Safeguard Analysis

CIS Controls v8.1 - Priority Scoring

Client Company | April 28, 2026

Summary

Safeguards in report: 139 (excluding 14 N/A)
Below-priority (score = 0): 0 Above-priority: 139
Priority Score = Tier number x Implementation Level. Lower scores indicate higher remediation priority.

Priority	ID	Safeguard	Tier	Level	Score
1	**3.1**	Establish and Maintain a Data Management Process	1	Initial	**1**
2	**4.1**	Establish and Maintain a Secure Configuration Process	1	Initial	**1**
3	**4.2**	Establish and Maintain a Secure Configuration Process for Network Infrastructure	1	Initial	**1**
4	**11.1**	Establish and Maintain a Data Recovery Process	1	Initial	**1**
5	**15.1**	Establish and Maintain an Inventory of Service Providers	1	Initial	**1**
6	**2.1**	Establish and Maintain a Software Inventory	1	Partial	**2**
7	**6.2**	Establish an Access Revoking Process	1	Partial	**2**
8	**7.1**	Establish and Maintain a Vulnerability Management Process	1	Partial	**2**
9	**8.1**	Establish and Maintain an Audit Log Management Process	1	Partial	**2**
10	**5.1**	Establish and Maintain an Inventory of Accounts	1	Majority	**3**
11	**5.2**	Use Unique Passwords	1	Majority	**3**
12	**6.1**	Establish an Access Granting Process	1	Majority	**3**
13	**7.2**	Establish and Maintain a Remediation Process	1	Majority	**3**
14	**17.3**	Establish and Maintain an Enterprise Process for Reporting Incidents	1	Majority	**3**
15	**3.2**	Establish and Maintain a Data Inventory	3	Initial	**3**
16	**10.3**	Disable Autorun and Autoplay for Removable Media	3	Initial	**3**
17	**14.5**	Train Workforce Members on Causes of Unintentional Data Exposure	3	Initial	**3**
18	**1.1**	Establish and Maintain Detailed Enterprise Asset Inventory	1	Complete	**4**
19	**11.3**	Protect Recovery Data	2	Partial	**4**
20	**3.4**	Enforce Data Retention	4	Initial	**4**
21	**3.5**	Securely Dispose of Data	4	Initial	**4**
22	**14.8**	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	4	Initial	**4**
23	**3.7**	Establish and Maintain a Data Classification Scheme	5	Initial	**5**
24	**3.8**	Document Data Flows	5	Initial	**5**
25	**3.9**	Encrypt Data on Removable Media	5	Initial	**5**
26	**7.7**	Remediate Detected Vulnerabilities	5	Initial	**5**

Priority	ID	Safeguard	Tier	Level	Score
27	**15.2**	Establish and Maintain a Service Provider Management Policy	5	Initial	**5**
28	**15.3**	Classify Service Providers	5	Initial	**5**
29	**1.2**	Address Unauthorized Assets	2	Majority	**6**
30	**6.3**	Require MFA for Externally-Exposed Applications	2	Majority	**6**
31	**6.5**	Require MFA for Administrative Access	2	Majority	**6**
32	**11.2**	Perform Automated Backups	2	Majority	**6**
33	**14.1**	Establish and Maintain a Security Awareness Program	2	Majority	**6**
34	**14.3**	Train Workforce Members on Authentication Best Practices	2	Majority	**6**
35	**17.2**	Establish and Maintain Contact Information for Reporting Security Incidents	2	Majority	**6**
36	**2.3**	Address Unauthorized Software	3	Partial	**6**
37	**4.3**	Configure Automatic Session Locking on Enterprise Assets	3	Partial	**6**
38	**5.3**	Disable Dormant Accounts	3	Partial	**6**
39	**14.4**	Train Workforce on Data Handling Best Practices	3	Partial	**6**
40	**14.6**	Train Workforce Members on Recognizing and Reporting Security Incidents	3	Partial	**6**
41	**3.11**	Encrypt Sensitive Data At Rest	6	Initial	**6**
42	**8.9**	Centralize Audit Logs	6	Initial	**6**
43	**2.6**	Allowlist Authorized Libraries	7	Initial	**7**
44	**9.4**	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	7	Initial	**7**
45	**17.7**	Conduct Routine Incident Response Exercises	7	Initial	**7**
46	**8.2**	Collect Audit Logs	2	Complete	**8**
47	**11.4**	Establish and Maintain an Isolated Instance of Recovery Data	2	Complete	**8**
48	**14.2**	Train Workforce Members to Recognize Social Engineering Attacks	2	Complete	**8**
49	**2.2**	Ensure Authorized Software is Currently Supported	4	Partial	**8**
50	**3.6**	Encrypt Data on End-User Devices	4	Partial	**8**
51	**7.4**	Perform Automated Application Patch Management	4	Partial	**8**
52	**8.3**	Ensure Adequate Audit Log Storage	4	Partial	**8**
53	**14.9**	Conduct Role-Specific Security Awareness and Skills Training	4	Partial	**8**
54	**17.1**	Designate Personnel to Manage Incident Handling	4	Partial	**8**
55	**3.13**	Deploy a Data Loss Prevention Solution	8	Initial	**8**
56	**4.12**	Separate Enterprise Workspaces on Mobile End-User Devices	8	Initial	**8**
57	**8.12**	Collect Service Provider Logs	8	Initial	**8**
58	**4.4**	Implement and Manage a Firewall on Servers	3	Majority	**9**
59	**4.5**	Implement and Manage a Firewall on End-User Devices	3	Majority	**9**

Priority	ID	Safeguard	Tier	Level	Score
60	**4.7**	Manage Default Accounts on Enterprise Assets and Software	3	Majority	**9**
61	**12.1**	Ensure Network Infrastructure is Up-to-Date	3	Majority	**9**
62	**13.9**	Deploy Port-Level Access Control	9	Initial	**9**
63	**4.8**	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	5	Partial	**10**
64	**15.4**	Ensure Service Provider Contracts Include Security Requirements	5	Partial	**10**
65	**17.4**	Establish and Maintain an Incident Response Process	5	Partial	**10**
66	**17.5**	Assign Key Roles and Responsibilities	5	Partial	**10**
67	**17.6**	Define Mechanisms for Communicating During Incident Response	5	Partial	**10**
68	**17.9**	Establish and Maintain Security Incident Thresholds	5	Partial	**10**
69	**1.5**	Use a Passive Asset Discovery Tool	10	Initial	**10**
70	**2.7**	Allowlist Authorized Scripts	10	Initial	**10**
71	**3.14**	Log Sensitive Data Access	10	Initial	**10**
72	**4.6**	Securely Manage Enterprise Assets and Software	3	Complete	**12**
73	**5.4**	Restrict Administrator Privileges to Dedicated Administrator Accounts	3	Complete	**12**
74	**10.1**	Deploy and Maintain Anti-Malware Software	3	Complete	**12**
75	**10.2**	Configure Automatic Anti-Malware Signature Updates	3	Complete	**12**
76	**6.4**	Require MFA for Remote Network Access	4	Majority	**12**
77	**7.3**	Perform Automated Operating System Patch Management	4	Majority	**12**
78	**9.1**	Ensure Use of Only Fully Supported Browsers and Email Clients	4	Majority	**12**
79	**14.7**	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	4	Majority	**12**
80	**7.5**	Perform Automated Vulnerability Scans of Internal Enterprise Assets	6	Partial	**12**
81	**10.4**	Configure Automatic Anti-Malware Scanning of Removable Media	6	Partial	**12**
82	**12.5**	Centralize Network Authentication, Authorization, and Auditing (AAA)	6	Partial	**12**
83	**13.1**	Centralize Security Event Alerting	6	Partial	**12**
84	**18.2**	Perform Periodic External Penetration Tests	6	Partial	**12**
85	**1.4**	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	7	Partial	**14**
86	**8.8**	Collect Command-Line Audit Logs	7	Partial	**14**
87	**8.10**	Retain Audit Logs	7	Partial	**14**
88	**8.11**	Conduct Audit Log Reviews	7	Partial	**14**
89	**13.2**	Deploy a Host-Based Intrusion Detection Solution	7	Partial	**14**
90	**13.5**	Manage Access Control for Remote Assets	7	Partial	**14**
91	**17.8**	Conduct Post-Incident Reviews	7	Partial	**14**

Priority	ID	Safeguard	Tier	Level	Score
92	**9.5**	Implement DMARC	5	Majority	**15**
93	**18.1**	Establish and Maintain a Penetration Testing Program	5	Majority	**15**
94	**3.3**	Configure Data Access Control Lists	4	Complete	**16**
95	**9.2**	Use DNS Filtering Services	4	Complete	**16**
96	**15.5**	Assess Service Providers	8	Partial	**16**
97	**15.6**	Monitor Service Providers	8	Partial	**16**
98	**2.5**	Allowlist Authorized Software	6	Majority	**18**
99	**3.12**	Segment Data Processing and Storage Based on Sensitivity	6	Majority	**18**
100	**4.10**	Enforce Automatic Device Lockout on Portable End-User Devices	6	Majority	**18**
101	**10.6**	Centrally Manage Anti-Malware Software	6	Majority	**18**
102	**12.2**	Establish and Maintain a Secure Network Architecture	6	Majority	**18**
103	**15.7**	Securely Decommission Service Providers	9	Partial	**18**
104	**18.5**	Perform Periodic Internal Penetration Tests	9	Partial	**18**
105	**3.10**	Encrypt Sensitive Data in Transit	5	Complete	**20**
106	**4.9**	Configure Trusted DNS Servers on Enterprise Assets	5	Complete	**20**
107	**5.5**	Establish and Maintain an Inventory of Service Accounts	5	Complete	**20**
108	**5.6**	Centralize Account Management	5	Complete	**20**
109	**6.6**	Establish and Maintain an Inventory of Authentication and Authorization Systems	5	Complete	**20**
110	**7.6**	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	5	Complete	**20**
111	**9.6**	Block Unnecessary File Types	5	Complete	**20**
112	**12.4**	Establish and Maintain Architecture Diagram(s)	5	Complete	**20**
113	**6.8**	Define and Maintain Role-Based Access Control	10	Partial	**20**
114	**2.4**	Utilize Automated Software Inventory Tools	7	Majority	**21**
115	**4.11**	Enforce Remote Wipe Capability on Portable End-User Devices	7	Majority	**21**
116	**12.6**	Use of Secure Network Management and Communication Protocols	7	Majority	**21**
117	**12.7**	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	7	Majority	**21**
118	**6.7**	Centralize Access Control	6	Complete	**24**
119	**8.4**	Standardize Time Synchronization	6	Complete	**24**
120	**10.5**	Enable Anti-Exploitation Features	6	Complete	**24**
121	**10.7**	Use Behavior-Based Anti-Malware Software	6	Complete	**24**
122	**11.5**	Test Data Recovery	6	Complete	**24**
123	**18.3**	Remediate Penetration Test Findings	6	Complete	**24**
124	**12.8**	Establish and Maintain Dedicated Computing Resources for All Administrative	9	Majority	**27**

Priority	ID	Safeguard	Tier	Level	Score
		Work			
125	**13.7**	Deploy a Host-Based Intrusion Prevention Solution	9	Majority	**27**
126	**1.3**	Utilize an Active Discovery Tool	7	Complete	**28**
127	**8.5**	Collect Detailed Audit Logs	7	Complete	**28**
128	**8.6**	Collect DNS Query Audit Logs	7	Complete	**28**
129	**8.7**	Collect URL Request Audit Logs	7	Complete	**28**
130	**9.3**	Maintain and Enforce Network-Based URL Filters	7	Complete	**28**
131	**12.3**	Securely Manage Network Infrastructure	7	Complete	**28**
132	**13.3**	Deploy a Network Intrusion Detection Solution	7	Complete	**28**
133	**13.4**	Perform Traffic Filtering Between Network Segments	7	Complete	**28**
134	**13.6**	Collect Network Traffic Flow Logs	7	Complete	**28**
135	**18.4**	Validate Security Measures	10	Majority	**30**
136	**9.7**	Deploy and Maintain Email Server Anti-Malware Protections	8	Complete	**32**
137	**13.10**	Perform Application Layer Filtering	8	Complete	**32**
138	**13.8**	Deploy a Network Intrusion Prevention Solutions	9	Complete	**36**
139	**13.11**	Tune Security Event Alerting Thresholds	9	Complete	**36**