliant with Anchor™
System and Information Integrity (SI)	SI.1.212	Update malicious code protection mechanisms when new releases are available.	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.1.213	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.		N/A
System and Information Integrity (SI)	SI.2.217	Identify unauthorized use of organizational systems.	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. Anchor does not provide detection for actions through email or user access to the system, unless they access data.	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 Information Integrity (SI)	SI.3.220	Utilize sandboxing to detect or block potentially malicious email.		N/A

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.

