



Resource  
Guide

## **nCircle Solutions for NIST Special Publication 800-53 Revision 3**

## Introduction

nCircle is the leader in automated security and compliance auditing, helping over 4,500 enterprises and government organizations worldwide achieve their security and compliance objectives. nCircle Suite360™ delivers the industry's most comprehensive IT audit capabilities in a single product line. No other solution can audit all networked assets, including their configurations, applications, vulnerabilities, and file integrity—with over 33,000 conditions—in a fully integrated product line.

The National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 3, Recommended Security Controls for Federal Information Systems, provides a unified security framework intended to help U.S. federal government organizations achieve more secure information systems. These guidelines are the most prescriptive and comprehensive set of information security guidelines to date and they form the foundation for many successful enterprise security programs in government organizations.

This resource guide provides a mapping of nCircle functional capabilities to the requirements of the NIST 800-53 controls with brief commentary.

| NIST SP 800-53 Controls |                             | Control Description  | nCircle Coverage   |
|-------------------------|-----------------------------|--|--|
| <b>Access Control</b>   |                             |  |  |
| AC-2                    | Account Management          | The organization manages information system accounts in order to identify authorized users and specify access privileges.  | nCircle audits systems for current and new users as well as user modifications or deletions.   |
| AC-3                    | Access Enforcement          | The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.   | nCircle provides policies for role-based and identity-based access controls and access enforcement mechanisms and monitors systems to identify deviations from policy. |
| AC-5                    | Separation of Duties        | The information system enforces separation of duties through assigned information system access authorizations.  | nCircle audits user accounts, roles, groups and access controls to ensure appropriate controls exist related to separation of duties.                                  |
| AC-6                    | Least Privilege             | The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.                             | nCircle audits system settings to determine if controls are in place to enforce least privilege access.  |
| AC-7                    | Unsuccessful Login Attempts | The information system enforces a limit of consecutive invalid access attempts by a user during a time period and automatically locks the account/node until released by an administrator; delays next login prompt according to when the maximum number of unsuccessful attempts is exceeded. | nCircle audits systems and registry settings to ensure appropriate rules and controls exist relating to login attempts.  |
| AC-8                    | System Use Notification     | The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.   | nCircle can audit systems to ensure this banner exists and monitor for any changes in the content.   |
| AC-10                   | Concurrent Session Control  | The information system limits the number of concurrent sessions for each system account to a designated number.  | nCircle can audit and monitor system settings to ensure this control remains in effect.  |



| NIST SP 800-53 Controls         |  | Control Description   | nCircle Coverage   |
|---------------------------------|--|---|--|
| <b>Access Control Continued</b> |  |   |  |
| AC-11                           | Session Lock   | The information system prevents further access to the system by initiating a session lock after a designated period of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.   | nCircle can detect system settings including screen-saver settings to ensure that screen savers lock system after a specific period of inactivity.   |
| AC-14                           | Permitted Actions without Identification or Authentication | The organization identifies specific user actions that can be performed on the information system without identification or authentication.   | nCircle can audit systems to determine user role and responsibility settings and can then compare the findings to the company policy regarding permitted actions.  |
| AC-17                           | Remote Access  | The organization documents allowed methods of remote access to the information system, establishes usage restrictions and implementation guidance for each allowed remote access method, monitors for unauthorized remote access to the information system, authorizes remote access to the information system prior to connection and enforces requirements for remote connections to the information system.  | nCircle can audit system settings to ensure that remote access controls are in effect and configured according to policy.  |
| AC-18                           | Wireless Access  | The organization establishes usage restrictions and implementation guidance for wireless access, monitors for unauthorized wireless access to the information system, authorizes wireless access to the information system prior to connection and enforces requirements for wireless connections to the information system.  | nCircle can audit systems to determine the configuration and settings of wireless access capabilities and ensure the proper configuration is in effect.  |
| <b>Audit and Accountability</b> |  |   |  |
| AU-2                            | Auditable Events   | The organization determines auditable events and utilizes systems to audit those events.  | nCircle audits the entire IT infrastructure for security and compliance status and provides an indelible audit trail of findings.  |
| AU-3                            | Content of Audit Records                                   | The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.   | nCircle audits the entire IT infrastructure for security status and configurations and provides an indelible audit trail of findings. nCircle identifies vulnerabilities, configuration changes and deviations from policies, including who made the changes, what changes were made, when the changes were made, and how the changes were made. |
| AU-4                            | Audit Storage Capacity                                     | The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.  | nCircle can monitor storage capacity and usage on systems that retain audit data and alert administrators when capacity reaches a set threshold.   |
| AU-5                            | Response to Audit Processing Failures                      | The information system alerts designated organizational officials in the event of an audit processing failure and takes additional action such as shutting down information systems, overwriting oldest audit records and ceasing audit generation.   | nCircle can alert on audit failures and alert on audit system disk usage thresholds.   |
| AU-6                            | Audit Review, Analysis, and Reporting                      | The organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity, and reports findings to designated organizational officials and adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. | nCircle aggregates vulnerability and configuration audit data in a central repository, the nCircle Suite360 Intelligence Hub. nCircle can also automatically export audit data to SIM/SEIM or other aggregation system. nCircle also provides a real time query engine for instant audit data analysis.  |



| NIST SP 800-53 Controls                      |                                       | Control Description   | nCircle Coverage  |
|--|---------------------------------------|---|---|
| <b>Audit and Accountability Continued</b>    |                                       |   |   |
| AU-7   | Audit Reduction and Report Generation | The information system provides an audit reduction and report generation capability.  | nCircle's real time query engine for instant audit data analysis, nCircle Focus™, enables administrators to easily analyze audit records based on selectable event criteria as specified in AU-7 Control Enhancements.  |
| AU-8   | Time Stamps                           | The information system uses internal system clocks to generate time stamps for audit records.   | nCircle provides timestamps for all instances of discovered vulnerabilities and configuration or monitored file changes.  |
| AU-9   | Protection of Audit Information       | The information system protects audit information and audit tools from unauthorized access, modification, and deletion.   | nCircle encrypts the entire data stream between the user's web browser, the management server and the audit scanner to protect against tampering.   |
| AU-11  | Audit Record Retention                | The organization retains audit records for to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. | nCircle audit data retention parameters can be configured by the user to ensure availability for investigation of security incidents and information retention requirements.  |
| <b>Security Assessment and Authorization</b> |                                       |   |   |
| CA-2   | Security Assessments                  | The organization develops a security assessment plan, assesses the security controls of the network and provides a security assessment report.  | nCircle solutions provide assurance that the network is secure from a vulnerability perspective, systems are in compliance with applicable policies and there are no unapproved changes to critical files.  |
| CA-7   | Continuous Monitoring                 | The organization establishes a continuous monitoring strategy and implements a continuous monitoring program.   | nCircle monitors system configurations and alerts on changes as per policy. nCircle also includes a risk rating of changes, providing insight into the security impact of the changes.  |
| <b>Configuration Management</b>              |                                       |   |   |
| CM-2   | Baseline Configuration                | The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.  | nCircle enables administrators to define a "gold standard" system configuration based on the operating system, applications and configuration status of a host that complies with control objectives. All similar systems may then be continuously measured against the gold standard to ensure compliance. Deviations from the gold standard caused because of the presence of an unauthorized application or outdated operating system can be efficiently identified and addressed based on the system's prioritized risk score determining its importance to the agency.<br><br>nCircle can also send alerts when systems deviate from the baseline configuration. |
| CM-3   | Configuration Change Control          | The organization determines the types of changes to be configuration controlled and approves, documents and audits changes.   | nCircle audits the configurations of all systems and identifies any changes. Reports and alerts can be used to notify administrators of any unapproved changes with remediation steps.  |
| CM-4   | Security Impact Analysis              | The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.   | nCircle audits system configurations, noting any changes and providing a security risk analysis of each change.   |
| CM-5   | Access Restrictions for Change        | The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.   | nCircle identifies changes to software on target assets and alerts and reports on those changes.  |



| NIST SP 800-53 Controls                   |  | Control Description  | nCircle Coverage   |
|---|--|--|--|
| <b>Configuration Management Continued</b> |  |  |  |
| CM-6                                      | Configuration Settings                   | The organization establishes, documents, implements and monitors mandatory configuration settings for IT products.   | nCircle provides several built-in configuration policies for various operating systems and applications which can be modified to suit the organization. nCircle can then monitor assets to identify any configuration changes. |
| CM-7                                      | Least Functionality                      | The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of unapproved functions, ports, protocols, and/or services.  | nCircle audits the configurations of assets, identifies changes and alerts and reports on those changes.   |
| CM-8                                      | Information System Component Inventory   | The organization develops, documents, and maintains an inventory of information system components.   | nCircle discovers all hosts, applications, services, configurations and vulnerabilities, providing a comprehensive system inventory.   |
| <b>Contingency Planning</b>               |  |  |  |
| CP-9                                      | Information System Backup                | The organization conducts backups of user- and system-level information and protects the confidentiality and integrity of the backup information.  | nCircle can monitor the backup files for proper permissions and security settings and keep an audit log of changes and who accessed or changed the files.  |
| <b>Identification and Authentication</b>  |  |  |  |
| IA-2                                      | User Identification and Authentication   | The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).   | nCircle audits systems to ensure identification and authentication mechanisms are configured according to policy.  |
| IA-3                                      | Device Identification and Authentication | The information system uniquely identifies and authenticates before establishing a connection.   | nCircle audits systems to ensure identification and authentication mechanisms are configured according to policy.  |
| IA-5                                      | Authenticator Management                 | The organization manages information system authenticators for users and devices by verifying identities, ensuring identifiers have sufficient strength of mechanism, changing default content of authenticators, establishing minimum and maximum lifetime restrictions and reuse conditions, etc.  | nCircle audits systems to ensure that authentication mechanisms meet policy as specified in the control.   |
| IA-7                                      | Cryptographic Module Authentication      | The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.   | nCircle solutions use FIPS 140-2-compliant cryptographic libraries for device and user communication and audits systems to ensure appropriate cryptographic modules are in use.  |
| <b>Incident Response</b>                  |  |  |  |
| IR-4                                      | Incident Handling                        | The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery, coordinates incident handling activities with contingency planning activities and incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. | nCircle provides an audit trail to assist with, among other things, incident handling and recovery.  |
| IR-5                                      | Incident Monitoring                      | The organization tracks and documents information system security incidents.   | nCircle provides an audit trail for vulnerabilities and configuration changes to assist with incident monitoring.  |



| NIST SP 800-53 Controls                |                             | Control Description  | nCircle Coverage  |
|--|-----------------------------|--|---|
| <b>Maintenance</b>                     |                             |  |   |
| MA-3                                   | Maintenance Tools           | The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.   | nCircle audits systems to ensure that maintenance tool installation follows acceptable policy.  |
| MA-4                                   | Non-Local Maintenance       | The organization authorizes, monitors and controls non-local maintenance and diagnostic activities.  | nCircle audits systems to ensure that remote access capabilities are configured as per policy.  |
| <b>Risk Assessment</b>                 |                             |  |   |
| RA-2                                   | Security Categorization     | The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.  | nCircle provides automated asset value assignment, custom asset grouping and support for FIPS-199 sensitivity categorizations. These features greatly simplify the asset grouping and reporting requirements of RA-2.   |
| RA-3                                   | Risk Assessment             | The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, documents and reviews results and updates the assessment as needed.   | nCircle performs vulnerability- and configuration-based risk assessments on the network assets and provides suggested remediations, reports and other assistance. nCircle also provides objective risk metrics and trending to track risk over time.  |
| RA-5                                   | Vulnerability Scanning      | The organization scans for vulnerabilities in the information system and hosted applications and employs vulnerability scanning tools that promote interoperability among tools to automate parts of the vulnerability management process by using standards for enumerating platforms, flaws and improper configurations, formatting checklists and test procedures and measuring vulnerability impact. The organization analyzes vulnerability scan reports, remediates vulnerabilities and shares vulnerability information with designated personnel to help eliminate similar vulnerabilities in other systems. | nCircle continuously and periodically gathers detailed intelligence about the endpoint devices on the network, and utilizes best-in-class reporting and analytics to prioritize vulnerabilities, including spyware and trojan software, and provide a comprehensive view of network risk. Scans can be run continuously or on a scheduled basis. The profile results and reports generated provide information to demonstrate whether systems were reviewed for known vulnerabilities and software patched promptly installed. With nCircle's IP360™ Dynamic Host Tracking, users can reliably identify, track, and audit hosts and their associated IP assignments over time, even as the network changes. This ensures a consistent and manageable approach that requires accurate, long-term trending of systems and the associated security audit data. nCircle uses granular role-based access controls in order to share information across the organization with the appropriate audiences from IT admins to executives. |
| <b>System and Services Acquisition</b> |                             |  |   |
| SA-3                                   | Life Cycle Support          | The organization manages the information system using a system development life cycle methodology that includes information security considerations, defines and documents information system security roles and responsibilities throughout the system development life cycle and identifies individuals having information system security roles and responsibilities.   | nCircle supports the system development lifecycle through asset discovery, vulnerability assessments with remediation guidance, trouble ticketing, remediation confirmation scans, and configuration audits. nCircle also supports granular role-based access control to easily map to the organization's roles and responsibilities.   |
| SA-6                                   | Software Usage Restrictions | The organization uses software and associated documentation in accordance with contract agreements and copyright laws, employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution and controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.   | nCircle identifies all IP-enabled assets on the network as well as any installed applications, enabling administrators to easily determine what applications are actually installed in order to ensure compliance with software licenses. nCircle can also identify peer-to-peer file sharing systems on the assets.  |



| NIST SP 800-53 Controls                          |  | Control Description  | nCircle Coverage   |
|--|--|--|--|
| <b>System and Services Acquisition Continued</b> |  |  |  |
| SA-7   | User Installed Software                | The organization enforces explicit rules governing the installation of software by users.  | nCircle can identify applications installed on assets and ensure their installation complies with policy. In the event of a policy violation, alerts can be generated to notify administrators.  |
| SA-9   | External Information Security Services | The organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; defines and documents government oversight and user roles and responsibilities with regard to external information system services; and monitors security control compliance by external service providers. | nCircle provides cloud-based and mobile scanning capabilities to enable the organization to assess the security of external information system services as needed.   |
| SA-10  | Developer Configuration Management     | The organization requires that information system developers/integrators perform configuration management during information system design, development, implementation, and operation, manage and control changes to the information system, implement only organization-approved changes, document approved changes to the information system and track security flaws and flaw resolution.  | nCircle solutions are suitable for use in the design, development, implementation and operation of information systems and can be utilized for configuration auditing and configuration policy compliance as well as vulnerability assessment. |
| SA-11  | Developer Security Testing             | The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers) create and implement a security test and evaluation plan, implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process and document the results of the security testing/evaluation and flaw remediation processes.   | nCircle solutions can be used to create baseline configurations for systems to ensure that systems remain in compliance throughout the development and testing process.  |
| SA-12  | Supply Chain Protection                | The organization protects against supply chain threats by employing appropriate measures as part of a comprehensive, defense-in-breadth information security strategy.   | nCircle solutions can be used to audit the supply chain to ensure security.  |
| <b>System and Communications Protection</b>      |  |  |  |
| SC-5   | Denial of Service Protection           | The information system protects against or limits the effects of denial of service attacks.  | nCircle audits the configurations and vulnerabilities of systems on the network to minimize the possibility of a denial of service.  |
| SC-7   | Boundary Protection                    | The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system and connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.  | nCircle can verify that routing rules are configured per policy and alert on any deviations.   |
| SC-8   | Transmission Integrity                 | The information system protects the integrity of transmitted information.  | nCircle can audit assets to ensure appropriate encryption controls are in place.   |
| SC-9   | Transmission Confidentiality           | The information system protects the confidentiality of transmitted information.  | nCircle can audit assets to ensure appropriate encryption controls are in place.   |



| NIST SP 800-53 Controls                               |  | Control Description  | nCircle Coverage  |
|---|--|--|---|
| <b>System and Communications Protection Continued</b> |  |  |   |
| SC-10   | Network Disconnect                             | The information system terminates the network connection associated with a communications session at the end of the session or after a defined period of inactivity.   | nCircle can audit asset configurations to ensure client disconnect settings meet organizational policy.   |
| SC-11   | Trusted Path                                   | The information system establishes a trusted communications path between the user and defined security functions of the system.  | nCircle can detect if applications are not using pre-determined ports or the appropriate level of encryption during transmission.   |
| SC-12   | Cryptographic Key Establishment and Management | The organization establishes and manages cryptographic keys for required cryptography employed within the information system.  | nCircle can identify weak encryption algorithms and expired SSL certificates as well as whether the level of encryption meets federal standards.  |
| SC-13   | Use of Cryptography                            | The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.   | nCircle can identify weak encryption algorithms and expired SSL certificates as well as whether the level of encryption meets federal standards.  |
| SC-15   | Collaborative Computing                        | The information system prohibits remote activation of collaborative computing devices and provides an explicit indication of use to users physically present at the devices.   | nCircle can audit assets to ensure that configurations meet policy and prohibit remote activation of collaborative computing devices.   |
| SC-23   | Session Authenticity                           | The information system provides mechanisms to protect the authenticity of communications sessions.   | nCircle audits the configuration of assets to ensure they protect the authenticity of communications sessions (such as ensuring that logon credentials are not cached).   |
| SC-29   | Heterogeneity                                  | The organization employs diverse information technologies in the implementation of the information system.   | nCircle identifies all IP-enabled network assets including their operating system and applications. nCircle generates reports with this information as proof of heterogeneity.  |
| <b>System and Information Integrity</b>               |  |  |   |
| SI-2  | Flaw Remediation                               | The organization identifies, reports, and corrects information system flaws, tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation and incorporates flaw remediation into the organizational configuration management process. | nCircle gathers detailed intelligence about the end-point devices on the network, prioritize vulnerabilities and configuration deviations. The results and reports generated by nCircle solutions provide the information to demonstrate periodic review for known vulnerabilities and software patches promptly installed. |
| SI-3  | Malicious Code Protection                      | The organization employs malicious code protection mechanisms.   | nCircle audits assets and can ensure that malicious code protection mechanisms are in place.  |
| SI-4  | Information System Monitoring                  | The organization monitors events on the information system.  | nCircle can identify unusual or unauthorized changes to asset configurations and alert administrators.  |
| SI-6  | Security Functionality Verification            | The information system verifies the correct operation of security functions when anomalies are discovered.   | nCircle automatically notifies administrators when vulnerability or configuration scans do not complete or complete with errors.  |
| SI-7  | Software and Information Integrity             | The information system detects unauthorized changes to software and information.   | nCircle can assess and monitor the integrity of software and information through its file integrity monitoring capability.  |



| NIST SP 800-53 Controls   |  | Control Description  | nCircle Coverage  |
|---------------------------|--|--|---|
| <b>Program Management</b> |  |  |   |
| PM-5                      | Information System Inventory                 | The organization develops and maintains an inventory of its information systems.                                 | nCircle discovers all IP-enabled assets on the network including servers, desktops, laptops, routers, switches, firewalls using agentless technology. nCircle utilizes both active and passive network scanning to discover and assess networked hosts. To make the discovery process accurate and manageable in a large network, nCircle correlates hosts across scans with multiple parameters including, IP address, MAC Address, host name, stack fingerprinting, open port fingerprinting and Net BIOS name. |
| PM-6                      | Information Security Measures of Performance | The organization develops, monitors, and reports on the results of information security measures of performance. | nCircle solutions provide built-in objective metrics to measure security and compliance performance and trending reports to track progress over time.   |

## About nCircle

nCircle is the leading provider of automated security and compliance auditing solutions. More than 4,500 enterprises, government agencies and service providers around the world rely on nCircle's proactive solutions to manage and reduce security risk and achieve compliance on their networks. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership. nCircle is headquartered in San Francisco, CA, with regional offices throughout the United States and in London and Toronto. Additional information about nCircle is available at [www.ncircle.com](http://www.ncircle.com).



**nCircle**  
info@ncircle.com  
[www.ncircle.com](http://www.ncircle.com)

**Corporate Headquarters**  
101 Second Street, Suite 400  
San Francisco, CA 94105  
Phone: +1 888 464 2900  
Fax: +1 415 625 5982

**Europe Headquarters**  
Venture House  
Arlington Square  
Downshire Way  
Bracknell  
RG12 1WA  
United Kingdom  
Phone: +44 (0) 1344 742829  
Fax: +44 (0) 1344 741001  
emea@ncircle.com