MEP CENTER
THE UNIVERSITY OF UTAH

Compliance to NIST SP 800-171 - Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations

GAP Analysis Tool

How to use this tool: This worksheet covers all 14 families and 110 points of the NIST SP 800-171 Standard. The first column Identifies the control number related to the security family (second number 1-14) and the second column list the specific control found in the standard. The middle column is a question or statement based on the security control statement from the standard. Some of the questions are "requirements" related to earlier questions in the same security family. The last three columns help determine the status of a company's CUI security plan. Completing this worksheet will help identify areas needing attention. This worksheet should be completed by the senior manager responsible for compliance with NIST SP 800-171. Other personnel may include senior management and IT management, both in-house and out sourced. This tool should only be used to identify gaps in a security plan. It does not take the place of actual standard operating procedures or policies.

NIST SP 800-171 Control Number	Control Name	Control Description	Fully Implemented Policy with Written SOP	In Process	Not Started
3.1 ACCESS CONTROL *Basic Security Requirements*					
AC 3.1.1	Account Management	Does the organization limit information system access to authorized users, or devices (including other information systems)?			

AC 3.1.2	Access Enforcement	Does the organization limit information system access to the types of transactions and functions that authorized users are permitted to			
Derived Security Requirements					
AC 3.1.3	Information Flow Enforcement	Is the control of the flow of CUI in accordance with approved authorizations as listed in the above policy?			
AC 3.1.4	Separation of Duties	Are the duties of individuals separated to reduce the risk of malevolent activity without collusion?			
AC 3.1.5	Least Privilege	Does the organization employ the principle of least privilege, including for specific security functions and privileged accounts?			
AC 3.1.6	Least Privilege	Does the organization use non-privileged accounts or roles when accessing non-security functions?			
AC 3.1.7	Least Privilege	Is there a system or policy in place to prevent non-privileged users from executing privileged functions and audit the execution of such functions?			
AC 3.1.8	Unsuccessful Logon Attempts	Does the system limit the number of unsuccessful logon attempts?			

AC 3.1.9	System Use Notification	Does the system provide privacy and security notices consistent with applicable CUI rules?			
AC 3.1.10	Session Lock	Does the organization's system lock/time-out with pattern-hiding displays to prevent access/viewing of data after period of inactivity?			
AC 3.1.11	Session Termination	Does the system terminate (automatically end) a user session after a defined condition?			
AC 3.1.12	Remote Access	Are there safeguards in place to monitor and control remote access sessions?			
AC 3.1.13	Remote Access	Does the system employ cryptographic mechanisms to protect the confidentiality of remote access sessions?			
AC 3.1.14	Remote Access	Are remote access sessions routed via managed access control points?			
AC 3.1.15	Remote Access	Does the system authorize remote execution of privileged commands and remote access to security-relevant information?			
AC 3.1.16	Wireless Access	Does the system employ an authorization/verification for wireless access prior to allowing such connections?			

AC 3.1.17	Wireless Access	Does wireless access employ authentication and encryption tools?			
AC 3.1.18	Access Control for Mobile Devices	Does the organization control connection of mobile devices to systems?			
AC 3.1.19	Access Control for Mobile Devices	Does the organization ensure the encryption of CUI on mobile devices?			
AC 3.1.20	Use of External Information Systems	Does the organization verify and control/limit connections to and use of external information systems?			
AC 3.1.21	Use of External Information Systems	Does the organization control and/or limit the use of organizational portable storage devices on external information systems?			
AC 3.1.22	Publically Accessible Content	Does the company control and monitor the information posted or processed on publicly accessible information systems?			
3.2 AWARENESS AND TRAINING *Basic Security Requirements*					
AT 3.2.1	Security Awareness Training	Are the managers, systems administrators, and users of organizational information systems made aware of the security risks associated with their activities and of the applicable			

AT 3.2.2	Role-Based Security Training	Are the organizational personnel adequately trained to carry out their assigned information security-related duties and responsibilities?			
Derived Security Requirements					
AT 3.2.3	Security Awareness Training	Does the organization provide security awareness training on recognizing and reporting potential indicators of insider threat?			
3.3 AUDIT AND ACCOUNTABILITY *Basic Security Requirements*					
AU 3.3.1	Audit Events	Does the organization have a way to create, protect, and retain information system audit records to the extent needed to enable the monitoring,			
AU 3.3.2	Audit Generation	Are systems and records in place to ensure that the actions of individual information system users can be uniquely traced to those users so they			
Derived Security Requirements					
AU 3.3.3	Audit Events	Review and update audited events.			
AU 3.3.4	Response to Audit Processing Failure	Alert in the event of an audit process failure.			
AU 3.3.5	Audit Review, Analysis, and Reporting	Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate,			

AU 3.3.6	Audit Redaction and Report Generation	Provide audit reduction and report generation to support on-demand analysis and reporting.			
AU 3.3.7	Time Stamps	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit			
AU 3.3.8	Protection of Audit Information	Protect audit information and audit tools from unauthorized access, modification, and deletion.			
AU 3.3.9	Protection of Audit Information	Limit management of audit functionality to a subset of privileged users.			
3.4 CONFIGURATION MANAGEMENT					
Basic Security Requirements					
CM 3.4.1	Baseline Configuration	Does the organization maintain an established baseline configurations and inventories of organizational information systems (including hardware, software,			
CM 3.4.2	Configuration Settings	Is there an established and enforced security configuration settings for information technology products employed in organizational information			
Derived Security Requirements					
CM 3.4.3	Configuration Change Control	Establish and enforce security configuration settings for information technology products employed in organizational information systems.			

CM 3.4.4	Security Impact Analysis	Analyze the security impact of changes prior to implementation.			
CM 3.4.5	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.			
CM 3.4.6	Least Functionality	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.			
CM 3.4.7	Least Functionality	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.			
CM 3.4.8	Least Functionality	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow			
CM 3.4.9	User-Installed Software	Control and monitor user-installed software.			
3.5 IDENTIFICATION AND AUTHENTICATION *Basic Security Requirements*					
IA 3.5.1	Identification and Authentication	Does the organization identify information system users, processes acting on behalf of users, or devices?			

IA 3.5.2	Authenticator Management	Does the system authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information			
Derived Security Requirements					
IA 3.5.3	Identification and Authentication	Is multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts employed?			
IA 3.5.4	Identifier Management	Is replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts employed?			
IA 3.5.5	Identifier Management	Does the system prevent reuse of identifiers for a defined period?			
IA 3.5.6	Identifier Management	Does the system disable identifiers after a defined period of inactivity?			
IA 3.5.7	Authenticator Management	Does the system enforce a minimum password complexity and change of characters when new passwords are created?			
IA 3.5.8	Authenticator Management	Does the system prohibit password reuse for a specified number of generations?			

IA 3.5.9	Authenticator Management	Does the system allow temporary password use for system logons with an immediate change to a permanent password?			
IA 3.5.10	Authenticator Management	Store and transmit only encrypted representation of passwords.			
IA 3.5.11	Authenticator Feedback	Obscure feedback of authentication information.			
3.6 INCIDENT RESPONSE *Basic Security Requirements*					
IR 3.6.1	Incident Response Training	Has the organization establish an operational incident-handling capability for organizational information systems that includes adequate preparation,			
IR 3.6.2	Incident Handling	Is there a policy maintained to track, document, and report incidents to appropriate officials and/or authorities both internal and external to the			
Derived Security Requirements					
IR 3.6.3	Incident Response Testing	Test the organizational incident response capability.			
3.7 MAINTENANCE *Basic Security Requirements*					

MA 3.7.1	Controlled Maintenance	Does the organization perform proper maintenance on organizational information systems?			
MA 3.7.2	Maintenance Tools	Does the organization provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance?			
Derived Security Requirements					
MA 3.7.3	Controlled Maintenance	Ensure equipment removed for off-site maintenance is sanitized of any CUI.			
MA 3.7.4	Maintenance Tools	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.			
MA 3.7.5	Nonlocal Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when			
MA 3.7.6	Maintenance Personnel	Supervise the maintenance activities of maintenance personnel without required access authorization.			
3.8 MEDIA PROTECTION *Basic Security Requirements*					
MP 3.8.1	Media Access	Does the organization protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital?			

MP 3.8.2	Media Storage	Is access to CUI on information system media limited to authorized users?			
MP 3.8.3	Media Sanitization	Does the organization sanitize or destroy information system media containing CUI before disposal or release for reuse?			
Derived Security Requirements					
MP 3.8.4	Media Marking	Mark media with necessary - CUI markings and distribution limitations.			
MP 3.8.5	Media Transport	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.			
MP 3.8.6	Media Transport	Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless			
MP 3.8.7	Media Use	Control the use of removable media on information system components.			
MP 3.8.8	Media Use	Prohibit the use of portable storage devices when such devices have no identifiable owner.			

MP 3.8.9	Information System Backup	Protect the confidentiality of backup CUI at storage locations.			
3.9 PERSONNEL SECURITY *Basic Security Requirements*					
PS 3.9.1	Personnel Screening	Are individuals screened prior to authorizing access to information systems containing CUI?			
PS 3.9.2	Personnel Termination/Transfer	Does the organization ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and			
3.10 PHYSICAL PROTECTION *Basic Security Requirements*					
PE 3.10.1	Physical Access Authorizations	Does the organization limit physical access to organizational information systems, equipment, and the respective operating environments to authorized			
PE 3.10.2	Monitoring Physical Access	Does the organization protect and monitor the physical facility and support infrastructure for those information systems?			
Derived Security Requirements					
PE 3.10.3	Physical Access Control	Are there policies outlining the escorting and monitoring of visitors and visitor activity?			

PE 3.10.4	Physical Access Control	Does the organization maintain audit logs of physical access (visitor sign-in)?			
PE 3.10.5	Physical Access Control	Does the organization control and manage physical access devices?			
PE 3.10.6	Alternate Work Site	Does the organization enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites)?			
3.11 RISK ASSESSMENT *Basic Security Requirements*					
RA 3.11.1	Risk Assessment	Are periodic risk assessments conducted to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals,			
Derived Security Requirements					
RA 3.11.2	Vulnerability Scanning	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.			
RA 3.11.3	Vulnerability Scanning	Remediate vulnerabilities in accordance with assessments of risk.			
3.12 SECURITY ASSESSMENT *Basic Security Requirements*					

CA 3.12.1	Security Assessments	Are periodic security assessments conducted of the controls in organizational information systems to determine if the controls are effective in			
CA 3.12.2	Plan of Action and Milestones	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.			
CA 3.12.3	Continuous Monitoring	Are policies in place to monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls?			
3.13 SYSTEM AND COMMUNICATIONS PROTECTION					
Basic Security Requirements					
SC 3.13.1	Boundary Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at			
SC 3.13.2	Security Engineering Principles	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within			
Derived Security Requirements					
SC 3.13.3	Application Partitioning	Separate user functionality from information system management functionality (e.g., privileged user functions).			
SC 3.13.4	Information in Shared Resources	Prevent unauthorized and unintended information transfer via shared system resources.			

SC 3.13.5	Boundary Protection	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.			
SC 3.13.6	Boundary Protection	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).			
SC 3.13.7	Boundary Protection	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other			
SC 3.13.8	Transmission and Confidentiality and Integrity	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical			
SC 3.13.9	Network Disconnect	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.			
SC 3.13.10	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys for cryptography employed in the information system.			
SC 3.13.11	Cryptographic Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.			
SC 3.13.12	Collaborative Computing Devices	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.			

SC 3.13.13	Mobile Code	Control and monitor the use of mobile code.			
SC 3.13.14	Voice over Internet Protocol	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.			
SC 3.13.15	Session Authenticity	Protect the authenticity of communications sessions.			
SC 3.13.16	Protection of Information at Rest	Protect the confidentiality of CUI at rest.			
3.14 SYSTEM AND INFORMATION INTEGRITY *Basic Security Requirements*					
SI 3.14.1	Flaw Remediation	Do the responsible individuals identify, report, and correct information and information system flaws in a timely manner?			
SI 3.14.2	Flaw Remediation	Does the organization provide protection from malicious code at appropriate locations within organizational information systems?			
SI 3.14.3	Security Alerts, Advisories, and Directives	Monitor information system security alerts and advisories and take appropriate actions in response.			
Derived Security Requirements					

SI 3.14.4	Malicious Code Protection	Are policies and schedules in place to update malicious code protection mechanisms when new releases are available?			
Si 3.14.5	Malicious Code Protection	Are periodic scans performed of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed?			
SI 3.14.6	Information System Monitoring	Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.			
SI 3.14.7	Information System Monitoring	Identify unauthorized use of the information system.			