Compliance Report

Project: Dev

Company: Test
Date: 30 March, 2023
Framework: Cmmc_v2

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 0.08% of controls

Evidence

The project is 0.0% complete with evidence collection

Total Controls

The project has a total of 110 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 Controlled Unclassified Information (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	Protect wireless access using authentication and encryption.	0%
16	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	0%
17	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	0%
18	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	0%
19	Terminate (automatically) user sessions after a defined condition.	0%
20	Control connection of mobile devices.	0%
21	Authorize remote execution of privileged commands and remote access to security-relevant information.	0%
22	Encrypt CUI on mobile devices and mobile computing platforms.	0%
23	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%
24	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	0%
25	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	0%
26	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%

ID	Name	Status
27	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%
28	Test the organizational incident response capability.	0%
29	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	0%
30	Review and update logged events.	0%
31	Alert in the event of an audit logging process failure.	0%
32	Protect audit information and audit logging tools from unauthorized access, modification and deletion.	0%
33	Limit management of audit logging functionality to a subset of privileged users.	0%
34	Enforce a minimum password complexity and change of characters when new passwords are created.	0%
35	Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.	0%
36	Provide audit record reduction and report generation to support on-demand analysis and reporting.	0%
37	Develop, document and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.	0%
38	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	0%
39	Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	0%

ID	Name	Status
40	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	0%
41	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles.	0%
42	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	0%
43	Control and monitor user-installed software.	0%
44	Establish and enforce security configuration settings for information technology products employed in organizational systems.	0%
45	Track, review, approve or disapprove and log changes to organizational systems.	0%
46	Analyze the security impact of changes prior to implementation.	0%
47	Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems.	0%
48	Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.	0%
49	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	0%
50	Identify information system users, processes acting on behalf of users or devices.	0%
51	Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.	0%
52	Prohibit password reuse for a specified number of generations.	0%
53		0%

ID	Name	Status
	Allow temporary password use for system logons with an immediate change to a permanent password.	
54	Store and transmit only cryptographically- protected passwords.	0%
55	Obscure feedback of authentication information.	0%
56	Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	0%
57	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	0%
58	Prevent the reuse of identifiers for a defined period.	0%
59	Disable identifiers after a defined period of inactivity.	0%
60	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities.	0%
61	Track, document and report incidents to designated officials and/or authorities both internal and external to the organization.	0%
62	Perform maintenance on organizational systems.	0%
63	Provide controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance.	0%
64	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	0%
65	Supervise the maintenance activities of personnel without required access authorization.	0%
66	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	0%
67		0%

ID	Name	Status
	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	
68	Sanitize or destroy information system media containing Federal Contract Information (FCI) before disposal or release for reuse.	0%
69	Protect (e.g., physically control and securely store) system media containing Federal Contract Information, both paper and digital.	0%
70	Limit access to CUI on system media to authorized users.	0%
71	Control the use of removable media on system components.	0%
72	Mark media with necessary CUI markings and distribution limitations.	0%
73	Prohibit the use of portable storage devices when such devices have no identifiable owner.	0%
74	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	0%
75	Protect and monitor the physical facility and support infrastructure for organizational systems.	0%
76	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	0%
77	Protect the confidentiality of backup CUI at storage locations.	0%
78	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.	0%
79	Escort visitors and monitor visitor activity.	0%
80	Maintain audit logs of physical access.	0%
81	Control and manage physical access devices.	0%
82	Enforce safeguarding measures for CUI at alternate work sites.	0%

ID	Name	Status
83	Screen individuals prior to authorizing access to organizational systems containing CUI.	0%
84	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	0%
85	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%
86	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	0%
87	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	0%
88	Remediate vulnerabilities in accordance with risk assessments.	0%
89	Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	0%
90	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	0%
91	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	0%
92	Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.	0%
93	Separate user functionality from system management functionality.	0%
94	Prevent unauthorized and unintended information transfer via shared system resources.	0%

ID	Name	Status
95	Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception).	0%
96	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (e.g., split tunneling).	0%
97	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	0%
98	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	0%
99	Establish and manage cryptographic keys for cryptography employed in organizational systems.	0%
100	Control and monitor the use of mobile code.	0%
101	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	0%
102	Protect the authenticity of communications sessions.	0%
103	Protect the confidentiality of CUI at rest.	0%
104	Monitor system security alerts and advisories and take action in response.	0%
105	Identify, report and correct information and information system flaws in a timely manner.	0%
106	Provide protection from malicious code at appropriate locations within organizational information systems.	0%
107	Update malicious code protection mechanisms when new releases are available.	0%

ID	Name	Status
108	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.	0%
109	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	0%
110	Identify unauthorized use of organizational systems.	0%