

# Configuration Auditing – The Next Critical Step in Compliance

Michael Santarcangelo  
Securitycatalyst.com

**nCircle**<sup>o</sup>

WHITEPAPER

## The Need for Configuration Auditing

Configuration auditing is the process of verifying the configurations of assets to ensure they match with stated security and compliance policies. While compliance may be the driver for many organizations, enterprises that utilize automated configuration auditing experience benefits in compliance, security and beyond. While common approaches to uncovering and managing risk – like vulnerability assessment – provide an essential foundation, developing a complete picture of an organization’s risk posture requires configuration auditing.

Configuration auditing does more than check the “compliance” box, it provides three key benefits:

1. **Lowers the cost of compliance** by reducing the time and cost to prepare for audits with increased confidence that assets are properly configured
2. **Increases security with actionable insights** -- with the ability to quickly and effectively establish a proper and secure baseline for the configuration of all assets and monitor incremental changes
3. **Reduces burden and increases efficiency** of operations with continued visibility and insight into the environment, including changes and new introductions (planned and unexpected), with meaningful and actionable reports

As the assets organizations depend on to process and protect information grow more complex and more numerous, configuring these assets properly gains importance. More hands, more complexity could mean more risk – especially if someone intentionally or accidentally modifies the configuration on key assets.

Configuration auditing entails verifying the configurations of all assets in the environment to make sure they have the correct settings. This includes auditing new assets, monitoring for changes and verifying that planned changes are carried out properly. Realizing the importance of configurations in protecting sensitive information, more and more compliance standards and regulations incorporate the need for regular and consistent audits of system configurations.

## The Importance of Automation

Conducted manually, checking the configurations on an asset-by-asset basis requires a huge investment of time and labor and can be disruptive to operations. Each asset has thousands of configuration options that can be audited such as password length and complexity, file permission levels, file integrity and installed software. Additionally, without automated discovery, new assets might be overlooked and changes may be impossible to identify.

## Configuration Change Monitoring

A significant challenge for any organization is to ensure system configurations remain compliant with internal and regulatory security and compliance policies. Even the best administrators can make mistakes, and the cost of missing a key configuration or accidentally skipping an asset could be catastrophic. All it takes is a misconfigured web server on a critical server or a port accidentally left open on the external router and the organization could be unwittingly granting access to hackers and worms.

Configuration auditing completes the picture of risk, enhancing the visibility of assets on the network with specific benefits to operations, audit and security. Time, money and talent are

scarce resources; configuration auditing saves time and money and provides immediate returns with actionable information, alerts and intelligence to make key decisions.

## Configuration Auditing: The Essentials

The value of configuration auditing is straightforward: gather information about the configuration of assets on the network, and compare those configurations to the desired state. Selecting and choosing the right solution to extract that value is made easier by considering some basic elements and understanding the implications of key decisions.

Compliance is a key driver for many organizations considering configuration auditing. The challenge is that security does not always equal compliance. Similarly, some organizations are able to demonstrate compliance without security. The key to success is to use this as an opportunity to select a configuration auditing solution that optimizes available budget to improve security and achieve compliance.

## Auditing versus Management

The purpose of auditing – useful to both security and audit teams – is to ensure the recommended and required configurations are in place and maintained. These assurances to management and others are benefitted by a solution that is able to provide a complete picture without modifying the target.

The same tool used by employees to make authorized changes could present an opportunity for an attacker to make unauthorized changes. And when legacy, new and custom assets are not covered by the management solution – there is no visibility and no reporting.

**Configuration auditing tools verify that current system configurations match desired configurations; Configuration management tools are used to change system configurations.**

The bottom line is that configuration management is not the right tool for auditing the IT infrastructure. Successful auditing of assets includes the asset, the people, process *and technology* to manage those assets. For example, if the configuration management tool reports changes being made, but those changes are not taking effect (for whatever reason), how much confidence can be invested in those reports? It's a bit like having students grade their own tests.

The point is to select a solution that provides insights that reduce the cost of audit preparation while also improving security and assuring the configurations of assets on an ongoing basis.

## File Integrity Monitoring

One of the core concepts of configuration auditing is file integrity monitoring. The concept is simple: create a listing of important files and regularly audit the files to see if they have changed. Often used as an alarm of sorts, file integrity monitoring is useful for alerting audit and security teams when key files – those generally not expected to change – are changed.

When considering the role of file integrity monitoring, consider the frequency of the monitoring relative to the speed of response. For example, PCI regulations require a weekly review. Most organizations would agree that checking configurations for changes on a more regular basis is best practice. The key to an effective solution is to ensure the ability to audit regularly – the right balance of information matched to the needs of the organization to manage risk and demonstrate compliance.

### **File Integrity Monitoring is required by the PCI DSS Standard 10.5 and 11.5:**

*Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or content files, and configure the software to perform critical file comparisons at least weekly.*

## Agent or Agentless

When it comes to auditing or maintaining the configuration of assets, the legacy approach was to install a small piece of software called an agent on the target machine. The drawbacks of utilizing agents are simple: they require disk space, memory and processor cycles in addition to a communication channel with the central management console. While agents have a place in some solutions, the next generation approach is an agentless solution.

A key benefit of agentless solutions is they do not require installation on the target asset. Eliminating the need to “touch” each asset to be audited provides several advantages for agentless solutions:

- significantly faster to implement
- cost less to own and operate
- utilize less system resources than agent-based solutions
- scale more easily to cover large numbers of assets
- provide coverage of devices that cannot support an agent

What happens if someone introduces a new asset into the environment without following protocols? In environments with agent-based configuration auditing tools, the new asset will likely only be discovered by accident or when there is a problem. Agentless solutions, on the other hand, do not rely on a pre-determined list of assets. Instead, they are able to discover and audit the entire network – reporting on known as well as unknown assets.

To help understand the efficiency of the agentless approach, consider the following:

- How many known assets are in the environment?
- How much time would it take to manually touch all those assets (either to add an agent or manually check each configuration)?
- What is the value of getting information within a few hours of deployment?

Agents typically require testing, permission and coordination among different groups, which can be politically challenging. Agents can generally be deployed at the rate of 10-20 per day, while agentless solutions can be set up within a few hours.

Agentless solutions provide the ability to scan, identify and report on non-standard assets or assets that do not readily allow for agents. For example, today's printers have fast processors, plenty of memory and are connected to the organization's network; perfect jumping off points for intruders, yet printers cannot accept agents for configuration auditing. Agentless solutions ensure these assets stay within compliance.

### ***Agentless Auditing Delivers***

- ***Faster deployment***
- ***Greater asset coverage***
- ***Instant time-to-value***

Agentless configuration auditing solutions provide inherent advantages: faster deployment, wider scope of reporting capabilities and insight when it is needed most.

## **Effective Asset Coverage**

It is challenging in ever-changing environments to define and agree to assets in scope of configuration auditing. But the real challenge extends beyond known assets and configurations to unknown assets and configurations. Things change fast in enterprise environments and without proper policies and good controls, things will slip by. It is essential to select a solution that is able to find and assess a wide variety of assets – actively and passively, known and unknown. Moreover, once assets are discovered, considered and determined to be in scope, how are baselines defined?

The right configuration auditing solution delivers the ability to leverage a wealth of industry standard guidance to properly – and quickly – assess all assets, make scoping decisions and gain actionable insights.

The key is coverage of the breadth and depth of the devices in the network. Breadth provides the ability to scan and recognize a wide (and growing) list of potential assets and devices on the network. Depth is the capacity to interrogate and report key information on what is discovered.

### ***Assessing the Entire Network***

- ***Web applications***
- ***Enterprise applications***
- ***Middleware***
- ***Databases***
- ***Operating Systems***
- ***Network Infrastructure***

For example, consider this recent experience and how common this is: A company deployed a configuration auditing solution for the first time, started the network discovery phase and went to lunch. When they returned and checked the initial report, they learned of a rogue wireless access point – clearly identified as an Apple Airport Express. And it was installed two doors down from the security manager!

This wasn't a case of malicious intent, but of a well-intentioned employee seeking an easier workday by not having to connect some wires. However, the employee hadn't fully considered the implications of their actions on the security or compliance of the organization. By quickly identifying this potential risk, the security manager was able to take action and prevent security or audit issues.

As environments continue to change, being able to rapidly detect – and report on – new assets (expected or otherwise) is essential to improving security and compliance.

## Actionable Intelligence

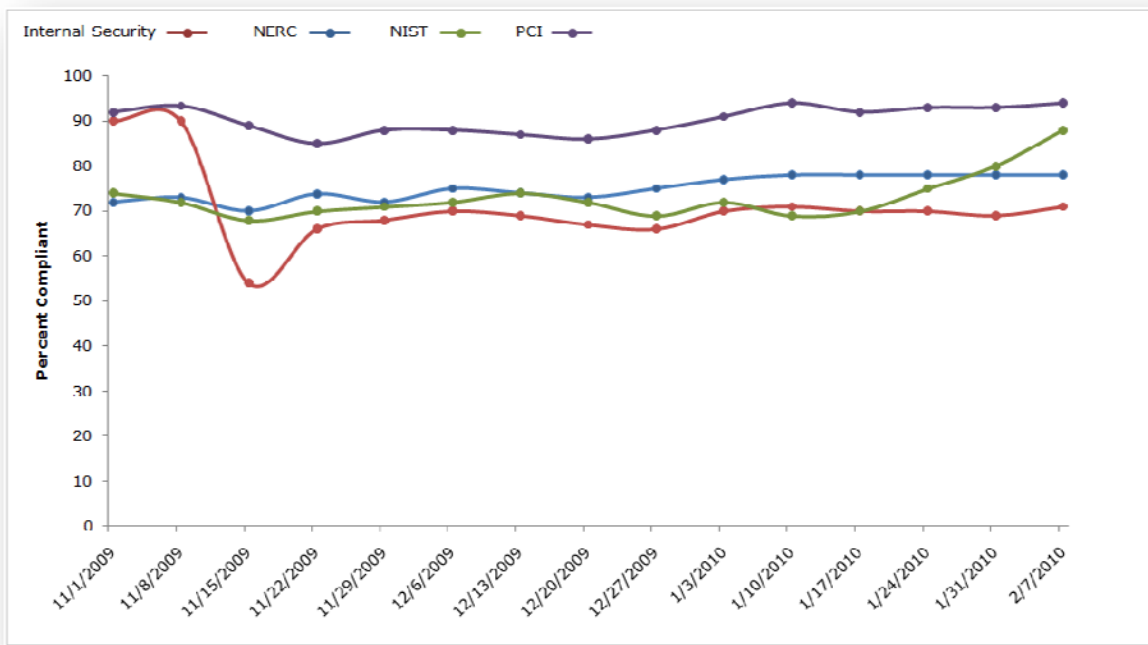
As important as it is to be able to see everything and gain key information, the real question is “what can you do with the information gathered?”

When considering how a solution will be used, one should explore how information is captured, processed and reported. To be effective, information needs to be presented in a way that makes sense, can be explained and is consumable.

Look beyond tools that seek to impress by dumping reams of data and ask if the analysis of the data is clear, easy to read and useful for explaining to others. Are assets and actions clearly prioritized, customizable and coupled with useful metrics that produce the right report for each audience?

Absolutely essential is the ability to prioritize information based on a variety of criteria to meet the needs of different audiences including security, IT operations, audit teams and upper management. For example, to prioritize a report based on an industry-standard compliance initiative to help prepare for an audit, or a custom-designed policy to reduce risk in the enterprise. It’s also necessary for the reporting to indicate whether or not expected changes – for compliance or security -- are permanent.

Effective solutions are designed to provide usable information, backed by empirical evidence. Reports are comprehensive, flexible and able to be focused on the specific audience by presenting what is needed to make better decisions.



*Configuration auditing delivers a comprehensive picture of the organization’s compliance with applicable policies such as PCI, NIST, NERC or internal security and compliance policies.*

## **Choosing the Right Configuration Auditing Solution**

Configuration auditing does more than check the “compliance” box; the right solution lowers costs, increases confidence and improves decision making across the organization. It guides the right actions, at the right time, backed with the insight and information to reduce risk. In fact, a single solution that benefits security, operations and compliance teams enables these organizations to do their jobs easier and faster and at a lower cost. nCircle Configuration Compliance Manager™ (CCM) delivers these benefits and more.

## **Lowering the Cost of Compliance and Increasing Confidence**

The challenges of compliance require the ability to identify and address problems *before* the next audit. An effective configuration auditing solution provides confidence in preparation for the audit by providing the actionable information required to make effective decisions.

Often the first step in the process of preparing for an audit – or simply assessing the current state of compliance – is to get a complete picture of the assets and configurations in the environment. While it is possible to set a configuration auditing solution to simply grab as much information as it can see, the comprehensive rush of information can be overwhelming to the point of paralysis. Advanced configuration auditing solutions, such as nCircle Configuration Compliance Manager (CCM), ease this initial process with the inclusion of industry-standard policies and templates.

This initial insight saves time and resources by helping to quickly determine which assets are in scope for compliance and what baseline to measure against. For example, standard PCI, FDCC, NERC and Sarbanes-Oxley policies enable organizations to easily compare their assets to the best practices baseline and generate a report based on those findings.

More important is the ability to rapidly obtain and act on information supported by evidence. Within hours of deploying CCM, actionable intelligence is presented that answers key questions like the problem areas that need to be addressed first. This forms a comprehensive plan of action that is readily understood by everyone involved in the process of preparing for an audit.

The ability to guide the right action at the right time reduces friction – saving time and money and ensuring necessary changes are made in a timely manner. In fact, the advantage to this approach is the ability to start with a baseline that reveals the actions necessary to ensure compliance in a way that allows for iterative changes and incremental reports. Instead of presenting a huge, seemingly insurmountable “information overload” challenge, CCM produces clear and prioritized reports that make the process of preparation easier and more palatable.

Equally important to preparing for audit is instilling confidence in the changes being made. Over time, regular reporting from configuration auditing provides additional important insights about whether the problems being addressed are actually being fixed, or if they keep cropping up in the environment. This extends to checking for new regulations or changes, too. CCM includes the ability to update and modify the profile of audit needs. This means the audit team is always aware, always ready and always prepared.

CCM enables enterprises to prepare for an audit more quickly, efficiently and thoroughly. But CCM provides more than just *preparation* for an audit. Once the environment is operating in a compliant state, CCM provides confidence and removes surprises with ongoing intelligence, measurement and proof of compliance. This reduces stress, complexity and burden on the audit and security teams while improving the performance of audit examinations. And CCM is part of

nCircle Suite360™, which enables organizations to perform comprehensive security and compliance audits across the entire enterprise network.

## Improving Security with Actionable Insights

In most production environments, risk is introduced through configuration changes. Therefore, effectively managing and reducing risk depends on capturing and acting on information that informs the decision-making process about where and how to best use available resources. The more accurate, complete and timely the information, the better the ability to respond appropriately to increase security and reduce risk.

Where an ounce of prevention is worth a pound of cure, early detection and notification about changes to configurations (regardless of the reason) allows organizations to improve security while demonstrating compliance. Better, a solution like Configuration Compliance Manager does more than alert on changes; it actually aids the process of improving security.

It starts with “one click compliance” – the use of industry-standard policies to measure risk and provide useful information about the current state of the environment. This matters, because it provides an accurate picture of the actual assets and configurations in the environment; not just what people report, but what actually exists.

The use of industry-established benchmarks has an additional benefit: less arguing. Rather than debate what should be in a policy or what needs to be audited, it is less complicated and quicker to agree on a standard policy – or even use different policies to form an initial picture. Discussions centered on actual information are more meaningful and productive.

Since CCM utilizes agentless technology, there are no concerns over disrupting any systems. The report generated from this step produces easy to understand intelligence, rating problems on a scale of 1 to 5. And the policies are easy to change, providing the ability to contrast, compare or modify the policy to ensure a complete and accurate audit.

The prioritized reporting enhances and guides the remediation process – important given limited time and resources. Make the changes with the biggest and most important impact first (and in line with the needs of system compliance). Changes can be compared against the stored baseline and policies, providing confirmation that the changes were made and indicating follow-on actions.

This iterative process guides incremental improvements – useful in environments that rely on a blended workforce of employees, contractors and partners. This allows people to get comfortable with incremental changes – step-by-step security is improved with minimal disruption. Utilizing CCM to audit assets on the network provides irrefutable evidence for

### Configuration Compliance Manager includes built in policies:

- NIST Hardening Guides
- Sarbanes-Oxley
- PCI
- PCI-File Integrity Monitoring
- NIST SP 800-53
- NERC
- HIPAA
- FDCC
- Center for Internet Security platform-specific policies

discussions about changes in a more neutral, supportive way. This tool is the pathway to constructive conversations that encourage and support necessary changes in the environment.

As the security profile is improved, deviations are easily addressed. What starts as an initial “sanity check” using prebuilt policies leads to improved insight, knowledge of the production environment and customized policies. The initial (prebuilt) policies can be copied and with simple cut-and-paste actions, new and customized policies are created.

A real advantage to this approach is the fact that when an asset is being monitored – but not directly controlled – a lot of complication and political wrangling can be avoided. The same system that helps maintain an “audit ready” mentality is equally beneficial to the security team to keep tabs on the environment by monitoring, not changing systems, thereby avoiding asset ownership disagreements.

## **Increasing Operational Efficiency**

Assets and the organizations that maintain them are not static. In a dynamic environment, planned and unplanned changes have an impact on audit, security and operations. Once the audit has been successfully passed and security increased in the environment, ongoing utilization of CCM supports healthy change management processes with verification and reporting and goes further by exposing new assets and prioritized risks with configurations. And utilizing CCM with nCircle’s Suite360 other solutions enables organizations to stay secure and compliant, dramatically reducing the preparation time for the next audit.

This means continued audit-readiness by maintaining logs useful for future audit preparation and continued reporting. The key is how: CCM becomes the system of record, reducing workload and burden on IT administrators and staff. Moreover, these same logs and reports are useful for incident response, forensics and other previously complicated, time-consuming and costly endeavors such as software licensing and inventory.

The key to productive use of time is the ability to get more complete and accurate information. Teams that utilize the insight and actionable reports from CCM are able to routinely and effectively do more with less. This creates a side benefit of a more informed, supported and motivated workforce – which is always a plus. With the ability to audit without agents installed on the asset – new assets, devices and changes in the environment become opportunities for improvement instead of surprises that ruin weekends.

As compliance and regulations evolve over time, policy updates and changes are easy – meaning a new report informing potential risks, changes and actions is quick and easy to develop.

But beyond these, a solution with the ability to discover new assets – and the breadth and depth to report more completely on a wider range of assets – provides more information and more insight. Information is power, and once in use, CCM can also be used for otherwise complicated tasks like inventory checking and general management reporting. It can even be used for reporting on software inventory and licensing.

## Learn more about Configuration Compliance Manager from nCircle

nCircle designed and built Configuration Compliance Manager from the ground up for the specific purpose of auditing configurations and presenting actionable, prioritized reports. It was designed to use agentless technology to provide faster, more comprehensive and more effective reporting. CCM examines the widest variety of assets and provides the broadest view with the most comprehensive configuration checks.

nCircle Configuration Compliance Manager is part of nCircle Suite360™, nCircle's award-winning security and compliance audit suite. nCircle Suite360 combines the broadest discovery of networked assets and their operating systems, applications, vulnerabilities and configurations with advanced analytics to help enterprises reduce security risk and achieve compliance. nCircle Suite360 includes:

- IT Governance, Risk and Compliance
  - **Suite360 Intelligence Hub™** for IT GRC Reporting, Intelligence and Analytics
- Agentless Discovery and Assessment
  - **IP360™** for vulnerability management
  - **Configuration Compliance Manager (CCM)™** for configuration auditing
  - **WebApp360™** for web application scanning
  - **File Integrity Monitor™** for file integrity monitoring and compliance
  - **Topology Risk Analyzer™** for line of sight risk analysis
- On Demand (SaaS) Services
  - **Certified PCI Scan Service™** for on demand, self-service PCI DSS compliance
  - **HITRUST™ Security and Configuration Audit Service** for on demand, self-service compliance with the HITRUST Common Security Framework of standards for the healthcare industry

Call nCircle today to speak with a knowledgeable and passionate professional to get a customized demonstration and visualize how the power of CCM will positively impact the organization.

### **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 is a registered trademark of nCircle Network Security, Inc. All other registered or unregistered trademarks are the sole property of their respective owners.

### **About Michael Santarcangelo**

The author of [\*Into the Breach\*](#), Michael Santarcangelo is a catalyst that guides smart investment in human capital, the return on which is immediate and far-reaching. He delivers *Awareness that Works™* through a highly effective, results-driven program that produces *measurable* results that are budget neutral or better. Guaranteed. Learn more at [www.securitycatalyst.com](http://www.securitycatalyst.com)