aunalytics

Cybersecurity Controls Checklist

Cybersecurity standards are constantly evolving as cyberattacks get increasingly complex. The following checklist from the Center for Internet Security (CIS) will allow your organization to evaluate whether the correct controls and safeguards are in place to meet global cybersecurity standards.

Cybersecurity Controls Overview

1. Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

2. Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

3. Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

4. Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

5. Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

6. Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

7. Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

8. Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

9. Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

10. Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

11. Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

12. Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

12. Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

14. Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

15. Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

16. Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

17. Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

18. Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Security Controls Checklist

1. Inventory and Control of Enterprise Assets

- □ Establish and Maintain Detailed Enterprise Asset Inventory
- □ Address Unauthorized Assets
- □ Utilize an Active Discovery Tool
- □ Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
- □ Use a Passive Asset Discovery Tool

2. Inventory and Control of Software Assets

- □ Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
- □ Establish and Maintain a Software Inventory
- □ Ensure Authorized Software is Currently Supported
- □ Address Unauthorized Software
- □ Utilize Automated Software Inventory Tools
- □ Allowlist Authorized Software
- □ Allowlist Authorized Libraries
- □ Allowlist Authorized Scripts

3. Data Protection

- □ Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
- □ Establish and Maintain a Data Management Process
- □ Establish and Maintain a Data Inventory
- □ Configure Data Access Control Lists
- □ Enforce Data Retention
- □ Securely Dispose of Data
- □ Encrypt Data on End-User Devices
- □ Establish and Maintain a Data Classification Scheme
- □ Document Data Flows
- □ Encrypt Data on Removable Media
- □ Encrypt Sensitive Data in Transit
- □ Encrypt Sensitive Data at Rest
- □ Segment Data Processing and Storage Based on Sensitivity
- □ Deploy a Data Loss Prevention Solution
- □ Log Sensitive Data Access

4. Secure Configuration of Enterprise Assets and Software

- □ Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
- □ Establish and Maintain a Secure Configuration Process
- □ Establish and Maintain a Secure Configuration Process for Network Infrastructure
- □ Configure Automatic Session Locking on Enterprise Assets
- □ Implement and Manage a Firewall on Servers
- □ Implement and Manage a Firewall on End-User Devices
- □ Securely Manage Enterprise Assets and Software
- □ Manage Default Accounts on Enterprise Assets and Software
- □ Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
- □ Configure Trusted DNS Servers on Enterprise Assets
- □ Enforce Automatic Device Lockout on Portable End-User Devices
- □ Enforce Remote Wipe Capability on Portable End-User Devices
- □ Separate Enterprise Workspaces on Mobile End-User Devices

5. Account Management

- □ Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
- □ Establish and Maintain an Inventory of Accounts
- □ Use Unique Passwords
- □ Disable Dormant Accounts
- □ Restrict Administrator Privileges to Dedicated Administrator Accounts
- □ Establish and Maintain an Inventory of Service Accounts]
- □ Centralize Account Management

6. Access Control Management

- □ Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.
- □ Establish an Access Granting Process
- □ Establish an Access Revoking Process
- □ Require MFA for Externally-Exposed Applications
- □ Require MFA for Remote Network Access
- □ Require MFA for Administrative Access
- □ Establish and Maintain an Inventory of Authentication and Authorization Systems Users
- □ Centralize Access Control
- □ Define and Maintain Role-Based Access Control

7. Continuous Vulnerability Management

- □ Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.
- □ Establish and Maintain a Vulnerability Management Process
- □ Establish and Maintain a Remediation Process
- □ Perform Automated Operating System Patch Management
- □ Perform Automated Application Patch Management
- □ Perform Automated Vulnerability Scans of Internal Enterprise Assets
- □ Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
- □ Remediate Detected Vulnerabilities

8. Audit Log Management

- □ Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
- □ Establish and Maintain an Audit Log Management Process
- □ Collect Audit Logs
- □ Ensure Adequate Audit Log Storage
- □ Standardize Time Synchronization
- □ Collect Detailed Audit Logs
- □ Collect DNS Query Audit Logs
- □ Collect URL Request Audit Logs
- □ Collect Command-Line Audit Logs
- □ Centralize Audit Logs
- □ Retain Audit Logs
- □ Conduct Audit Log Reviews
- □ Collect Service Provider Logs

9. Email and Web Browser Protections

- □ Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.
- □ Ensure Use of Only Fully Supported Browsers and Email Clients
- □ Use DNS Filtering Services
- □ Maintain and Enforce Network-Based URL Filters
- □ Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
- □ Implement DMARC
- □ Block Unnecessary File Types
- □ Deploy and Maintain Email Server Anti-Malware Protections

10. Malware Defenses

- □ Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
- □ Deploy and Maintain Anti-Malware Software
- □ Configure Automatic Anti-Malware Signature Updates
- □ Disable Autorun and Autoplay for Removable Media
- □ Configure Automatic Anti-Malware Scanning of Removable Media
- □ Enable Anti-Exploitation Features
- □ Centrally Manage Anti-Malware Software
- □ Use Behavior-Based Anti-Malware Software

11. Data Recovery

- □ Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.
- □ Establish and Maintain a Data Recovery Process
- □ Perform Automated Backups
- □ Protect Recovery Data
- □ Establish and Maintain an Isolated Instance of Recovery Data
- □ Test Data Recovery

12. Network Infrastructure Management

- □ Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.
- □ Ensure Network Infrastructure is Up-to-Date
- □ Establish and Maintain a Secure Network Architecture
- □ Securely Manage Network Infrastructure
- □ Establish and Maintain Architecture Diagram(s)
- □ Centralize Network Authentication, Authorization, and Auditing (AAA)
- □ Use of Secure Network Management and Communication Protocols
- □ Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
- □ Establish and Maintain Dedicated Computing Resources For all Administrative Work

13. Network Monitoring and Defense

- □ Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
- □ Centralize Security Event Alerting
- □ Deploy a Host-Based Intrusion Detection Solution
- □ Deploy a Network Intrusion Detection Solution
- □ Perform Traffic Filtering Between Network Segments
- □ Manage Access Control for Remote Assets
- □ Collect Network Traffic Flow Logs
- □ Deploy a Host-Based Intrusion Prevention Solution
- □ Deploy a Network Intrusion Prevention Solution
- □ Deploy Port-Level Access Control
- □ Perform Application Layer Filtering
- □ Tune Security Event Alerting Thresholds

14. Security Awareness and Skills Training

- □ Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
- □ Establish and Maintain a Security Awareness Program
- □ Train Workforce Members to Recognize Social Engineering Attacks
- □ Train Workforce Members on Authentication Best Practices
- □ Train Workforce on Data Handling Best Practices
- □ Train Workforce Members on Causes of Unintentional Data Exposure
- □ Train Workforce Members on Recognizing and Reporting Security Incident
- □ Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
- □ Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
- □ Conduct Role-Specific Security Awareness and Skills Training

15. Service Provider Management

- □ Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.
- □ Establish and Maintain an Inventory of Service Providers
- □ Establish and Maintain a Service Provider Management Policy
- □ Classify Service Providers
- □ Ensure Service Provider Contracts Include Security Requirements
- □ Assess Service Providers
- □ Monitor Service Providers
- □ Securely Decommission Service Providers

16. Application Software Security

- □ Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.
- □ Establish and Maintain a Secure Application Development Process
- □ Establish and Maintain a Process to Accept and Address Software Vulnerabilities
- □ Perform Root Cause Analysis on Security Vulnerabilities
- □ Establish and Manage an Inventory of Third-Party Software Components
- □ Use Up-to-Date and Trusted Third-Party Software Components
- □ Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
- □ Use Standard Hardening Configuration Templates for Application Infrastructure
- □ Separate Production and Non-Production Systems
- □ Train Developers in Application Security Concepts and Secure Coding
- □ Apply Secure Design Principles in Application Architectures
- □ Leverage Vetted Modules or Services for Application Security Components
- □ Implement Code-Level Security Checks
- □ Conduct Application Penetration Testing
- □ Conduct Threat Modeling

17. Incident Response Management

- □ Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
- □ Designate Personnel to Manage Incident Handling
- □ Establish and Maintain Contact Information for Reporting Security Incidents
- □ Establish and Maintain an Enterprise Process for Reporting Incidents
- □ Establish and Maintain an Incident Response Process
- □ Assign Key Roles and Responsibilities
- □ Define Mechanisms for Communicating During Incident Response
- □ Conduct Routine Incident Response Exercises
- □ Conduct Post-Incident Reviews
- □ Establish and Maintain Security Incident Thresholds

18. Penetration Testing

- □ Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.
- □ Establish and Maintain a Penetration Testing Program
- □ Perform Periodic External Penetration Tests
- □ Remediate Penetration Test Findings
- □ Validate Security Measures
- □ Perform Periodic Internal Penetration Tests

> After utilizing this list to identify areas for improvement, your business may benefit from enlisting a team of security experts to assist. Let Aunalytics guide you on your Security Maturity journey to implement the controls that make sense for your business in a phased, prioritized approach. Contact us to find out how.

About Aunalytics

Aunalytics is the data platform company delivering answers for your business. Aunalytics provides Insights-as-a-Service to answer enterprise and midsized companies' most important IT and business questions. The Aunalytics® cloud-native data platform is built for universal data access, advanced analytics and AI while unifying disparate data silos into a single golden record of accurate, actionable business information. Its Daybreak™ industry intelligent data mart combined with the power of the Aunalytics data platform provides industry-specific data models with built-in queries and AI to ensure access to timely, accurate data and answers to critical business and IT questions. Through its side-by-side digital transformation model, Aunalytics provides on-demand scalable access to technology, data science, and AI experts to seamlessly transform customers' businesses. To learn more contact us at +1 855-799-DATA or visit Aunalytics at https://www.aunalytics.com or on Twitter and LinkedIn.