NCP CDPP Standard #	NCP CSOP Procedure #	NCP CDPP Standard Name	NIST 800-171 rev 2	NIST 800-171A [assessment criteria]	US CMMC v2.0	CMMC Level 2 Assessment Criteria	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CIS CSC v8.0	CSA CCM v3.0.1	ISO 27001 v2013	ISO 27001 v2022	ISO 27002 v2013	ISO 27002 v2022	NIST 800-53 rev4	NIST 800-53 rev5	NIST CSF v1.1	PCI DSS v3.2	US CERT RMM v1.2	US FedRAMP [moderate]	US HIPAA	ITAR Part 120 [limited]	US NISPOM	EMEA UK Cyber Essentials	SCF #
AC-01	P-AC-01	Account Management	3.1.2	3.1.1[a] 3.1.1[b] 3.1.1[c] 3.1.1[d] 3.1.1[e] 3.1.1[f]	AC.L1-3.1.2	AC.L1-3.1.1[a] AC.L1-3.1.1[b] AC.L1-3.1.1[c] AC.L1-3.1.1[d] AC.L1-3.1.1[e] AC.L1-3.1.1[f]	CC6.1	16.13		IAM-10			9.2.5 9.2.6	5.15 5.16 5.18	AC-2	AC-2	PR.AC-1	8.1.3-8.1.5 8.2.2 8.5-8.5.1 8.6 8.7	AM:SG1.SP1 AM:SG1.SP2 AM:SG1.SP3 AM:SG1.SP4 ID:SG2.SP1 ID:SG2.SP2	AC-2	164.312(a)(2)(ii)		8-606		IAC-15
AC-02	P-AC-02	Access Enforcement	3.1.1	3.1.2[a] 3.1.2[b] 3.1.7[a] 3.1.7[b] 3.1.7[c]	AC.L1-3.1.1	AC.L1-3.1.2[a] AC.L1-3.1.2[b] AC.L2-3.1.7[a] AC.L2-3.1.7[b] AC.L2-3.1.7[c]	CC6.1						9.2.6 9.4	5.18	AC-3 AC-6	AC-3 AC-6		7.1-7.1.4 7.2-7.2.1 7.2.3	AM:SG1.SP1 ID:SG1.SP1 ID:SG1.SP2 ID:SG1.SP3 TM:SG4.SP1	AC-3 AC-6			8-606		IAC-20
AC-03	P-AC-03	Data Flow Enforcement – Access Control Lists (ACLs)	3.1.3	3.1.3[a] 3.1.3[b] 3.1.3[c] 3.1.3[d] 3.1.3[e]	AC.L2-3.1.3	AC.L2-3.1.3[a] AC.L2-3.1.3[b] AC.L2-3.1.3[c] AC.L2-3.1.3[d] AC.L2-3.1.3[e]	CC6.1 CC6.6	11.2	3.3 4.6 12.6 13.4				9.4.1 13.1.1	5.14 8.3 8.20	AC-4	AC-4		1.1-1.1.7 1.2-1.2.3 3.3 3.5 7.2-7.2.3	TM:SG4.SP1	AC-4					NET-04
AC-04	P-AC-04	Least Privilege	3.1.5	3.1.5[a] 3.1.5[b] 3.1.5[c] 3.1.5[d]	AC.L2-3.1.5	AC.L2-3.1.5[a] AC.L2-3.1.5[b] AC.L2-3.1.5[c] AC.L2-3.1.5[d]	CC6.1	14.6	5.4				9.1.2 9.2.2	5.15 5.18 8.3 8.12	AC-6	AC-6	PR.AC-4		AM:SG1.SP1 ID:SG1.SP1 ID:SG1.SP2 ID:SG1.SP3	AC-6			8-303		IAC-21
AC-05	P-AC-05	Authorize Access to Security Functions	3.1.5		AC.L2-3.1.5										AC-6(1)	AC-6(1)				AC-6(1)					IAC-21.1
AC-06	P-AC-06	Privileged Accounts	3.1.5		AC.L2-3.1.5										AC-6(5)	AC-6(5)				AC-6(5)					IAC-21.3
AC-07	P-AC-07	Non-Privileged Access for Non-Security Functions	3.1.6	3.1.6[a] 3.1.6[b]	AC.L2-3.1.6	AC.L2-3.1.6[a] AC.L2-3.1.6[b]			5.4						AC-6(2)	AC-6(2)				AC-6(2)					IAC-21.2
AC-08	P-AC-08	Auditing Use of Privileged Functions	3.1.7	3.1.7[d]	AC.L2-3.1.7	AC.L2-3.1.7[d]		4.3							AC-6(9)	AC-6(9)		10.2-10.2.7		AC-6(9)					IAC-21.4
AC-09	P-AC-09	Prohibit Non-Privileged Users from Executing Privileged Functions	3.1.7		AC.L2-3.1.7			4.8							AC-6(10)	AC-6(10)				AC-6(10)					IAC-21.5
AC-10	P-AC-10	Account Lockout	3.1.8	3.1.8[a] 3.1.8[b]	AC.L2-3.1.8	AC.L2-3.1.8[a] AC.L2-3.1.8[b]		16.11	4.10				6.2.1	8.1	AC-7	AC-7		8.1.6 8.1.7	TM:SG4.SP1	AC-7	164.312(a)(2)(iii)		8-609		IAC-22
AC-11	P-AC-11	System Use Notification (Logon Banner)	3.1.9	3.1.9[a] 3.1.9[b]	AC.L2-3.1.9	AC.L2-3.1.9[a] AC.L2-3.1.9[b]									AC-8	AC-8			TM:SG4.SP1	AC-8			8-609		SEA-18
AC-12	P-AC-12	Session Lock	3.1.10	3.1.10[a] 3.1.10[b] 3.1.10[c]	AC.L2-3.1.10	AC.L2-3.1.10[a] AC.L2-3.1.10[b] AC.L2-3.1.10[c]		16.11	4.3						AC-2(5) AC-11	AC-2(5) AC-11			TM:SG4.SP1	AC-2(5) AC-11	164.312(a)(2)(iii)		8-609		IAC-24
AC-13	P-AC-13	Pattern-Hiding Displays	3.1.10		AC.L2-3.1.10										AC-11(1)	AC-11(1)				AC-11(1)					IAC-24.1

Mapping & Assessment Criteria							Methods To Comply				Compliance Tracker		
CMMC Group	CMMC Practice #	NIST 800-171 R2 Control #	FAR 52.204-21 Control #	CMMC Assessment #	Assessment Objective	Reference	Focus of Practice / Control	Group Policy Object (GPO)	Documented Practices	Technology Considerations	Compliance Status	Assigned Stakeholder	Notes
Access Control (AC)	AC.L1-3.1.1	3.1.1	(b)(1)(i)	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).	Determine if:	Reference: NIST 800 171A 3.1.1	Technical Configurations (e.g., security settings)	Yes	- Active Directory (AD) or LDAP authentication. - Architectural review of planned network topology changes. - Change Control Board (CCB) approval for changes. - Data flow diagrams - Documented service tickets from managers are required to justify any user changes. - Disable session after fifteen (15) minutes of inactivity. - For standard users, access is revoked within twenty-four (24 hours) of notification to service desk. - Information Assurance (IA) testing for new technologies. - Initial passwords are issued to the user's manager. - Network diagrams - Operating systems & allocations lock the user/service out after six (6) consecutive failed attempts. - Password reset is forced upon entering a temporary password. - Role Based Access Control (RBAC) for user permission categories. - Secure system configurations to enforce authorized methods of remote access. - Security Incident Event Manager (SIEM) or log aggregator that alerts on certain event criteria. - SOPs for vendor management. - SOP exist for how accounts are added, deleted or modified. - SOP exist for how user identities are verified to reset passwords (e.g., answer several predetermined security questions). - SOP exist for remote access management. - SOP exist for service desk to remove/disable inactive user accounts that have not been used within ninety (90) days. - SOP for remote access management. - Thirty (30) minutes -For high-risk terminations, access is revoked within one (1) [illegible] notification to service desk.	- Active Directory - Network Policy Server (NPS) - Privileged Account Management (PAM) - Security Incident Event Manager (SIEM) - VPN Concentrator	Compliant		
				AC.L1-3.1.1[a]	authorized users are identified.	3.1.1[a]							
				AC.L1-3.1.1[b]	processes acting on behalf of authorized users are identified.	3.1.1[b]							
				AC.L1-3.1.1[c]	devices (and other systems) authorized to connect to the system are identified.	3.1.1[c]							
				AC.L1-3.1.1[d]	system access is limited to authorized users.	3.1.1[d]							
				AC.L1-3.1.1[e]	system access is limited to processes acting on behalf of authorized users.	3.1.1[e]							
				AC.L1-3.1.1[f]	system access is limited to authorized devices (including other systems).	3.1.1[f]							
				Examine	Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records.								
				Interview	Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities.								
				Test	Organizational processes for managing system accounts; mechanisms for implementing account management.								
	AC.L2-3.1.9	3.1.9		Provide privacy and security notices consistent with applicable Controlled Unclassified Information [CUI] rules.	Determine if:	Reference: NIST 800 171A 3.1.9	Administrative (e.g., policies, standards & procedures)	Yes	- Active Directory Group Policy Objects (GPOs) [illegible] banner for all Windows-based workstations and servers. - Non-Windows systems are configured with [illegible] banner that will work on Unix/Linux systems, as well as network gear, such as firewalls and routers. - Standardized logon banners are created one for Windows-based systems and one for non-Windows systems. - Users must acknowledge (e.g., [illegible] the logon banner to proceed with logon.	- Active Directory	Non-Compliant		
				AC.L2-3.1.9[a]	privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.	3.1.9[a]							
				AC.L2-3.1.9[b]	privacy and security notices are displayed.	3.1.9[b]							
				Examine	Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records.								
				Interview	System or network administrators; personnel with information security responsibilities; personnel with responsibility for providing legal advice; system developers.								
				Test	Mechanisms implementing system use notification.								
	AC.L2-3.1.21	3.1.21		Limit use of portable storage devices on external systems.	Determine if:	Reference: NIST 800 171A 3.1.21	Administrative (e.g., policies, standards & procedures)	Possible 3rd Party Solution	- Acceptable Use policies - Security awareness training.	- Active Directory - Mobile Device Management (MDM)	Not Applicable		
				AC.L2-3.1.21[a]	the use of portable storage devices containing CUI on external systems is identified and documented.	3.1.21[a]							
				AC.L2-3.1.21[b]	limits on the use of portable storage devices containing CUI on external systems are defined.	3.1.21[b]							
				AC.L2-3.1.21[c]	the use of portable storage devices containing CUI on external systems is limited as defined.	3.1.21[c]							
				Examine	Access control policy; procedures addressing the use of external systems; system security plan; [illegible] configuration settings and associated documentation; system connection or processing agreements; account management documentation; other relevant documents or records.								
				Interview	Personnel with responsibilities for restricting or prohibiting use of organization-controlled portable storage devices on external systems; system or network administrators; personnel with information security responsibilities.								
				Test	Mechanisms implementing restrictions on use of portable storage devices.								
	AC.L1-3.1.2	3.1.2	(b)(1)(ii)	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Determine if:	Reference: NIST 800 171A 3.1.2	Technical Configurations (e.g., security settings)	Yes	- Active Directory (AD) or LDAP authentication. - Architectural review of planned network topology changes. - Change Control Board (CCB) approval for changes. - Data flow diagrams - Documented service tickets from managers are required to justify any user changes. - Disable session after fifteen (15) minutes of inactivity. - For standard users, access is revoked within twenty-four (24 hours) of notification to service desk. - Information Assurance (IA) testing for new technologies. - Initial passwords are issued to the user's manager. - Network diagrams - Operating systems & allocations lock the user/service out after six (6) consecutive failed attempts. - Password reset is forced upon entering a temporary password. - Role Based Access Control (RBAC) for user permission categories. - Secure system configurations to enforce authorized methods of remote access. - Security Incident Event Manager (SIEM) or log aggregator that alerts on certain event criteria. - SOPs for vendor management. - SOP exist for how accounts are added, deleted or modified. - SOP exist for how user identities are verified to reset passwords (e.g., answer several predetermined security questions). - SOP exist for remote access management. - SOP exist for service desk to remove/disable inactive user accounts that have not been used within ninety (90) days.	- Active Directory - Network Policy Server (NPS) - Privileged Account Management (PAM) - Security Incident Event Manager (SIEM) - VPN Concentrator	Outsourced / Contracted		
				AC.L1-3.1.2[a]	the types of transactions and functions that authorized users are permitted to execute are defined.	3.1.2[a]							
				AC.L1-3.1.2[b]	system access is limited to the defined types of transactions and functions for authorized users.	3.1.2[b]							
				Examine	Access control policy; procedures addressing access enforcement; system security plan; system design documentation; [illegible] approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records.								
				Interview	Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers.								
				Test	Mechanisms implementing access control policy.								
	AC.L2-3.1.5	3.1.5		Employ the principle of least privilege, including for specific security functions and privileged accounts.	Determine if:	Reference: NIST 800 171A 3.1.5	Technical Configurations (e.g., security settings)	N/A	- Managers and/or process owners determine what least privilege means in practical terms to conduct operations. - Based on least privilege roles are assigned permissions and other criteria (e.g., time restrictions). - Only authorized security personnel are provided permissions to access security and security functions and security-related information. - To obtain privileged access, those users must have a valid business justification. - Specialized security awareness training is provided to privileged users. - Privileged users acknowledge in writing that they received specialized awareness training. - Privileged users provide evidence of technical competence (e.g., CISSP, CISA, MCITP, CCNA, etc.).	- Active Directory - Privileged Account Management (PAM)	Unknown		
				AC.L2-3.1.5[a]	privileged accounts are identified.	3.1.5[a]							
				AC.L2-3.1.5[b]	access to privileged accounts is authorized in accordance with the principle of least privilege.	3.1.5[b]							
				AC.L2-3.1.5[c]	security functions are identified.	3.1.5[c]							
				AC.L2-3.1.5[d]	access to security functions is authorized in accordance with the principle of least privilege.	3.1.5[d]							
				Examine	Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring/audit records; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access is to be explicitly authorized; list of system-generated privileged accounts; list of system administration personnel; other relevant documents or records.								
				Interview	Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities; personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.								
				Test	Organizational processes for managing system accounts; mechanisms for implementing account management; mechanisms implementing least privilege functions; mechanisms prohibiting privileged access to the system.								
	AC.L2-3.1.6	3.1.6		Use non-privileged accounts or roles when accessing nonsecurity functions.	Determine if:	Reference: NIST 800 171A 3.1.6	Administrative (e.g., policies, standards & procedures)	N/A	- SOP dictate users are prohibited from using privileged accounts to perform non-privileged functions.	N/A	Unknown		
				AC.L2-3.1.6[a]	nonsecurity functions are identified.	3.1.6[a]							
				AC.L2-3.1.6[b]	users are required to use non-privileged accounts or roles when accessing nonsecurity functions.	3.1.6[b]							
				Examine	Access control policy; procedures addressing least privilege; system security plan; list of system-generated security functions assigned to system accounts or roles; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records.								
				Interview	Personnel with responsibilities for defining least privileges necessary to accomplish specified organizational tasks; personnel with information security responsibilities; system or network administrators.								
				Test	Mechanisms implementing least privilege functions.								
	AC.L2-3.1.8	3.1.8		Limit unsuccessful logon attempts.	Determine if:	Reference: NIST 800 171A 3.1.8	Technical Configurations	Yes	- Active Directory Group Policy Objects (GPOs) lock accounts until released by an administrator. - Active Directory Group Policy Objects (GPOs) lock accounts after six (6) consecutive, unsuccessful access attempts.	- Active Directory	Unknown		
				AC.L2-3.1.8[a]	the means of limiting unsuccessful logon attempts is defined.	3.1.8[a]							
				AC.L2-3.1.8[b]	the defined means of limiting unsuccessful logon attempts is implemented.	3.1.8[b]							

Standard #	Procedure #	Standard Name	NIST 800-171 rev 2	CMMC v2.0	Security Concept Being Addressed By Standard	Implementation Status	Primary "Owner" To Ensure Implementation (e.g., team, group or role)	Individual(s) Assigned To Role
AC-01	P-AC-01	Account Management	3.1.2	AC.L1-3.1.2	Does the organization proactively govern account management of individual, group, system, application, guest and temporary accounts?	Compliant		
AC-02	P-AC-02	Access Enforcement	3.1.1	AC.L1-3.1.1	Does the organization enforce logical access permissions through the principle of "least privilege?"	Non-Compliant		
AC-03	P-AC-03	Data Flow Enforcement – Access Control Lists (ACLs)	3.1.3	AC.L2-3.1.3	Does the organization design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems?	Not Applicable		
AC-04	P-AC-04	Least Privilege	3.1.5	AC.L2-3.1.5	Does the organization utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions?	Outsourced / Contracted		
AC-07	P-AC-07	Non-Privileged Access for Non-Security Functions	3.1.6	AC.L2-3.1.6	Does the organization prohibit privileged users from using privileged accounts, while performing non-security functions?	Unknown		
AC-08	P-AC-08	Auditing Use of Privileged Functions	3.1.7	AC.L2-3.1.7	Does the organization audit the execution of privileged functions?	Unknown		
AC-09	P-AC-09	Prohibit Non-Privileged Users from Executing Privileged Functions	3.1.7	AC.L2-3.1.7	Does the organization prevent non-privileged users from executing privileged functions to include disabling, circumventing, altering implemented security safeguards / countermeasures?	Unknown		
AC-10	P-AC-10	Account Lockout	3.1.8	AC.L2-3.1.8	Does the organization enforce a limit for consecutive invalid logon attempts by a user during a organization-defined time period and automatically [illegible] when the maximum number of unsuccessful attempts is exceeded?	Unknown		
AC-11	P-AC-11	System Use Notification (Logon Banner)	3.1.9	AC.L2-3.1.9	Does the organization utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to the system that provides privacy and security notices?	Unknown		
AC-12	P-AC-12	Session Lock	3.1.10	AC.L2-3.1.10	Does the organization initiate a session lock after an organization-defined time period of inactivity or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods?	Unknown		
AC-13	P-AC-13	Pattern-Hiding Displays	3.1.10	AC.L2-3.1.10	Does the organization implement pattern-hiding displays to conceal information previously visible on the display during the session lock?	Unknown		
AC-14	P-AC-14	Session Termination	3.1.11	AC.L2-3.1.11	Are automated mechanisms used to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity?	Unknown		
AC-15	P-AC-15	Automated Monitoring & Control	3.1.12	AC.L2-3.1.12	Are automated mechanisms used to monitor and control remote access sessions?	Unknown		
AC-16	P-AC-16	Protection of Confidentiality / Integrity Using Encryption	3.1.13	AC.L2-3.1.13	Are cryptographic mechanisms used to protect the confidentiality and integrity of remote access sessions?	Unknown		
AC-17	P-AC-17	Managed Access Control Points	3.1.14	AC.L2-3.1.14	Does the organization route all remote accesses through managed network access control points (e.g.?, VPN concentrator)?	Unknown		
AC-18	P-AC-18	Privileged Commands & Access	3.1.15	AC.L2-3.1.15	Does the organization restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs?	Unknown		
AC-19	P-AC-19	Wireless Networking	3.1.16	AC.L2-3.1.16	Does the organization control authorized wireless usage and monitor for unauthorized wireless access?	Unknown		
AC-20	P-AC-20	Authentication & Encryption	3.1.17	AC.L2-3.1.17	Are authentication and cryptographic mechanisms used to protect wireless access?	Unknown		
AC-21	P-AC-21	Access Control For Mobile Devices	3.1.18	AC.L2-3.1.18	Do access control mechanisms for mobile devices enforce requirements for the connection of mobile devices to organizational systems?	Unknown		
AC-22	P-AC-22	Full Device & Container-Based Encryption	3.1.19	AC.L2-3.1.19	Are cryptographic mechanisms utilized to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption?	Unknown		
AC-23	P-AC-23	Use of External Information Systems	3.1.20	AC.L1-3.1.20	Does the organization govern how external parties, systems and services are used to securely store, process and transmit data?	Unknown		