NIST 800-53 Requirements

The NIST 800-53 is a catalog of control guidelines developed to heighten the security of information systems within the federal government. These controls are used by information systems to maintain the integrity, confidentiality, and security of federal information systems that store, process, or transmit federal information.

The NIST guidelines consider a multi-facet approach to risk management through control compliance. SP 800-53 focuses on the controls which can be used along with SP 800-37 (Risk Management Framework for Information Systems and Organizations) for a comprehensive approach to information security and risk mitigation.

The controls are broken into three classes based on impact – low, moderate, and high – and are divided into 18 different security control families.

AC	Access Control
AT	Awareness Training
AU	Audit & Accountability
CA	Security Assessment & Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification & Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PS	Personnel Security
PE	Physical & Environmental Protection
PL	Planning
PM	Program Management
RA	Risk Assessment
SA	System & Services Acquisition
SC	System & Communications Protection
SI	System & Information Integrity

NIST 800-53 Objective

The ultimate objective of 800-53 is to make the information systems we depend on more resistant to penetration and attack, limit the damage from cyber-attacks when they happen, and make the systems resilient as security threats continue to evolve.

How does this impact my Agency?

Each federal agency is responsible for implementing the minimum-security requirements outlined by NIST. Agency's' compliance levels are scored periodically, and poor performance numbers can result in penalties and reflect poorly on the agency's management team and staff.

Where to start and why?

The security requirements outlined in 800-53 are very mature and describe over 800 controls across the 18 security categories which helps define what needs to be accomplished. However, it lacks any prescriptive detail of how to accomplish compliance success and what should be the priority of those requirements.

Find out which specific NIST 800-53 requirements you can address with Netwrix solutions

Netwrix solutions place emphasis on Configuration Management Policy and Procedures and Information Integrity where:

- Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components such as kernels, drivers), middleware, and applications.
- State-of-the-art integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.
- The solution uses automated mechanisms to maintain an up-to-date, complete, accurate and readily available baseline configuration data of the information system.

Netwrix Change Tracker uses a continuous monitoring approach to provide integrity verification in real-time, providing audit trail evidence and alerts in line with NIST 800-53.

NIST 800-53	Purpose	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
AC-2 Account Management AC-3 Access Enforcement AC-4 Information Flow Enforcement AC-6 Least Privilege AC-7 Unsuccessful Logon Attempts AC-8 System Use Notification AC-9 Previous Logon (access) Notification AC-11 Session Lock AC-12 Session Termination AC-17 Remote Access AC-18 Wireless Access	AC-7 Enforces a limit of consecutive invalid logon attempts by a user during a defined time period and automatically locks the account/node for a defined time period when the maximum number of unsuccessful attempts is exceeded AC-2 Account Monitoring	✓		✓
AU-2 Audit Events AU-3 Content Of Audit Records AU-4 Audit Log Storage AU-5 Response To Logging Failures AU-6 Audit Record Analysis AU-7 Audit Record Reduction AU-8 Time Stamps AU-9 Protection Of Audit Information AU-10 Non-Repudiation AU-11 Audit Record Retention AU-16 Cross-Organization Logging	Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage	✓		✓
CA-2 Security Assessments CA-7 Continuous Monitoring	Ensure that information security is built into organizational information systems; identify weaknesses and deficiencies early in the development process; and ensure compliance to vulnerability mitigation procedures. The term continuous implies that organizations assess security controls and risks at a frequency sufficient to support organizational risk-based decisions	✓	✓	✓

NIST 800-53	Purpose	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
CM-2 Baseline Configuration CM-3 Configuration Change Control CM-4 Security Impact Analysis CM-5 Access Restrictions For Signed Components CM-6 Configuration Settings CM-7 Least Functionality CM-8 Information System Component Inventory CM-10 Software Usage Restrictions CM-11 User-Installed Software	Baseline configurations serve as a basis for future builds, releases, and changes to information systems. Baseline configurations include information about system components (e.g., standard software packages installed; current version numbers and patch information and configuration settings/parameters). Maintaining baseline configurations requires new baselines as information systems change over time.	✓	✓	
IA-2 Identification and Authentication IA-5 Password-Based Authentication	Organizations may choose to establish certain rules for password generation. Uniquely identify users and associate that unique identification with processes acting on behalf of those users.	✓		✓
IR-4 Incident Handling	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	✓		✓
MA-2 Controlled Maintenance MA-3 Updates and Patches MA-4 Logging and Review	Employ automated mechanisms to schedule, conduct, and document maintenance/repairs; and produce up-to date, accurate, and complete records of all actions.	✓	✓	✓

NIST 800-53	Purpose	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
MP-2 Media Access MP-4 Restricted Access	Information system media includes digital media. Restricting access to media includes limiting access to design specifications stored on compact disks in the media library to the project leader and the development team. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used.	✓		✓
PE-3 Physical Access Control PE-6 Monitoring Physical Access	Physical access control applies to employees and visitors. Physical access devices include keys, locks, combinations, and card readers. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof			✓
PM-5 System Inventory PM-31 Continuous Monitoring Strategy	Maintain an inventory of all systems and applications that process personally identifiable information.	✓	✓	✓
RA-5 Vulnerability Scanning RA-10 Threat Hunting	Vulnerability scanning includes, scanning for patch levels, scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. Review historic audit logs to determine if a vulnerability identified has been previously exploited.	✓	✓	✓

NIST 800-53	Purpose	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
SA-4 Development Methods SA-5 System Documentation SA-8 Security Engineering Principles SA-9 Identification of Open Ports SA-10 Developer Configuration Management SA-11 Developer Penetration Testing SA-15 Attack Surface Reduction	Maintaining the integrity of changes to the information system, component, or service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Attack surface reduction includes implementing layered defenses; applying the principles of least privilege/least functionality; reducing entry points available to unauthorized users; reducing the amount of code executing; and eliminating application programming interfaces (APIs) vulnerable to attack.	✓	✓	✓
SC-7 Boundary Protection SC-8 Transmission Confidentiality and Integrity SC-10 Network Disconnect SC-13 Cryptographic Protection SC-23 Session Authenticity SC-34 Integrity Of Read-Only Media SC-45 System Time Synchronization SC-51 OT and IOT Technologies	Restricting interfaces within organizational information systems includes, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Cryptographic mechanisms implemented to protect information integrity include cryptographic hash functions.	✓	✓	✓
SI-2 Flaw Remediation SI-3 Malicious Code Protection SI-4 Information System Monitoring SI-6 Security Verification SI-7 Software, Firmware, And Information Integrity SI-12 Information Management SI-16 Memory Protection	Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems, including kernels and drivers, middleware, and applications. Firmware includes the BIOS. Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms e.g. cryptographic hashes and associated tools can automatically monitor the integrity of information systems and applications.	✓	✓	✓

NIST 800-53	Purpose	Product		
		Change Tracker	Greenbone Enterprise	Log Tracker
SR-5 Assessment Prior To Acceptance Or Update SR-11 Anti-Counterfeit Scanning	Organizational personnel or independent, external entities conduct assessments of systems, components, products, tools, and services to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of non-compliance with supply chain controls. These include malicious code, malicious processes, defective software, backdoors, and counterfeits.		✓	

About Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

Learn More - Check out more information about Change Tracker: netwrix.com/integrity

Live demo — Take a product tour with a Netwrix expert: netwrix.com/integrity

Request quote — Receive pricing information: netwrix.com/integrity

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social