Compliance Report

Project: Dev

Company: Test
Date: 09 March, 2023
Framework: Cmmc

Contact: bmarshall735@gmail.com
Generated by: Gapps

Table of contents

Overview

Project Metrics

The following page displays a quick overview of your compliance project along with key metrics. For more information, please view the project within the console.

Completion Progress

The project is 0.0% complete

Implemented

The project has implemented 0.0% of controls

Evidence

The project is 0.0% complete with evidence collection

Total Controls

The project has a total of 238 controls

Total Policies

The project has a total of 0 policies

Control Status

The table below displays the completion status of each applicable control within your project. Typically a control is considered complete if it is 100% implemented and has evidence attached. However each framework may have other requirements that are not represented in the table. Please view the project in the console for more details.

ID	Name	Status
1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	0%
2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	0%
3	Verify and control/limit connections to and use of external information systems.	0%
4	Control information posted or processed on publicly accessible information systems.	0%
5	Provide privacy and security notices consistent with applicable CUI rules.	0%
6	Limit use of portable storage devices on external systems.	0%
7	Employ the principle of least privilege, including for specific security functions and privileged accounts.	0%
8	Use non-privileged accounts or roles when accessing nonsecurity functions.	0%
9	Limit unsuccessful logon attempts.	0%
10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	0%
11	Authorize wireless access prior to allowing such connections.	0%

ID	Name	Status
12	Monitor and control remote access sessions.	0%
13	Route remote access via managed access control points.	0%
14	Control the flow of CUI in accordance with approved authorizations.	0%
15	Document the CMMC practices to implement the Access Control policy.	0%
16	Establish a policy that includes Access Control.	0%
17	Protect wireless access using authentication and encryption.	0%
18	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	0%
19	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	0%
20	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	0%
21	Terminate (automatically) user sessions after a defined condition.	0%
22	Control connection of mobile devices.	0%
23	Authorize remote execution of privileged commands and remote access to security-relevant information.	0%
24	Encrypt CUI on mobile devices and mobile computing platforms.	0%
25	Establish, maintain, and resource a plan that includes Access Control.	0%
26	Control information flows between security domains on connected systems.	0%
27	Periodically review and update CUI program access permissions.	0%
28	Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location,	0%

ID	Name	Status
	network connection state, and measured properties of the current user and role.	
29	Review and measure Access Control activities for effectiveness.	0%
30	Identify and mitigate risk associated with unidentified wireless access points connected to the network.	0%
31	Standardize and optimize a documented approach for Access Control across all applicable organizational units.	0%
32	Document the CMMC practices to implement the Asset Management policy.	0%
33	Establish a policy that includes Asset Management.	0%
34	Define procedures for the handling of CUI data.	0%
35	Establish, maintain, and resource a plan that includes Asset Management.	0%
36	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	0%
37	Review and measure Asset Management activities for effectiveness.	0%
38	Standardize and optimize a documented approach for Asset Management across all applicable organizational units.	0%
39	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	0%
40	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	0%
41	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	0%

ID	Name	Status
42	Review audit logs.	0%
43	Document the CMMC practices to implement the Audit and Accountability policy.	0%
44	Establish a policy that includes Audit and Accountability.	0%
45	Review and update logged events.	0%
46	Alert in the event of an audit logging process failure.	0%
47	Collect audit information (e.g., logs) into one or more central repositories.	0%
48	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	0%
49	Limit management of audit logging functionality to a subset of privileged users.	0%
50	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	0%
51	Provide audit record reduction and report generation to support on-demand analysis and reporting.	0%
52	Establish, maintain, and resource a plan that includes Audit and Accountability.	0%
53	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	0%
54	Review audit information for broad activity in addition to per-machine activity.	0%
55	Review and measure Audit and Accountability activities for effectiveness.	0%
56	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	0%

ID	Name	Status
57	Standardize and optimize a documented approach for Audit and Accountability across all applicable organizational units.	0%
58	Ensure that managers, system 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.	0%
59	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	0%
60	Document the CMMC practices to implement the Awareness and Training policy.	0%
61	Establish a policy that includes Awareness and Training.	0%
62	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	0%
63	Establish, maintain, and resource a plan that includes Awareness and Training.	0%
64	Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.	0%
65	Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training.	0%
66	Review and measure Awareness and Training activities for effectiveness.	0%
67	Standardize and optimize a documented approach for Awareness and Training across all applicable organizational units.	0%
68	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	0%

ID	Name	Status
69	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	0%
70	Control and monitor user-installed software.	0%
71	Establish and enforce security configuration settings for information technology products employed in organizational systems.	0%
72	Track, review, approve, or disapprove, and log changes to organizational systems.	0%
73	Analyze the security impact of changes prior to implementation.	0%
74	Document the CMMC practices to implement the Configuration Management policy.	0%
75	Establish a policy that includes Configuration Management.	0%
76	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	0%
77	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	0%
78	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	0%
79	Establish, maintain, and resource a plan that includes Configuration Management.	0%
80	Employ application whitelisting and an application vetting process for systems identified by the organization.	0%
81	Review and measure Configuration Management activities for effectiveness.	0%
82	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).	0%

ID	Name	Status
83	Standardize and optimize a documented approach for Configuration Management across all applicable organizational units.	0%
84	Identify information system users, processes acting on behalf of users, or devices.	0%
85	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	0%
86	Enforce a minimum password complexity and change of characters when new passwords are created.	0%
87	Prohibit password reuse for a specified number of generations.	0%
88	Allow temporary password use for system logons with an immediate change to a permanent password.	0%
89	Store and transmit only cryptographically-protected passwords.	0%
90	Obscure feedback of authentication information.	0%
91	Document the CMMC practices to implement the Identification and Authentication policy.	0%
92	Establish a policy that includes Identification and Authentication.	0%
93	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	0%
94	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.	0%
95	Prevent the reuse of identifiers for a defined period.	0%
96	Disable identifiers after a defined period of inactivity.	0%
97	Establish, maintain, and resource a plan that includes Identification and Authentication.	0%

ID	Name	Status
98	Review and measure Identification and Authentication activities for effectiveness.	0%
99	Standardize and optimize a documented approach for Identification and Authentication across all applicable organizational units.	0%
100	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	0%
101	Detect and report events.	0%
102	Analyze and triage events to support event resolution and incident declaration.	0%
103	Develop and implement responses to declared incidents according to pre-defined procedures.	0%
104	Perform root cause analysis on incidents to determine underlying causes.	0%
105	Document the CMMC practices to implement the Incident Response policy.	0%
106	Establish a policy that includes Incident Response.	0%
107	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	0%
108	Test the organizational incident response capability.	0%
109	Establish, maintain, and resource a plan that includes Incident Response.	0%
110	Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.	0%
111	Establish and maintain a security operations center capability that facilitates a 24/7 response capability.	0%
112	Review and measure Incident Response activities for effectiveness.	0%

ID	Name	Status
113	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.	0%
114	In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.	0%
115	Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.	0%
116	Perform unannounced operational exercises to demonstrate technical and procedural responses.	0%
117	Standardize and optimize a documented approach for Incident Response across all applicable organizational units.	0%
118	Perform maintenance on organizational systems.	0%
119	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	0%
120	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	0%
121	Supervise the maintenance activities of personnel without required access authorization.	0%
122	Document the CMMC practices to implement the Maintenance policy.	0%
123	Establish a policy that includes Maintenance.	0%
124	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	0%
125	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	0%
126	Establish, maintain, and resource a plan that includes Maintenance.	0%

ID	Name	Status
127	Review and measure Maintenance activities for effectiveness.	0%
128	Standardize and optimize a documented approach for Maintenance across all applicable organizational units.	0%
129	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	0%
130	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	0%
131	Limit access to CUI on system media to authorized users.	0%
132	Control the use of removable media on system components.	0%
133	Document the CMMC practices to implement the Media Protection policy.	0%
134	Establish a policy that includes Media Protection.	0%
135	Mark media with necessary CUI markings and distribution limitations.	0%
136	Prohibit the use of portable storage devices when such devices have no identifiable owner.	0%
137	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	0%
138	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	0%
139	Establish, maintain, and resource a plan that includes Media Protection.	0%
140	Review and measure Media Protection activities for effectiveness.	0%
141	Standardize and optimize a documented approach for Media Protection across all applicable organizational units.	0%
142		0%

ID	Name	Status
	Screen individuals prior to authorizing access to organizational systems containing CUI.	
143	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	0%
144	Document the CMMC practices to implement the Personnel Security policy.	0%
145	Establish a policy that includes Personnel Security.	0%
146	Establish, maintain, and resource a plan that includes Personnel Security.	0%
147	Review and measure Personnel Security activities for effectiveness.	0%
148	Standardize and optimize a documented approach for Personnel Security across all applicable organizational units.	0%
149	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	0%
150	Escort visitors and monitor visitor activity.	0%
151	Maintain audit logs of physical access.	0%
152	Control and manage physical access devices.	0%
153	Protect and monitor the physical facility and support infrastructure for organizational systems.	0%
154	Document the CMMC practices to implement the Physical Protection policy.	0%
155	Establish a policy that includes Physical Protection.	0%
156	Enforce safeguarding measures for CUI at alternate work sites.	0%
157		0%

ID	Name	Status
	Establish, maintain, and resource a plan that includes Physical Protection.	
158	Review and measure Physical Protection activities for effectiveness.	0%
159	Standardize and optimize a documented approach for Physical Protection across all applicable organizational units.	0%
160	Regularly perform and test data back-ups.	0%
161	Protect the confidentiality of backup CUI at storage locations.	0%
162	Document the CMMC practices to implement the Recovery policy.	0%
163	Establish a policy that includes Recovery.	0%
164	Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined.	0%
165	Establish, maintain, and resource a plan that includes Recovery.	0%
166	Review and measure Recovery activities for effectiveness.	0%
167	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	0%
168	Standardize and optimize a documented approach for Recovery across all applicable organizational units.	0%
169	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.	0%
170	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	0%
171	Remediate vulnerabilities in accordance with risk assessments.	0%

ID	Name	Status
172	Document the CMMC practices to implement the Risk Management policy.	0%
173	Establish a policy that includes Risk Management.	0%
174	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	0%
175	Develop and implement risk mitigation plans.	0%
176	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	0%
177	Establish, maintain, and resource a plan that includes Risk Management.	0%
178	Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.	0%
179	Catalog and periodically update threat profiles and adversary TTPs.	0%
180	Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	0%
181	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.	0%
182	Review and measure Risk Management activities for effectiveness.	0%
183	Utilize an exception process for non-whitelisted software that includes mitigation techniques.	0%
184	Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.	0%
185	Standardize and optimize a documented approach for Risk Management across all applicable organizational units.	0%

ID	Name	Status
186	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.	0%
187	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	0%
188	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	0%
189	Document the CMMC practices to implement the Security Assessment policy.	0%
190	Establish a policy that includes Security Assessment.	0%
191	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	0%
192	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.	0%
193	Establish, maintain, and resource a plan that includes Security Assessment.	0%
194	Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.	0%
195	Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.	0%
196	Periodically perform red teaming against organizational assets in order to validate defensive capabilities.	0%
197	Review and measure Security Assessment activities for effectiveness.	0%
198	Standardize and optimize a documented approach for Security Assessment across all applicable organizational units.	0%

ID	Name	Status
199	Document the CMMC practices to implement the Situational Awareness policy.	0%
200	Establish a policy that includes Situational Awareness.	0%
201	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	0%
202	Establish, maintain, and resource a plan that includes Situational Awareness.	0%
203	Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.	0%
204	Design network and system security capabilities to leverage, integrate, and share indicators of compromise.	0%
205	Review and measure Situational Awareness activities for effectiveness.	0%
206	Standardize and optimize a documented approach for Situational Awareness across all applicable organizational units.	0%
207	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.	0%
208	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	0%
209	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	0%
210	Use encrypted sessions for the management of network devices.	0%
211	Document the CMMC practices to implement the System and Communications Protection policy.	0%
212		0%

ID	Name	Status
	Establish a policy that includes System and Communications Protection.	
213	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	0%
214	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	0%
215	Separate user functionality from system management functionality.	0%
216	Prevent unauthorized and unintended information transfer via shared system resources.	0%
217	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	0%
218	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).	0%
219	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	0%
220	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	0%
221	Establish and manage cryptographic keys for cryptography employed in organizational systems.	0%
222	Control and monitor the use of mobile code.	0%
223	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	0%
224	Protect the authenticity of communications sessions.	0%

ID	Name	Status
225	Protect the confidentiality of CUI at rest.	0%
226	Implement Domain Name System (DNS) filtering services.	0%
227	Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).	0%
228	Establish, maintain, and resource a plan that includes System and Communications Protection.	0%
229	Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization.	0%
230	Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.	0%
231	Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries.	0%
232	Isolate administration of organizationally defined high-value critical network infrastructure components and servers.	0%
233	Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization.	0%
234	Review and measure System and Communications Protection activities for effectiveness.	0%
235	Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizationally defined boundaries.	0%
236	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	0%
237	Enforce port and protocol compliance.	0%

ID	Name	Status
238	Standardize and optimize a documented approach for System and Communications Protection across all applicable organizational units.	0%