Gap Analysis

CIS Controls v8.1 - Prioritized Remediation Targets

Client Company | April 28, 2026

Summary

68 controls require attention (target: Majority (Level 3)).
Unscored controls included. Excludes 14 N/A controls.
Priority = Tier number x gap severity. Higher = more urgent.

Priority	Tier	ID	Control	Current	Target
#1	10	1.5	Use a Passive Asset Discovery Tool	Level 1	Majority (Level 3)
#2	10	2.7	Allowlist Authorized Scripts	Level 1	Majority (Level 3)
#3	10	3.14	Log Sensitive Data Access	Level 1	Majority (Level 3)
#4	9	13.9	Deploy Port-Level Access Control	Level 1	Majority (Level 3)
#5	8	3.13	Deploy a Data Loss Prevention Solution	Level 1	Majority (Level 3)
#6	8	4.12	Separate Enterprise Workspaces on Mobile End-User Devices	Level 1	Majority (Level 3)
#7	8	8.12	Collect Service Provider Logs	Level 1	Majority (Level 3)
#8	7	2.6	Allowlist Authorized Libraries	Level 1	Majority (Level 3)
#9	7	9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Level 1	Majority (Level 3)
#10	7	17.7	Conduct Routine Incident Response Exercises	Level 1	Majority (Level 3)
#11	6	3.11	Encrypt Sensitive Data At Rest	Level 1	Majority (Level 3)
#12	6	8.9	Centralize Audit Logs	Level 1	Majority (Level 3)
#13	5	3.7	Establish and Maintain a Data Classification Scheme	Level 1	Majority (Level 3)
#14	5	3.8	Document Data Flows	Level 1	Majority (Level 3)
#15	5	3.9	Encrypt Data on Removable Media	Level 1	Majority (Level 3)
#16	5	7.7	Remediate Detected Vulnerabilities	Level 1	Majority (Level 3)
#17	5	15.2	Establish and Maintain a Service Provider Management Policy	Level 1	Majority (Level 3)
#18	5	15.3	Classify Service Providers	Level 1	Majority (Level 3)
#19	10	6.8	Define and Maintain Role-Based Access Control	Level 2	Majority (Level 3)
#20	9	15.7	Securely Decommission Service Providers	Level 2	Majority (Level 3)
#21	9	18.5	Perform Periodic Internal Penetration Tests	Level 2	Majority (Level 3)
#22	4	3.4	Enforce Data Retention	Level 1	Majority (Level 3)
#23	4	3.5	Securely Dispose of Data	Level 1	Majority (Level 3)
#24	4	14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Level 1	Majority (Level 3)
#25	8	15.5	Assess Service Providers	Level 2	Majority (Level 3)
#26	8	15.6	Monitor Service Providers	Level 2	Majority (Level 3)

Priority	Tier	ID	Control	Current	Target
#27	7	1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Level 2	Majority (Level 3)
#28	7	8.8	Collect Command-Line Audit Logs	Level 2	Majority (Level 3)
#29	7	8.10	Retain Audit Logs	Level 2	Majority (Level 3)
#30	7	8.11	Conduct Audit Log Reviews	Level 2	Majority (Level 3)
#31	7	13.2	Deploy a Host-Based Intrusion Detection Solution	Level 2	Majority (Level 3)
#32	7	13.5	Manage Access Control for Remote Assets	Level 2	Majority (Level 3)
#33	7	17.8	Conduct Post-Incident Reviews	Level 2	Majority (Level 3)
#34	3	3.2	Establish and Maintain a Data Inventory	Level 1	Majority (Level 3)
#35	3	10.3	Disable Autorun and Autoplay for Removable Media	Level 1	Majority (Level 3)
#36	3	14.5	Train Workforce Members on Causes of Unintentional Data Exposure	Level 1	Majority (Level 3)
#37	6	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Level 2	Majority (Level 3)
#38	6	10.4	Configure Automatic Anti-Malware Scanning of Removable Media	Level 2	Majority (Level 3)
#39	6	12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)	Level 2	Majority (Level 3)
#40	6	13.1	Centralize Security Event Alerting	Level 2	Majority (Level 3)
#41	6	18.2	Perform Periodic External Penetration Tests	Level 2	Majority (Level 3)
#42	5	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Level 2	Majority (Level 3)
#43	5	15.4	Ensure Service Provider Contracts Include Security Requirements	Level 2	Majority (Level 3)
#44	5	17.4	Establish and Maintain an Incident Response Process	Level 2	Majority (Level 3)
#45	5	17.5	Assign Key Roles and Responsibilities	Level 2	Majority (Level 3)
#46	5	17.6	Define Mechanisms for Communicating During Incident Response	Level 2	Majority (Level 3)
#47	5	17.9	Establish and Maintain Security Incident Thresholds	Level 2	Majority (Level 3)
#48	4	2.2	Ensure Authorized Software is Currently Supported	Level 2	Majority (Level 3)
#49	4	3.6	Encrypt Data on End-User Devices	Level 2	Majority (Level 3)
#50	4	7.4	Perform Automated Application Patch Management	Level 2	Majority (Level 3)
#51	4	8.3	Ensure Adequate Audit Log Storage	Level 2	Majority (Level 3)
#52	4	14.9	Conduct Role-Specific Security Awareness and Skills Training	Level 2	Majority (Level 3)
#53	4	17.1	Designate Personnel to Manage Incident Handling	Level 2	Majority (Level 3)
#54	3	2.3	Address Unauthorized Software	Level 2	Majority (Level 3)
#55	3	4.3	Configure Automatic Session Locking on Enterprise Assets	Level 2	Majority (Level 3)
#56	3	5.3	Disable Dormant Accounts	Level 2	Majority (Level 3)
#57	3	14.4	Train Workforce on Data Handling Best Practices	Level 2	Majority (Level 3)
#58	3	14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	Level 2	Majority (Level 3)

Priority	Tier	ID	Control	Current	Target
#59	1	**3.1**	Establish and Maintain a Data Management Process	Level 1	Majority (Level 3)
#60	1	**4.1**	Establish and Maintain a Secure Configuration Process	Level 1	Majority (Level 3)
#61	1	**4.2**	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Level 1	Majority (Level 3)
#62	1	**11.1**	Establish and Maintain a Data Recovery Process	Level 1	Majority (Level 3)
#63	1	**15.1**	Establish and Maintain an Inventory of Service Providers	Level 1	Majority (Level 3)
#64	2	**11.3**	Protect Recovery Data	Level 2	Majority (Level 3)
#65	1	**2.1**	Establish and Maintain a Software Inventory	Level 2	Majority (Level 3)
#66	1	**6.2**	Establish an Access Revoking Process	Level 2	Majority (Level 3)
#67	1	**7.1**	Establish and Maintain a Vulnerability Management Process	Level 2	Majority (Level 3)
#68	1	**8.1**	Establish and Maintain an Audit Log Management Process	Level 2	Majority (Level 3)