NIST Security Controls Implementation Guide

The following table outlines key NIST security controls from SP 800-53 with practical implementation guidance:

Control ID	Control Title	Control Category
AC-1 - Access Control Policy and Procedure	Access Controls	Develop a formal access control policy, including least privilege principle. Define and enforce rules for user access rights based on roles and responsibilities.
AC-2 - Identification and Authentication	Access Controls	Implement multifactor authentication (password + token/biometric) for all users, especially administrators. Regularly review and update authentication methods to ensure they remain secure.
AC-3 - Access Enforcement	Access Controls	Enforce access control policies via automated tools or manual verification. Use access certification processes periodically.
AC-4 - Audit Record Content	Audit and Accountability	Log security-relevant events such as login attempts, changes, and system modifications. Store logs securely with configured retention policies.
AC-5 - Transmission Security	Transmission Security	Encrypt sensitive data during transmission using appropriate cryptographic protocols (e.g., TLS/SSL).
AU-1 - Audit Policy and Procedure	Audit and Accountability	Develop a formal audit policy, outlining frequency, scope, and methods for conducting audits.
AU-2 - Audit Event Collection and Transmission	Audit and Accountability	Implement mechanisms to collect and transmit audit logs securely to an appropriate storage location.
AU-3 - Audit Record Content	Audit and Accountability	Log security-relevant events like login attempts, changes, and system modifications. Store logs securely with configured retention policies.

Control ID	Control Title	Control Category
AU-4 - Audit Processing and Analysis	Audit and Accountability	Use automated tools or manual processes to analyze audit records for anomalies and potential threats.
AU-5 - Audit Report Generation and Distribution	Audit and Accountability	Generate periodic reports summarizing audit findings, distributing them to appropriate stakeholders.
MA-2 - Media Protection	Media Security	Encrypt data on removable media, store it in secured locations, and limit access to authorized personnel.
MA-3 - Removable/Portable Media Control	Media Security	Limit the use of removable/portable media by implementing policies and procedures for approval, storage, and access controls.
MA-4 - Media Protection	Media Security	Encrypt data on removable media, store it in secured locations, and limit access to authorized personnel.
PS-1 - Personnel Screening	Personnel Security	Implement a comprehensive personnel screening program that includes background checks for employees and contractors.
PS-2 - Personnel Background Investigation	Personnel Security	Conduct periodic background investigations on personnel with access to sensitive information or systems.
PS-3 - Personnel Access Review	Personnel Security	Periodically review personnel security clearances, access rights, and overall suitability for their roles.
PL-1 - Position-Specific Training	Privacy Controls	Provide position-specific training on privacy requirements and responsibilities to employees who handle sensitive information.
PL-2 - Incident Response Plan	Privacy Controls	Establish a plan to respond to privacy incidents, including procedures for containment, notification, and mitigation.
PL-3 - Notification of Privacy Breaches	Privacy Controls	Develop procedures for notifying affected parties in case of a privacy breach or data exfiltration event.
PL-4 - Data Minimization	Privacy Controls	Limit the collection and retention of personal information to what is necessary for organizational purposes.
PL-5 - Retention	Privacy Controls	Define and implement data retention periods based on legal, regulatory, or business requirements.

Control ID	Control Title	Control Category
PL-6 - Deletion of Unnecessary Personal Information	Privacy Controls	Establish processes for secure deletion of personal information when it is no longer needed.
SI-1 - System Development	System Development	Implement a formal system development process with security controls integrated into each phase, including planning, design, coding, and testing.
SI-2 - Supply Chain Risk Management	System Development	Assess potential risks in the supply chain for hardware, software, or services, and take appropriate mitigations to protect against threats.
SI-3 - Data Integrity	Data Integrity	Implement mechanisms to ensure data integrity, including checksums, hashes, and digital signatures for critical data.
SI-4 - System Maintenance	System Maintenance	Establish regular software updates, patch deployments, and system monitoring with clear incident response procedures.
SI-5 - Organizational Security Policy	System Maintenance	Develop a formal security policy that addresses organizational roles, responsibilities, and expectations for system maintenance activities.
SI-6 - Security Assessment and Authorization	System Maintenance	Conduct regular security assessments and authorization processes to validate ongoing suitability of systems and components.
SI-7 - Configuration Management Plan	System Maintenance	Develop a formal configuration management plan that covers versioning, change control, and impact assessment for system configurations.
CM-1 - Identification of Content	Controlled Access Information	Categorize information based on sensitivity and apply appropriate protection controls according to its classification level.
CM-2 - Classification	Controlled Access Information	Implement a formal process for classifying information based on its sensitivity and potential impact if disclosed or compromised.
CM-3 - Safeguarding	Controlled Access Information	Apply safeguards commensurate with the classification level of controlled access information (e.g., encryption, access controls).

Control ID	Control Title	Control Category
CM-4 - Distribution	Controlled Access Information	Restrict distribution and sharing of controlled access information according to its classification level and organizational need-to-know.
CM-5 - Monitoring and Reporting	Controlled Access Information	Establish mechanisms for monitoring access and use of controlled access information, including auditing and reporting capabilities.
CM-6 - Audit Record Retention	Controlled Access Information	Preserve audit records related to controlled access information in secure storage, with defined retention periods based on legal, regulatory, or business requirements.
CM-7 - System Security Plan	Controlled Access Information	Develop a system security plan that addresses protection of controlled access information across the system lifecycle.
CA-1 - Identification and Authentication	Configuration Management	Implement strong identification and authentication mechanisms for all users accessing systems and data.
CA-2 - Configuration Management	Configuration Management	Establish a formal configuration management program with version control, change management, and regular audits. Set baseline configurations and monitor for deviations.
CA-3 - Configuration Control	Configuration Management	Implement controls to manage changes in system configurations, including approval processes, review boards, and documentation.
CA-4 - Identification and Authentication of Devices	Device Management	Ensure devices connecting to systems are authenticated and authorized according to organizational policies.
MA-1 - Media Protection Service	Media Security	Establish a media protection service that includes encryption, access controls, and secure disposal processes for removable/portable media.
SC-1 - Incident Response Plan	System Architecture Design and Implementation	Develop an incident response plan outlining procedures for containing, eradicating, and recovering from security incidents.
SC-2 - Incident Response Team	System Architecture Design and Implementation	Identify a formal incident response team with defined roles and responsibilities to manage potential security incidents.

Control ID	Control Title	Control Category
SC-3 - Communication Plan	System Architecture Design and Implementation	Establish a communication plan for disseminating information regarding security incidents, both internally and externally as needed.
SC-4 - Incident Response Policy	System Architecture Design and Implementation	Develop an incident response policy that defines the organizational approach to responding to security incidents, including escalation procedures.
SC-5 - Incident Response Coordination	System Architecture Design and Implementation	Define coordination processes for engaging internal and external stakeholders (e.g., law enforcement, vendors) during a security incident.
SC-6 - Information Sharing	System Architecture Design and Implementation	Develop formal mechanisms for sharing information related to security threats and incidents with trusted partners or organizations.
SC-7 - Incident Response Metrics	System Architecture Design and Implementation	Define metrics for evaluating the effectiveness of security incident response efforts, including response time, containment efficiency, and recovery speed.
SI-1 - System Development	System Architecture Design and Implementation	Implement a formal system development process with security controls integrated into each phase, including planning, design, coding, and testing.
SI-2 - Supply Chain Risk Management	System Architecture Design and Implementation	Assess potential risks in the supply chain for hardware, software, or services, and take appropriate mitigations to protect against threats.
SI-3 - Data Integrity	System Architecture Design and Implementation	Implement mechanisms to ensure data integrity, including checksums, hashes, and digital signatures for critical data.
SI-4 - System Maintenance	System Architecture Design and Implementation	Establish regular software updates, patch deployments, and system monitoring with clear incident response procedures.
SC-8 - Software Component Verification	System Architecture Design and Implementation	Verify the integrity of third-party software components by validating cryptographic signatures or hashes before deployment.

Control ID	Control Title	Control Category
PR-1 - Publicly Disclosed Vulnerabilities	Program Management	Implement a process for identifying, tracking, and prioritizing remediation efforts for publicly disclosed vulnerabilities affecting organizational systems.
PR-2 - Privately Disclosed Vulnerabilities	Program Management	Establish procedures for receiving, evaluating, and responding to privately disclosed vulnerabilities by vendors or researchers.
PR-3 - System Inventory	Program Management	Maintain an up-to-date inventory of all systems within the organization's environment, including hardware, software, and firmware configurations.
PL-1 - Privacy Impact Assessment	Privacy Controls	Conduct privacy impact assessments for new projects or initiatives to identify potential privacy risks and mitigations before implementation.
PL-2 - Privacy Policies and Practices	Privacy Controls	Establish formal privacy policies and practices that define organizational expectations regarding collection, use, retention, and disclosure of personal information.
PL-3 - Data Minimization	Privacy Controls	Limit the collection and retention of personal information to what is necessary for organizational purposes.
PL-4 - Retention	Privacy Controls	Define and implement data retention periods based on legal, regulatory, or business requirements.
PL-5 - Deletion of Unnecessary Personal Information	Privacy Controls	Establish processes for secure deletion of personal information when it is no longer needed.
CA-3 - Configuration Control	Configuration Management	Implement controls to manage changes in system configurations, including approval processes, review boards, and documentation.
CM-1 - Identification of Content	Controlled Access Information	Categorize information based on sensitivity and apply appropriate protection controls according to its classification level.
CM-2 - Classification	Controlled Access Information	Implement a formal process for classifying information based on its sensitivity and potential impact if disclosed or compromised.

Control ID	Control Title	Control Category
CM-3 - Safeguarding	Controlled Access Information	Apply safeguards commensurate with the classification level of controlled access information (e.g., encryption, access controls).
CM-4 - Distribution	Controlled Access Information	Restrict distribution and sharing of controlled access information according to its classification level and organizational need-to-know.
CM-5 - Monitoring and Reporting	Controlled Access Information	Establish mechanisms for monitoring access and use of controlled access information, including auditing and reporting capabilities.
CM-6 - Audit Record Retention	Controlled Access Information	Preserve audit records related to controlled access information in secure storage, with defined retention periods based on legal, regulatory, or business requirements.
CM-7 - System Security Plan	Controlled Access Information	Develop a system security plan that addresses protection of controlled access information across the system lifecycle.
PL-6 - Data Sharing	Privacy Controls	Establish formal processes for sharing personal information with third parties while ensuring compliance with legal, regulatory, or contractual obligations.
SC-9 - Information System Component Security Plan	System Architecture Design and Implementation	Develop a security plan for each critical system component, including security controls, risk mitigations, and monitoring strategies.
SI-8 - System Development Process	System Architecture Design and Implementation	Implement a formal system development process that includes security considerations at every stage, from initial planning through deployment and maintenance.
SC-10 - Incident Response Plan Update	System Architecture Design and Implementation	Regularly update the incident response plan to address emerging threats, new technologies, or organizational changes.
PR-4 - Vulnerability Scanning	Program Management	Implement a program of regular vulnerability scanning across organizational systems to identify potential security weaknesses.
PL-7 - Privacy Impact Assessment Update	Privacy Controls	Periodically review and update privacy impact assessments as system changes, new technologies are adopted, or regulatory requirements evolve.

Control ID	Control Title	Control Category
CA-4 - Identification and Authentication of Devices	Device Management	Ensure devices connecting to systems are authenticated and authorized according to organizational policies, including endpoint security configurations and access controls.
CA-5 - Security Technical Implementation Guides	Configuration Management	Utilize formal security technical implementation guides (STIGs) or other technical standards to enforce consistent configuration settings across the organization's system landscape.
SC-11 - Network Security Planning	System Architecture Design and Implementation	Develop a network security plan that addresses secure design, segmentation, and monitoring of organizational networks.
SI-9 - System Development Life Cycle Methodology Selection	System Architecture Design and Implementation	Select an established system development life cycle methodology (e.g., Agile, Waterfall) to provide a structured approach for managing system development projects within the organization.
PR-5 - Automated Indicators of Compromise	Program Management	Implement automated systems or processes for detecting indicators of compromise (IOCs) across organizational networks and endpoints to facilitate rapid response to security incidents.
SC-12 - Network Configuration Monitoring	System Architecture Design and Implementation	Establish monitoring mechanisms to track changes in network configurations, including access control lists, routing tables, and firewall rules.
CA-6 - Access Enforcement	Identification and Authentication	Implement access enforcement controls at all system entry points, including firewalls, routers, and application gateways, to ensure adherence to the principle of least privilege (PoLP).
SC-13 - Network Segmentation Planning	System Architecture Design and Implementation	Develop a formal plan for network segmentation that addresses logical isolation and access controls between critical system components and sensitive data.
SI-10 - System Development Life Cycle Methodology Training	System Architecture Design and Implementation	Provide training to development teams on the selected system development life cycle methodology, ensuring consistent application across projects.

Control ID	Control Title	Control Category
PR-6 - Supply Chain Risk Management	Program Management	Implement a supply chain risk management process that evaluates potential risks associated with third-party vendors, software components, or services used within organizational systems.
CA-7 - Wireless Access Controls	Identification and Authentication	Establish access control measures for wireless network infrastructure to prevent unauthorized access, ensuring encryption and authentication mechanisms are in place.
SC-14 - Network Security Monitoring	System Architecture Design and Implementation	Implement ongoing monitoring of organizational networks to detect anomalous or malicious activities that may indicate a security incident.
SI-11 - System Development Life Cycle Methodology Adaptation	System Architecture Design and Implementation	Regularly review and adapt the selected system development life cycle methodology to accommodate new technologies, emerging threats, or organizational requirements.
PR-7 - Automated Vulnerability Scanning for Host Systems	Program Management	Implement automated vulnerability scanning of host systems within the organization's environment to identify potential security weaknesses and prioritize remediation efforts.
CA-8 - Media Protection Service	Device Management	Establish a media protection service that includes encryption, access controls, and secure disposal processes for removable/portable media used across the organization's system landscape.
SC-15 - Network Traffic Analysis	System Architecture Design and Implementation	Implement network traffic analysis capabilities to identify abnormal or malicious patterns within organizational network communications.
PR-8 - Third-Party Risk Management	Program Management	Establish a third-party risk management process that assesses the security posture of critical vendors, service providers, and software components used within organizational systems.
CA-9 - Remote Access Controls	Identification and Authentication	Implement controls to secure remote access mechanisms, including virtual private networks (VPNs), remote desktop protocols, or other forms of remote connectivity.

Control ID	Control Title	Control Category
SC-16 - Security Monitoring Planning	System Architecture Design and Implementation	Develop a security monitoring plan that addresses the organizational approach for collecting, analyzing, and acting upon security-related data from various sources across the system landscape.
SI-12 - System Development Life Cycle Methodology Review	System Architecture Design and Implementation	Periodically review the selected system development life cycle methodology to ensure continued relevance and alignment with organizational objectives, security standards, and emerging technologies.
PR-9 - Security Incident Response Plan Update	Program Management	Regularly update the security incident response plan to reflect lessons learned from past incidents, changes in threat landscape, or evolving organizational requirements.
CA-10 - Physical Access Controls	Identification and Authentication	Implement physical access control measures, including badge systems, biometric authentication, or mantrap facilities, to restrict unauthorized individuals' entry into critical system areas.
SC-17 - Security Monitoring for Virtualization and Cloud Services	System Architecture Design and Implementation	Establish security monitoring capabilities specifically tailored for virtualized environments and cloud services, ensuring consistent application of organizational security policies across diverse infrastructure types.
PR-10 - Automated Threat Intelligence Sharing	Program Management	Implement automated systems or processes for sharing threat intelligence with trusted partners, industry groups, or public repositories to enhance the overall security posture of organizational systems.
CA-11 - Media Protection Service for Virtual and Cloud Systems	Device Management	Extend media protection services to include virtualized environments and cloud services, ensuring encryption, access controls, and secure disposal processes are in place for digital artifacts stored or transmitted across these platforms.

Control ID	Control Title	Control Category
SC-18 - Security Monitoring for Third-Party Services	System Architecture Design and Implementation	Implement security monitoring capabilities specifically designed for third-party services and platforms integrated into the organization's system landscape to ensure ongoing compliance with service level agreements (SLAs) and security standards.
SI-13 - System Development Life Cycle Methodology Documentation	System Architecture Design and Implementation	Develop and maintain formal documentation of the selected system development life cycle methodology, including process workflows, templates, and training materials for organizational teams.
PR-11 - Automated Vulnerability Scanning for Host Systems in Virtual Environments	Program Management	Implement automated vulnerability scanning tailored to virtualized host systems within the organization's environment, ensuring comprehensive security assessment across diverse infrastructure types.
CA-12 - Mobile Device Security Controls	Identification and Authentication	Establish mobile device security controls, including encryption, remote wipe capabilities, and access control mechanisms, to protect sensitive data accessed or stored on mobile devices used within the organization's system landscape.
SC-19 - Data Center Network Segmentation	System Architecture Design and Implementation	Implement network segmentation strategies specifically tailored for data center environments, addressing logical isolation and access controls between critical systems and sensitive data.
PR-12 - Automated Security Orchestration and Response	Program Management	Implement automated security orchestration and response capabilities to streamline the detection, analysis, and remediation of security incidents across organizational systems and technologies.
SI-14 - System Development Life Cycle Methodology Training for Project Managers	System Architecture Design and Implementation	Provide training to project managers on the selected system development life cycle methodology, ensuring consistent application and understanding of methodologies across projects and teams.

Control ID	Control Title	Control Category
PR-13 - Automated Security Configuration Management	Program Management	Implement automated security configuration management processes that enforce organizational security policies and standards across diverse systems and environments, reducing manual errors and improving consistency.
CA-13 - Media Protection Service for Mobile Devices	Device Management	Establish a media protection service specifically designed for mobile devices used within the organization's system landscape, ensuring encryption, access controls, and secure disposal processes are in place for digital artifacts accessed or stored on these devices.
SC-20 - Security Monitoring for Cloud Services	System Architecture Design and Implementation	Implement security monitoring capabilities specifically tailored for cloud services and platforms integrated into the organization's system landscape, ensuring ongoing compliance with service level agreements (SLAs) and security standards.

Plain English Explanation of NIST Controls:

1. **AC-2: Encrypt Data in Transit**
   - Use encryption protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to protect data during transmission, ensuring sensitive information remains confidential and secure from unauthorized access.
2. **AC-5: Implement a Public Key Infrastructure (PKI)**
   - Establish a PKI framework that includes certificate authorities, registration authorities, and key management processes to securely manage digital certificates for identity verification, data encryption, and nonrepudiation in electronic transactions.
3. **AU-2: Control Nonpublic Facing Ports**
   - Implement access controls and firewall rules to restrict unauthorized access to nonpublic facing ports on systems and devices within the organization's network perimeter, ensuring only authorized traffic can traverse these communication channels.
4. **AU-5: Protect System Components from Unintended Modification**
   - Utilize file integrity monitoring tools, access controls, and configuration management practices to detect unauthorized changes to system components, software, and configurations, ensuring the security and stability of organizational systems.
5. **BM-3: Implement a Data Backup and Restore Plan**
   - Develop and maintain a comprehensive data backup plan that includes regular backups of critical data assets, secure storage, and a tested restore process to

minimize the impact of potential data loss or system failures on organizational operations.

6. **DM-5: Implement an Access Request and Approval Process**
   - Establish formal access request and approval processes for granting user access to systems, resources, and data within the organization's environment, ensuring proper authorization is provided based on job responsibilities and security clearance levels.
7. **IA-2: Maintain System Inventory and Documentation**
   - Track and document all hardware, software, firmware, and configuration settings within the organization's system landscape to ensure accurate asset management, facilitating efficient maintenance, upgrades, and incident response efforts.
8. **MP-10: Implement Automated Tools for Software Update Management**
   - Utilize automated tools and processes to manage software updates across organizational systems, ensuring timely installation of security patches, bug fixes, and feature enhancements while minimizing potential disruptions or errors in the update process.
9. **PM-4: Protect Against Unauthorized Data Transfer**
   - Implement access controls, network segmentation, and monitoring mechanisms to prevent unauthorized data transfer within the organization's system landscape, safeguarding sensitive information from potential exfiltration attempts by malicious actors or insider threats.
10. **RA-5: Perform Regular System Vulnerability Scans**
    - Conduct regular vulnerability assessments of organizational systems and applications using automated scanning tools to identify potential weaknesses in security configurations, software versions, or patch levels, enabling proactive remediation efforts to address identified vulnerabilities.

These plain English explanations provide practical guidance for implementing the respective NIST security controls, facilitating a clear understanding of the necessary actions to achieve compliance and enhance organizational cybersecurity posture.

Revision #4
Created 23 April 2025 16:56:49 by CGChambers
Updated 23 April 2025 17:57:48 by CGChambers