The CIS Critical Security Controls

CIS CONTROLS	EXPLANATION
Inventory and Control of Hardware Assets	Identify devices on your organization’s network, keep them updated, and maintain an inventory of assets that store or process information.
Inventory and Control of Software Assets	Use software inventory tools to automate all software documentation to ensure unauthorized software is blocked from executing on assets.
Continuous Vulnerability Management	Utilize a complaint vulnerability scanning tool to monitor your systems on the network to identify vulnerabilities and keep them up to date.
Controlled Use of Administrative Privileges	Configure systems to issue a log entry, alert when accounts are changed, and ensure administrative accounts have proper access.
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Maintain documented, standard security configuration standards for all authorized operating systems and software.
Maintenance, Monitoring, and Analysis of Audit Logs	Ensure that local logging has been enabled and appropriate logs are aggregated to a central log management system for analysis and review.
Email and Web Browser Protections	Ensure that only supported web browsers and email clients can execute in the organization using the latest official version.
Malware Defenses	Utilize centrally managed anti-malware software to monitor and defend each organization's workstations and servers continuously.
Limitations and Control of Network Ports, Protocols, and Services	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system, and perform automated port scans on a regular basis.
Data Recovery Capabilities	Ensure that all system data and key systems are automatically backed up on a regular basis.
Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Compare all network device configurations against approved security configurations, and manage all network devices using multi-factor authentication and encrypted sessions.

The CIS Critical Security Controls (cont)	
Boundary Defense	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges.
Data Protection	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
Controlled Access Based on the Need to Know	Segment the network based on the label or classification level of the information stored.
Wireless Access Control	Leverage the Advanced Encryption Standard to encrypt wireless data in transit and create a separate wireless network for personal or untrusted devices.
Account Monitoring and Control	Require multi-factor authentication for all user accounts on all systems, whether managed onsite or by a third-party provider.
Implement a Security Awareness and Training Program	Perform a skills gap analysis and train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
Application Software Security	Establish secure coding practices appropriate to the programming language and development environment being used.
Incident Response & Management	Ensure that there are written incident response plans that define the roles of personnel as well as phases of incident handling/management.
Penetration Tests and Red Team Exercises	Establish a program for penetration tests that includes a full scope of common attacks, such as wireless, client-based, and web application attacks.

The CIS Critical Security Controls

CIS CONTROLS	EXPLANATION
Inventory and Control of Hardware Assets	Identify devices on your organization’s network, keep them updated, and maintain an inventory of assets that store or process information.
Inventory and Control of Software Assets	Use software inventory tools to automate all software documentation to ensure unauthorized software is blocked from executing on assets.
Continuous Vulnerability Management	Utilize a complaint vulnerability scanning tool to monitor your systems on the network to identify vulnerabilities and keep them up to date.
Controlled Use of Administrative Privileges	Configure systems to issue a log entry, alert when accounts are changed, and ensure administrative accounts have proper access.
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Maintain documented, standard security configuration standards for all authorized operating systems and software.
Maintenance, Monitoring, and Analysis of Audit Logs	Ensure that local logging has been enabled and appropriate logs are aggregated to a central log management system for analysis and review.
Email and Web Browser Protections	Ensure that only supported web browsers and email clients can execute in the organization using the latest official version.
Malware Defenses	Utilize centrally managed anti-malware software to monitor and defend each organization's workstations and servers continuously.
Limitations and Control of Network Ports, Protocols, and Services	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system, and perform automated port scans on a regular basis.
Data Recovery Capabilities	Ensure that all system data and key systems are automatically backed up on a regular basis.
Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Compare all network device configurations against approved security configurations, and manage all network devices using multi-factor authentication and encrypted sessions.

The CIS Critical Security Controls (cont)	
Boundary Defense	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges.
Data Protection	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
Controlled Access Based on the Need to Know	Segment the network based on the label or classification level of the information stored.
Wireless Access Control	Leverage the Advanced Encryption Standard to encrypt wireless data in transit and create a separate wireless network for personal or untrusted devices.
Account Monitoring and Control	Require multi-factor authentication for all user accounts on all systems, whether managed onsite or by a third-party provider.
Implement a Security Awareness and Training Program	Perform a skills gap analysis and train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
Application Software Security	Establish secure coding practices appropriate to the programming language and development environment being used.
Incident Response & Management	Ensure that there are written incident response plans that define the roles of personnel as well as phases of incident handling/management.
Penetration Tests and Red Team Exercises	Establish a program for penetration tests that includes a full scope of common attacks, such as wireless, client-based, and web application attacks.