WHITEPAPER

Compliance Management’s
Seven Steps to Success
Why Everyone Needs Compliance

Compliance has grown into one of the most troublesome responsibilities IT staff encounter on a daily basis. From PCI for credit cards to HIPAA for healthcare to NERC/FERC for energy regulation to Sarbanes-Oxley for public accounting, compliance requirements have proliferated industry by industry in amounts that cause IT departments to devote considerable resources to ensuring — and proving — that their networks are meeting the mandates to which they are subject. Failure to meet compliance requirements, and to prove consistent adherence to them, can result in enormous fines, negative exposure, and deleterious impacts on performance of the network and, ultimately, the organization itself.

In addition to external mandates, every IT organization should also adhere to internal compliance requirements that are particular to its goals and mission. Whether you call them standardization, consistency, best practices, gold standards, mandates or governance, all of compliance's internal and external aliases lead to the same end: making your network look and behave in the particular way you want in order to promote seamless, secure and efficient operation. The fundamental intent of compliance requirements is to keep IT safe, reliable and consistent for everyone who uses it. Today, that's just about all the people on the planet. So compliance is a global responsibility, even though it sometimes feels like a personal problem.

Since no network is exempt from compliance requirements, the big question is this: how can your organization best and most cost-effectively meet the requirements of your security or compliance officer?

Compliance as a Catch-up Game

Most commonly, organizations come face-to-face with compliance either when something in the network breaks or when an audit comes due. Either of those instances can send IT staff on mad scrambles to research the compliance requirements, and then to find ways of documenting that they have been fulfilled. Even in cases where the organization believes that the processes are good best practices, IT staff is often too involved with the tasks of keeping the network functioning and productive to attend faithfully and proactively to ensuring compliance throughout the year.
So the scramble to meet the audit or fix the break ensues: a task force gets pulled to collect, analyze and tabulate the results device-by-device and rule-by-rule — manually. Given the growth in the number of devices, the quantity of compliance requirements, the amount of problems caused by inconsistencies, not to mention the increase in audit frequency and the growing complexity of networks, the undertaking can occupy the ad hoc task force for days, weeks or even longer.

Not surprisingly, reliance on legacy efforts and traditional techniques to attain and maintain compliance has left many organizations flailing and failing with non-compliant networks. Making the game of “compliance catch-up” even more of a fool's errand is the fact that the next break in the system or the subsequent periodic audit will occasion a re-start of the cycle all the way from the beginning because so much on today's networks changes so quickly.

**Why Is Compliance So Difficult — and Costly?**

Besides the increasing complexity of networks and the rise in the number of mandated requirements, compliance challenges reside within the very nature of IT. For example, configuration drift can be a dangerous impediment to compliance, as can errors in change management and manual execution of change processes, especially one-offs. Neither problem is easily solved because inconsistent configurations and out-of-date information are difficult to troubleshoot. Device logs, on their own, are simply not enough, nor is the practice of merely backing up configurations.

Moreover, many mandates are not well-defined and do not describe specific network configuration requirements. Not one-time snapshots, mandates move their focus and expectations with the evolution of the network and ongoing changes in the regulations they seek to enforce. Mandates are often not static from audit to audit. Additionally, external mandates required by the government or an industry sector, such as PCI, HIPAA, SOX, NERC/FERC, etc., entail extensive auditing and reporting requirements. So how can an organization keep up?

Instituting best practices and standardization is the route many organizations take, essentially setting up their own “internal” mandates. The IT and networking teams also often create and define their own gold standard for optimizing their organization's network. They will build best practices for network compliance based on industry standards within their sector, such as PCI, NSA, SANS and DISA, to name but a few. The goal is to track and audit configurations, identify device changes and monitor the network proactively for compliance so that reports and documentation can be presented when needed. Defining standards and showing control typically meets network compliance requirements.

But when an audit comes due, the organization still has to rely on a task force to collect and tabulate all the data, the logs, the reports, and the documentation, and then put it into a format that will get the auditors to nod their heads. Depending on the size of the organization, the types and number of requirements, and the complexity of the network, it can take two people a week or a dozen people a couple of months.

Is anyone at the organization tallying the time and expense reports for this task force approach to proving compliance?
Seven Steps in the Compliance Game Plan

These days, IT teams are taxed with more responsibility than ever before, and many of them — rightfully so — dread the coming of the audit and the extra work and time spent on a task force devoted to proving compliance. Most IT teams would much rather be focused on more company-centric productive tasks. The reason the task force approach to compliance is so costly in terms of manpower is that it starts with the last of the seven steps in the compliance process, and then tries to go back and complete the ones it skipped.

Here are the seven steps for successful compliance in the order in which they should be carried out:

1. **Inventory**
   Know what's on your network in order to determine whether it's in compliance.

2. **Auditing**
   Determine what is going on now.

3. **Definitions**
   Lay out what you need to accomplish in order to be in compliance.

4. **Segmentation**
   Determine what devices and network components belong to which mandates.

5. **Monitoring**
   Assess everything on the network constantly to detect anything that falls out of compliance.

6. **Remediation**
   Fix non-compliant situations immediately before they cause additional problems.

7. **Reporting**
   Document the state of compliance on the network from end to end.

The task force approach begins with the last step and works backwards, causing potential errors, risking non-compliance, incurring excessive expenses in time and labor, and often skirting the issues that the compliance mandates were instituted to solve or prevent in the first place.

There is a better way to achieve compliance on an ongoing basis, 24x7, with a minimum of IT staff involvement — automating compliance management.
How to Automate Compliance Management

The automation of the seven steps of compliance management is rooted in a common sense approach to the compliance challenge: identification, implementation and validation.

An automated compliance management solution first engages in identification of all that is on your network by understanding the foundation of both the network components and all the compliance requirements. This stage of automation puts accurate and up-to-date information at your fingertips at any given moment. You cannot plan for future needs unless you know what you have today.

The second stage in automating compliance is the implementation of the compliance mandates, whether external or internal. The keys to this stage are knowing what it takes to become compliant the first time for each individual mandate, determining how the mandates impact your network and determining which devices are affected by any given requirement.

Validation is the third stage of compliance automation in which you prove that the network is in compliance from end to end. The individual compliance procedures must be verified for all devices, and their proof must be available to auditors in reports and documentation. But that is not enough because, remember, this is not a snapshot: validation must be ongoing so that reports and documentation can be available to prove past and present compliance at any given moment. Consequently, surprise audits are no problem.

Let’s examine in detail how automation uses identification, implementation and validation to execute each of the seven steps for successful compliance management.

Create an Inventory for the Entire Network

Virtually no network today is a single vendor shop. So an automated solution must accommodate multiple vendors on the same network. Since spreadsheets contribute not only to out-of-date information but also to human error and labor-intensive expenses, automation eliminates them. Visio diagrams and “smart staff” work well for topological information but not for compliance and auditing, so they are not in the mix either.

Instead, automation uses auto-discovery of multivendor devices to ensure current and correct network information, including unplanned devices, and maintains a detailed inventory of all chassis and device components, interfaces, operating systems and model inventories. An automated compliance solution also provides Layer 2 and 3 summary views, and monitors Layer 3 logical information, including routes, subnets, VLANs, HSRP/VRRP groups, ports and other components — all in a single system. The presentation of network components in this way enables IT teams to visualize the complex relationships among multiple devices for a detailed topological view of the network from end to end.
Complete and Audit of Configuration and Change

Reliance on the change management process results in limited documentation and cannot account for changes made outside the process. The use of basic tools or scripts to save historical configurations leads to thousands of saved files that must be reviewed, and documentation is inefficient when roles are generally “admin or nothing.”

An automated compliance management approach tracks every network change — both planned and unplanned — including what device was changed and by whom at what time and what changed. Every configuration is automatically collected and archived, with baselines set for easy comparison side-by-side with any file in color-coded views. User-based access rights and roles maintain security in an automated solution while enabling more IT staff to use the system with control capabilities.

Define Requirements with Embedded Rules

Determining the impact of each standard on the network is difficult because variations exist between mandates and best practices. Typically standards are customized to meet the unique requirements of distinct organizations. The multitude of rules associated with the myriad number of mandates that must be followed creates a huge challenge in determining and selecting which rules apply to which components of the network infrastructure.

An automated compliance management solution addresses all these concerns by leveraging embedded rules and policies (such as those associated with PCI/DSS, ISO, DISA, STIG, IAVA, SANS and NSA) as well as templates for customized requirements unique to your organization. Because “standards” are not standardized for each organization, an automated solution lets you customize standards according to your specific organizational needs. Since IT staffers are not specialists in all the compliance rules, an automated solution has that “expertise” embedded within it to determine which of them should be implemented across your organization.

Segment Policies for Specific Groups of Devices

Because all devices are not subject to every mandate — for example, PCI affects only those devices that touch credit, debit or charge cards — requirements must be discriminatingly applied. Many networks are not segmented or well-defined, and are in need of logical groupings of devices for efficient application of mandates. The absence of segmentation creates unnecessary work and adds inappropriate requirements, resulting in an increase in labor costs and inefficiencies.

Automation allows you to define internal and/or external policies, and then individually segment the policies to a single- or multiple-device group for ongoing monitoring. Doing so greatly reduces IT staff time and effort and increases network efficiency. Devices can be grouped by the types of compliance requirement that affect them, thereby allowing the mandates to be applied efficiently and correctly.
Monitor All Components on the Network 24x7

Organizations know that they should monitor their networks for compliance on an ongoing basis, but most do not have the time or the staff to do so when the monitoring is done by manual means. While most admit that compliance and standardization should be 24x7, they normally think of monitoring to verify network compliance only when something breaks or an audit is imminent. Few consider the risks and exposure involved if violations happen to occur months before an audit.

Compliance management automation obviates these risks and exposures by proactively monitoring current settings against standards 24x7. An automated solution provides proactive violation notifications, and even includes auto-remediation options for correcting and resolving any problem immediately, usually with little or no IT staff intervention.

Remediate Violations Before They Become Problems

Most violations of compliance requirements cause problems before they are detected. Often the problem is what signals that a violation has occurred, frequently at some time in the past. The reason for this too-little-too-late discovery is because manual processes for finding and remediating a problem require a great deal of time and effort. Less experienced staff may even prolong the problem because of the difficulty in understanding how and why a violation occurred.

In an automated compliance management solution, remediating change happens within the same interface. Embedded expertise, scripts and templates automate many tasks typically handled manually or by ad hoc Perl writing. That means the requirement violation can be fixed automatically before a problem ensues, which can save considerable expense in fines and penalties.

Report with Confidence Based on Proof

Creating the report is the step where many organizations begin rather than end, thinking that a report is all they need to fulfill compliance mandates. When adherence to requirements has been less than optimal, some organizations try to befuddle auditors by overwhelming them with excessive amounts of data. Sometimes an organization will perform a self-assessment, essentially an internal audit, and let some aspects “slide” with the intent to “fix” them in the future, a decision that almost always has repercussions, usually sooner rather than later. These approaches to the compliance conundrum are simply inadequate. They occur because in most organizations day-to-day tasks so overburden IT staff that compliance is often relegated to a backseat.
Pre-built reports in an automated compliance management solution can prove compliance quickly and with far less manual time and effort. You can schedule generation of the automated reports or request them on demand in real time. High-level reporting in an automated solution allows you to visualize current compliance status easily on a customizable interface and drill down to inspect individual violations or parameters. The reason that an automated solution can achieve these ad hoc reports that prove successful compliance is because the first six steps have been automated and performed on an ongoing basis. In short, automated compliance management lets you deliver proof of compliance to an auditor at any time, on demand, with a simple click.

**Infoblox Automation Delivers Total Compliance Management**

The automated compliance management solution from Infoblox delivers all seven steps to compliance success on an ongoing basis 24x7 to keep your network in consistent, reliable, efficient and secure compliance at all times. The reports to prove it are just one click away on demand. Embedded rules and policies reduce the need for staff expertise and let you build templates easily for both internal and external compliance mandates. Industry standards are included, such as PCI-DSS, NSA, SANS and DISA, and device grouping allows you to set multiple policies for single devices, including customizable attributes. Automatic discovery, change detection, configuration backup and archiving are integral parts of the solution, and continuous monitoring and automatic violation detection with drill-down views and auto-remediation options keep your network in continuous and consistent compliance 24x7.

Infoblox takes the dread out of the audit process by making standard and custom reports available at any time with a single click, including visual validation of compliance to show proof of full compliance on demand. The solution also correlates the impact of change for you to help you understand what is happening now on your network and to plan for the future.

Incorporating a compliance management from Infoblox into your IT arsenal can improve the stability and consistency of your network and the efficiency and productivity of your staff. Automating compliance eliminates manual, repetitive and mundane processes, allowing you to show proof of compliance with far less manual collection of data. Multiple-vendor device support means identification and resolution of violations through remediation options will greatly reduce your organization's risk of fines, adverse exposure and performance problems.

In sum, let Infoblox help you leverage automation, intelligence and reporting to verify the process, intent tracking and auditing features that put compliance under your complete control.
About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,500 enterprises and service providers in 25 countries control their networks.