CIS Controls™

CIS Critical Security Controls® (CIS Controls®) Measures and Metrics for Version 7

Sub--Control	Title	Description	Sensor	Measure	Sigma Level One	Sigma Level Two	Sigma Level Three	Sigma Level Four	Sigma Level Five	Sigma Level Six
1.1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	Active Device Discovery System	What percentage of the organization's networks have not recently been scanned by an active asset discovery tool?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	Passive Device Discovery System	What percentage of the organization's networks are not being monitored by a passive asset discovery tool?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	Log Management System / SIEM	What percentage of the organization's DHCP servers do not have logging enabled?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	Asset Inventory System	What percentage of the organization's hardware assets are not presently included in the organization's asset inventory?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Asset Inventory System	What percentage of the organization's hardware assets as a whole are not documented in the organization's asset inventory with the appropriate network address, hardware address, machine name, data asset owner, and department for each asset?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	Asset Inventory System	What percentage of the organization's unauthorized assets have not been removed from the network, quarantined or added to the inventory in a timely manner?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Network Level Authentication (NLA)	What percentage of the organization's network switches are not configured to require network-based port level access control for all client connections?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	Public Key Infrastructure (PKI)	What percentage of the organization's network switches are not configured to require network-based port level access control utilizing client certificates to authenticate all client connections?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	Software Application Inventory	What percentage of the organization's software are not presently included in the organization's software inventory?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.2	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	Software Application Inventory	What percentage of the organization's software applications or operating systems are not currently supported by the software's vendor?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.3	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	Software Application Inventory	What percentage of the organization's hardware assets have not recently been scanned by a software inventory tool to document the software installed on the system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.4	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	Software Application Inventory	What percentage of software assets are not documented in a software inventory system that tracks the name, version, publisher, and install date for all software, including operating systems authorized by the organization?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.5	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	Software Application Inventory	Is the organization's software inventory system tied into the hardware asset inventory system?	No			Yes		
2.6	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	Software Application Inventory	What percentage of the organization unauthorized software are either removed or the inventory is updated in a timely manner?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.7	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	Software Whitelisting System	What percentage of the organization's hardware assets are not utilizing application whitelisting technology to block unauthorized applications from executing on the system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.8	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.	Software Whitelisting System	What percentage of the organization's hardware assets are not utilizing application whitelisting technology to block unauthorized applications at the library level from executing on the system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.9	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.	Software Whitelisting System	What percentage of the organization's hardware assets are not utilizing application whitelisting technology to block unauthorized scripts from executing on the system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
2.10	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.	Network Firewall / Access Control System	What percentage of high risk business applications have not been physically or logically segregated from other business systems?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
3.1	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets have not recently been scanned by an SCAP compliant configuration monitoring system to identify all potential vulnerabilities on the organization's systems?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
3.2	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets have not recently been scanned by an SCAP compliant configuration monitoring system to identify all potential vulnerabilities on the organization's systems utilizing an authenticated connection to the system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
3.3	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets have not recently been scanned by an SCAP compliant configuration monitoring system to identify all potential vulnerabilities on the organization's systems utilizing a dedicated service account and host-based restrictions?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
3.4	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	Patch Management System	What percentage of the organization's hardware assets are not regularly updated by an automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
3.5	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	Patch Management System	What percentage of the organization's hardware assets are not regularly updated by an automated software update tools in order to ensure that third-party software is running the most recent security updates provided by the software vendor?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
3.6	Compare Back-to-back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	SCAP Based Vulnerability Management System	What percentage of the organization's identified vulnerabilities have not been remediated in a timely manner?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
3.7	Utilize a Risk-rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	SCAP Based Vulnerability Management System	Has the organization utilized a risk-rating process to prioritize the remediation of discovered vulnerabilities?	No			Yes		
4.1	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Privileged Account Management System	What percentage of the organization's hardware assets have not recently utilized automated tools to inventory all administrative accounts to ensure that only authorized individuals have elevated privileges?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	Privileged Account Management System	What percentage of the organization's systems utilize default passwords for accounts with elevated capabilities?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.3	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	Privileged Account Management System	What percentage of the organization's user accounts with elevated rights do not utilize a dedicated or secondary account for elevated activities?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.4	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	Privileged Account Management System	What percentage of the organization's systems, where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.5	Use Multifactor Authentication For All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.	Multi-Factor Authentication System	What percentage of the organization's hardware assets are not configured to utilize multi-factor authentication and encrypted channels for all elevated access?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.6	Use of Dedicated Machines For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.	Dedicated Administration Systems	What percentage of the organization's system administrators are not required to use a dedicated machine for all administrative tasks or tasks requiring elevated access?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.7	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.	Software Whitelisting System	What percentage of the organization's systems limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.8	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	Log Management System / SIEM	What percentage of the organizations hardware assets are not configured to issue a log entry and alert when an account is added to or removed from any group assigned elevated privileges?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
4.9	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	Log Management System / SIEM	What percentage of the organization's hardware assets are not configured to issue a log entry and alert on unsuccessful logins to an administrative account?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
5.1	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.	System Configuration Baselines & Images	What percentage of the organization's authorized operating systems and software does not have a documented, standard security configuration?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
5.2	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	System Configuration Baselines & Images	What percentage of the organization's hardware assets are not based upon secure images or templates based on the organization's approved configuration standards?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
5.3	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	System Configuration Baselines & Images	What percentage of the organization's master images are not stored on securely configured servers, validated with integrity checking tools, to ensure that only authorized changes to the images are possible?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
5.4	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	System Configuration Enforcement System	What percentage of the organization's hardware assets are not automatically configured via system configuration management tools that automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
5.5	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets have not recently been scanned by an SCAP compliant configuration monitoring system to verify all security configuration elements, and alert when unauthorized changes occur?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.1	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	Network Time Protocol (NTP) Systems	What percentage of the organization's hardware assets do not utilize at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.2	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.	Log Management System / SIEM	What percentage of the organization's hardware assets are not configured to require local logging on the asset?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.3	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	Log Management System / SIEM	What percentage of the organization's hardware assets are not configured to require local logging to include detailed information such as a event source, date, timestamp, source addresses, destination addresses, and other useful elements on the asset?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.4	Ensure adequate storage for logs	Ensure that all systems that store logs have adequate storage space for the logs generated.	Log Management System / SIEM	What percentage of the organization's hardware assets do not have adequate storage space for the logs generated?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.5	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Log Management System / SIEM	What percentage of the organization's hardware assets are not configured to aggregate appropriate logs to a central log management system for analysis and review?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.6	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	Log Management System / SIEM	What percentage of the organization's hardware assets are not configured to aggregate appropriate logs to a Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.7	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	Log Management System / SIEM	What percentage of the organization's hardware assets have not had their logs reviewed recently to identify anomalies or abnormal events?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
6.8	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	Log Management System / SIEM	What percentage of the organization's SIEM systems have not recently been tuned to better identify actionable events and decrease event noise?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	Software Whitelisting System	What percentage of the organization's hardware assets are running unsupported web browsers and email client software?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	Software Whitelisting System	What percentage of the organization's hardware assets are utilizing unauthorized browser or email client plugins or add-on applications?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	System Configuration Enforcement System	What percentage of the organization's hardware assets are utilizing unauthorized scripting languages that run in all web browsers and email clients?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
7.4	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	Network URL Filtering System	What percentage of the organization's hardware assets (whether physically at an organization's facilities or not) are not required to utilize network-based URL filters?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
7.5	Subscribe to URL-Categorization service	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	Network URL Filtering System	Has the organization subscribed to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available?	No			Yes		
7.6	Log all URL requests	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	Log Management System / SIEM	What percentage of the organization's hardware assets (whether physically at an organization's facilities or not) are not required to log all URL requests made from the organization's system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
7.7	Use of DNS Filtering Services	Use DNS filtering services to help block access to known malicious domains.	DNS Domain Filtering System	What percentage of the organization's DNS servers are using DNS filtering to help block access to known malicious domains?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
7.8	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.	Anti-Spam Gateway	Has the organization implemented Domain-based Message Authentication, Reporting and Conformance (DMARC), starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards?	No			Yes		
7.9	Block Unnecessary File Types	Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.	Anti-Spam Gateway	Has the organization blocked all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business?	No			Yes		
7.10	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	Anti-Spam Gateway	Does the organization utilize sandboxing to analyze and block inbound email attachments with malicious behavior?	No			Yes		
8.1	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Endpoint Protection System	What percentage of the organization's hardware assets do not utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
8.2	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	Endpoint Protection System	What percentage of the organization's hardware assets do not utilize recently updated, centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	System Configuration Enforcement System	What percentage of the organization's hardware assets are not configured to require anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
8.4	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	Endpoint Protection System	What percentage of the organization's hardware assets are not configured so that they automatically conduct an anti-malware scan of removable media when inserted or connected?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
8.5	Configure Devices Not To Auto-run Content	Configure devices to not auto-run content from removable media.	System Configuration Enforcement System	What percentage of the organization's hardware assets are not configured to not auto-run content from removable media?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
8.6	Centralize Anti-malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	Endpoint Protection System	What percentage of the organization's hardware assets do not utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
8.7	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	DNS Domain Filtering System	What percentage of the organization's Domain Name System (DNS) servers are not configured to require query logging to detect hostname lookups for known malicious domains?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
8.8	Enable Command-line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.	Log Management System / SIEM	What percentage of the organization's hardware assets have not enabled command-line audit logging for command shells, such as Python or Windows PowerShell with enhanced logging enabled?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
9.1	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets do not associate active ports, services and protocols to the hardware assets in the asset inventory?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
9.2	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets are not configured to require that only network ports, protocols, and services listening on a system with validated business needs, are running on each system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
9.3	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets are not regularly scanned by a port scanner to alert if unauthorized ports are detected on a system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
9.4	Apply Host-based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Host Based Firewall	What percentage of the organization's hardware assets are not utilizing host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
9.5	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Application Aware Firewall	What percentage of the organization's critical servers are not required to utilize application layer firewalls to verify and validate the traffic going to the server?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
10.1	Ensure Regular Automated Back Ups	Ensure that all system data is automatically backed up on regular basis.	Backup / Recovery System	What percentage of the organization's hardware assets are not configured to back up system data automatically on a regular basis?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
10.2	Perform Complete System Backups	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	Backup / Recovery System	What percentage of the organization's hardware assets are not configured to back up the complete asset automatically on a regular basis?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Backup / Recovery System	What percentage of the organization's hardware asset backups have not been tested recently to ensure that the backup is working properly?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
10.4	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	Backup / Recovery System	What percentage of the organization's hardware asset backups are not properly protected via physical security or encryption when they are stored, as well as when they are moved across the network (this includes remote backups and cloud services as well)?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.	Backup / Recovery System	What percentage of the organization's hardware assets does not have at least one backup destination that is not continuously addressable through operating system calls?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
11.1	Maintain Standard Security Configurations for Network Devices	Maintain standard, documented security configuration standards for all authorized network devices.	Network Device Management System	What percentage of the organization's network devices do not utilize a standard, documented security configuration standard for the device?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
11.2	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	Network Device Management System	What percentage of the organization's network devices do not have all configuration rules that allow traffic to flow through network devices be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	Network Device Management System	What percentage of the organization's network devices are not regularly compared against approved security configurations defined for each network device in use and alert when any deviations are discovered?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
11.4	Install the Latest Stable Version of Any Security-related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.	Network Device Management System	What percentage of the organization's network devices are not utilizing the latest stable version of any security-related updates?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.	Multi-Factor Authentication System	What percentage of the organization's network devices are not managed using multi-factor authentication and encrypted sessions?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less

CIS Controls™

CIS Controls Measures and Metrics for Version 7

Sub--Control	Title	Description	Sensor	Measure	Sigma Level One	Sigma Level Two	Sigma Level Three	Sigma Level Four	Sigma Level Five	Sigma Level Six
11.6	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	Dedicated Administration Systems	What percentage of the organization's network engineers are not utilizing a dedicated machine for all administrative tasks or tasks requiring elevated access to the organization's network devices?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
11.7	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Dedicated Administration Systems	What percentage of the organization's network engineers are not utilizing a dedicated machine, located on a dedicated management network, for all administrative tasks or tasks requiring elevated access to the organization's network devices?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.1	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	Network Firewall / Access Control System	Does the organization maintain an up-to-date inventory of all of the organization's network boundaries?	No			Yes		
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	System Configuration Enforcement System	What percentage of the organization's hardware assets have not recently been scanned to identify unauthorized network boundaries?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.3	Deny Communications with Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	Network Firewall / Access Control System	Are each of the organization's network boundaries configured to deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges?	No			Yes		
12.4	Deny Communication over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	Network Firewall / Access Control System	Are each of the organization's network boundaries configured to deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network?	No			Yes		
12.5	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	Network Packet Capture System	What percentage of the organization's network boundaries are not configured to record network packets passing through the boundary?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.6	Deploy Network-based IDS Sensor	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	Network Based Intrusion Detection System (NIDS)	What percentage of the organization's network boundaries are not configured to require network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems the boundary?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.7	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	Network Based Intrusion Prevention System (IPS)	What percentage of the organization's organization's network boundaries are not configured to require network-based Intrusion Prevention Systems (IPS) sensors to look for unusual attack mechanisms and detect compromise of these systems the boundary?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.8	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	Network Device Management System	What percentage of the organization's network boundary devices are not required to use NetFlow and logging data on the devices?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.9	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	Network Firewall / Access Control System	What percentage of the organization's network boundaries are not configured to pass through an authenticated application layer proxy that is configured to filter unauthorized connections?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.10	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Network Firewall / Access Control System	What percentage of the organization's network boundaries are not configured to decrypt all encrypted network traffic prior to analyzing the content?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.11	Require All Remote Login to Use Multi-factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	Multi-Factor Authentication System	What percentage of the organization's hardware devices are not required to utilize encryption and multi-factor authentication when remotely accessing the organization's network systems?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
12.12	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	System Configuration Enforcement System	What percentage of the organization's devices remotely logging into the organization's network are not scanned prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
13.1	Maintain an Inventory Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	Data Inventory / Classification System	Does the organization maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider?	No			Yes		
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	Data Inventory / Classification System	Does the organization regularly remove sensitive data sets or systems not regularly accessed by the organization from the network?	No			Yes		
13.3	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	Network Based Data Loss Prevention (DLP) System	Has the organization deployed an automated tool on network perimeters that monitors for sensitive information and blocks such transfers while alerting information security professionals?	No			Yes		
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	Network Firewall / Access Control System	Does the organization only allow access to authorized cloud storage or email providers?	No			Yes		
13.5	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	Network Based Data Loss Prevention (DLP) System	What percentage of the organization's network boundaries are not configured to monitor all traffic leaving the organization and detect any unauthorized use of encryption?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
13.6	Encrypt the Hard Drive of All Mobile Devices.	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	Whole Disk Encryption System	What percentage of the organization's mobile devices do not utilize approved whole disk encryption software?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
13.7	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	Endpoint Protection System	What percentage of the organization's hardware assets are not configured to only allow the use of specific USB devices?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
13.8	Manage System's External Removable Media's Read/write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	Endpoint Protection System	What percentage of the organization's hardware assets are not configured not to write data to USB storage devices, if there is no business need for supporting such devices?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
13.9	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	Endpoint Protection System	What percentage of the organization's hardware assets are not configured to encrypt all data stored on USB devices?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.1	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	Network Firewall / Access Control System	What percentage of the organization's network devices are not located on dedicated Virtual Local Area Networks (VLANs)?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.2	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	Network Firewall / Access Control System	What percentage of the organization's network devices are not located on dedicated Virtual Local Area Networks (VLANs) separated by firewall filters?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.3	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.	Network Firewall / Access Control System	What percentage of the organization's workstation devices are not located on dedicated Private Virtual Local Area Networks (PVLANs)?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.4	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	System Configuration Enforcement System	What percentage of the organization's sensitive information is not encrypted in transit?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.	Data Inventory / Classification System	What percentage of the organization's assets have not been scanned by an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.6	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	System Configuration Enforcement System	What percentage of the organization's hardware assets have not been configured with appropriate file system, network share, claims, application, or database specific access control lists?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.7	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Host Based Data Loss Prevention (DLP) System	What percentage of the organizations systems do not use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.8	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Host Based Data Loss Prevention (DLP) System	What percentage of the organization's sensitive information is not encrypted at rest and requires a secondary authentication mechanism not integrated into the operating system, in order to access the information?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	Log Management System / SIEM	What percentage of the organization's sensitive information does not require detailed audit logging when the data is accessed?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.1	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.	Network Device Management System	What percentage of the organization's wireless access points have not been authorized in the organization's wireless access point inventory?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.2	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	SCAP Based Vulnerability Management System	What percentage of the organization's hardware assets have not recently been scanned to detect and alert on unauthorized wireless access points connected to the wired network?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.3	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	Wireless Intrusion Detection System (WIDS)	What percentage of the organization's facilities do not have a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.4	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	System Configuration Enforcement System	What percentage of the organization's hardware assets is not configured to disable wireless access in devices that do not have a business purpose for wireless access?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.5	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	System Configuration Enforcement System	What percentage of the organization's hardware assets are not configured to allow access only to authorized wireless networks and to restrict access for other wireless networks?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.6	Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.	System Configuration Enforcement System	What percentage of the organization's hardware assets are not configured to disable peer-to-peer (adhoc) wireless network capabilities on wireless clients?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	Network Device Management System	What percentage of the organization's hardware assets are not configured to leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.8	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.	Network Device Management System	What percentage of the organization's hardware assets are not configured to utilize wireless networks to use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.9	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	System Configuration Enforcement System	What percentage of the organization's hardware assets are not configured to disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a business purpose?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
15.10	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	Network Device Management System	Does the organization utilize a separate a wireless network for personal or untrusted devices?	No			Yes		
16.1	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.	Identity & Access Management System	What percentage of the organization's authentication systems are not included in the organization's inventory?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
16.2	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	Identity & Access Management System	Has the organization configured access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems?	No			Yes		
16.3	Require Multi-factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	Multi-Factor Authentication System	What percentage of the organization's user accounts do not require multi-factor authentication?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
16.4	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	Identity & Access Management System	What percentage of the organization's hardware assets' authentication files cannot be accessed without root or administrator privileges and are not encrypted or hashed?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
16.5	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	Identity & Access Management System	What percentage of the organization's user accounts and authentication credentials are not transmitted across networks using encrypted channels?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
16.6	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	Identity & Access Management System	What percentage of the organization's accounts are not included in the organization's inventory?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
16.7	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	Identity & Access Management System	Has the organization established and followed an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor?	No			Yes		
16.8	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	Identity & Access Management System	What percentage of the organization's user accounts are not disabled if they cannot be associated with a business process or owner?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
16.9	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	Identity & Access Management System	Does the organization automatically disable dormant accounts after a set period of inactivity?	No			Yes		
16.10	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	Identity & Access Management System	What percentage of the organization's user accounts do not have an expiration date that is monitored and enforced?	69% or Less	31% or Less	6.7% or Less	0.62% or Less	0.023% or Less	0.00034% or Less
16.11	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	Identity & Access Management System	Does the organization automatically lock workstation sessions after a standard period of inactivity?	No			Yes		
16.12	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	Log Management System / SIEM	Does the organization monitor attempts to access deactivated accounts through audit logging?	No			Yes		
16.13	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Log Management System / SIEM	Does the organization alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration?	No			Yes		
17.1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	Training / Awareness Education Plans	Has the organization performed a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	No			Yes		
17.2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	Training / Awareness Education Plans	Has the organization delivered training to address the skills gap identified to positively impact workforce members' security behavior.	No			Yes		
17.3	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	Training / Awareness Education Plans	Has the organization created a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	No			Yes		
17.4	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	Training / Awareness Education Plans	Has the organization ensured that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	No			Yes		
17.5	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	Training / Awareness Education Plans	Has the organization trained workforce members on the importance of enabling and utilizing secure authentication.	No			Yes		
17.6	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	Training / Awareness Education Plans	Has the organization trained the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	No			Yes		
17.7	Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	Training / Awareness Education Plans	Has the organization trained workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	No			Yes		
17.8	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	Training / Awareness Education Plans	Has the organization trained workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	No			Yes		
17.9	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	Training / Awareness Education Plans	Has the organization trained employees to be able to identify the most common indicators of an incident and be able to report such an incident.	No			Yes		
18.1	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.	Secure Coding Standards	Has the organization established secure coding practices appropriate to the programming language and development environment being used.	No			Yes		
18.2	Ensure Explicit Error Checking is Performed for All In-house Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Secure Coding Standards	For in-house developed software, has the organization ensured that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	No			Yes		
18.3	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	Secure Coding Standards	Has the organization verified that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	No			Yes		
18.4	Only Use Up-to-date And Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.	Secure Coding Standards	Has the organization only used up-to-date and trusted third-party components for the software developed by the organization.	No			Yes		
18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized and extensively reviewed encryption algorithms.	Secure Coding Standards	Has the organization used only standardized and extensively reviewed encryption algorithms.	No			Yes		
18.6	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	Training / Awareness Education Plans	Has the organization ensured that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	No			Yes		
18.7	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	Software Vulnerability Scanning Tool	Has the organization applied static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	No			Yes		
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	Software Vulnerability Scanning Tool	Has the organization established a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	No			Yes		
18.9	Separate Production and Non-Production Systems	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.	Secure Coding Standards	Has the organization maintained separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.	No			Yes		
18.10	Deploy Web Application Firewalls (WAFs)	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Web Application Firewall (WAF)	Has the organization protected web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	No			Yes		
18.11	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	System Configuration Enforcement System	For applications that rely on a database, has the organization used standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	No			Yes		
19.1	Document Incident Response Procedures	Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.	Incident Management Plans	Has the organization ensured that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.	No			Yes		
19.2	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.	Incident Management Plans	Has the organization assigned job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.	No			Yes		
19.3	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	Incident Management Plans	Has the organization designated management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	No			Yes		
19.4	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	Incident Management Plans	Has the organization devised organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	No			Yes		
19.5	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	Incident Management Plans	Has the organization assembled and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	No			Yes		
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	Incident Management Plans	Has the organization published information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	No			Yes		
19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	Incident Management Plans	Has the organization planned and conducted routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	No			Yes		
19.8	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	Incident Management Plans	Has the organization created incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	No			Yes		
20.1	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	Penetration Testing Plans	Has the organization established a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	No			Yes		

CIS Controls™

CIS Controls Measures and Metrics for Version 7

Sub--Control	Title	Description	Sensor	Measure	Sigma Level One	Sigma Level Two	Sigma Level Three	Sigma Level Four	Sigma Level Five	Sigma Level Six
20.2	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	Penetration Testing Plans	Has the organization conducted regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	No			Yes		
20.3	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	Penetration Testing Plans	Has the organization performed periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	No			Yes		
20.4	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	Penetration Testing Plans	Has the organization included tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	No			Yes		
20.5	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	Penetration Testing Plans	Has the organization created a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	No			Yes		
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	Penetration Testing Plans	Has the organization used vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	No			Yes		
20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	Penetration Testing Plans	Has the organization, wherever possible, ensured that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	No			Yes		
20.8	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	Penetration Testing Plans	Has the organization ensured that any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	No			Yes		

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

License for Use