Why Passing Your Compliance Audit is only the Beginning...

Produced on behalf of New Net Technologies by

STEVE BROADHEAD

BROADBAND TESTING

www.nntws.com

NNT™
SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

‘Everything you wanted to know about Compliance’...

“...software won’t make your organization compliant”

If you haven’t yet been asked ‘The auditors want us to...’ or ‘The auditor suggested...’ or ‘...wants to know how we...’ the likelihood is, you will be soon!

This whitepaper is a Guide for IT professionals – an ‘Everything you wanted to know about Compliance’. Anyone with experience of being audited in the past will learn how to remain compliant with your required standards, making the next round of Audits much more straightforward.

‘Software won’t make your organization compliant’

We’ll start by breaking the rules for any software vendor when publishing a whitepaper of this nature by making the statement that our software won’t make your organization compliant. In fact, we are not alone in this respect - there isn’t any software available that will make your organization compliant and as you read the rest of this paper, you will understand why. Compliance requires a cultural alignment at a personnel and process level, together with specific standards of access control and security for IT systems.

Software tools are an essential component in providing a bulk, automated and real-time assessment of your IT systems’ compliance that no human process could ever achieve. NNT Change Tracker Enterprise is an example of the state of the art in compliance audit technology.

From legislation to measurable practise

“Compliance requires a cultural alignment to compliance at a personnel and process level as well as specific standards of access control and security for IT systems””

As IT has become inextricably linked with the ability of any organization to conduct its business, so it has become the remit of auditors to not just verify that sound accounting practises are being observed, but that sound governance of IT is in place too.

In the case of the US Sarbanes-Oxley (SOX) legislation, one of the key objectives that drove the development of the act in the first place was a need to ensure that the kind of financial malpractice evident at the time could not happen again. The SOX act made the executive board directly responsible for the integrity of financial reporting – no ‘if’s or but’s’ - and no turning a blind eye to balance sheet anomalies.

How can this be achieved? There must be no way that any financial reports can be tampered with, adjusted or altered, so that any statement signed off by the Executive Team is verbatim. Since all reports originate, are communicated by, and stored using IT systems, SOX has a direct bearing on the security and integrity requirements of IT systems.

Similarly, for PCI DSS, the Payment Card Industry Data Security Standard, all cardholder and card data must be protected, or in the case of HIPAA, the US Health Insurance act, it is patient data which must be kept private. In all three examples this means that the entire IT infrastructure must be secure and ‘locked down’.

From legislation to measurable practise ...contd.

The fine detail of exactly what the definition of 'sound governance' encompasses will be driven by the particular industry you are in although there is a high degree of convergence across the various policies not least because there is a general consensus between IT Service Delivery teams and Auditors that this is all a 'good idea'. You may also find that the scale of your organization determines the extent to which you may be able to 'self-certify' compliance rather than requiring an auditor visit and report.

The challenge arises over the exact detail of how to achieve compliance, with complicating factors being the potentially high stakes involved (fines for non-compliance, being subject to more rigorous audits in the future, and in the case of PCI, being blacklisted as a payment card merchant, not to mention the corporate shame and scandal as your organization hits the headlines...) coupled with deadlines for audits taking place.

A financial services customer reports being subject to at least five different standards for compliance. These are a mixture of US and UK/European regulatory body standards, plus PCI DSS plus their own internal company standards of IT security. They are always being audited...

The case for PCI DSS

Two years ago, US clothing retailer TJX suffered a long-running security breach, later traced as starting off from an insecure wireless network at one of its stores, which resulted in the exposure of 45.7m credit card records, going by conservative estimates. Other estimates put the figure at 94m accounts.

The retailer set aside $118m to cover costs and potential liability arising from the breach in August 2007, later earmarking $40.9m of these funds to settle a lawsuit from banks hit by fraudulent losses tied to the attack in December 2007

source- www.theregister.co.uk

The Basics - Governance, Policy, Compliance, Regulatory Control, Audit

If you are reading this whitepaper as a novice in the world of Governance, Regulation, Compliance (GRC) then you will probably want to know what it means and what you need to do to 'get compliant'.

You may have already found that getting a simple answer is not as easy as you imagined!

One of the difficulties with having this goal as a starting point is that to give a general overview of GRC as a whole is somewhat of a paradox. The best way to approach getting an understanding is to focus in on what your organization needs to do to be compliant then work outwards to understand the picture.

Governance – do you run a 'tight ship'? Do you manage, control, document and check your IT systems to a high standard?

Regulatory Compliance – operating standards your organization must adhere to in order to meet with legal obligations or industry standards

Policy - Do you have robust systems and processes for ensuring good governance? Can you define and document what 'good' standards are for system security and access control?

Compliance – Can you prove you are maintaining systems to be in line with required standards?

What exactly is a Governance Policy in IT Terms?

"a formal change management process is mandatory"

Specifically it is a checklist of standards in operational procedures and network and server configuration practises, with the objective of securing and making tamper-proof sensitive data, and ensuring mission-critical business processes dependent on IT are assured.

For instance, in the PCI DSS policy, section 1 calls for the following procedural measures to be in place -

> *"A formal process for approving and testing all external network connections and changes to the firewall configuration"*

An auditor will be looking for a process to exist and be sufficiently robust to ensure that the firewall doesn't get changed without proper authorisations and security checks being observed – this is one of the ways the auditor can be satisfied that a firewall that is in place and securely operating remains so. In summary – a formal change management process is mandatory.

Similarly, an example of a specific network and server configuration requirement -

> *"Always change vendor supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts)"*

An almost all pervasive check when it comes to IT system compliance is that of ensuring the Guest Account is not enabled on a server, for example.

"we are going to need an agreed definition of what constitutes a suitably 'locked down' or 'hardened' system"

Given a clean-sheet of paper you could probably summarise a list of basic steps needed to achieve this – firewall all your external connections, strip down user accounts to the bare minimum and reset passwords, similarly cut out all but essential drive shares and network access. But then you need to make sure there is no malware exposure that could be introduced at a user PC level – a Trojan could be resident on a user's laptop used at home that is now attached to your network? And while we are at it we should disable all the other potential access means to a system such as the Messenger Service, Terminal Services access, Remote Access Connection Manager – any others?

In summary we are going to need an agreed definition of what constitutes a suitably 'locked down' or 'hardened' system. Pick any of the common policies in circulation like PCI DSS, NERC CIP and HIPPA (N.B. see our glossary of terms at the end for details of these various standards) and they all encompass details of requirements with a high degree of consensus on what needs to be done in this area.

By now you will be starting to get the picture of what the high level aims and the fine detail of a typical policy portray. So little surprise then that as a natural progression from the initial perimeter and end-point security outlined above, there is also an operational, every day dimension to ensure systems remain secured. Again there is a consensus across all the most common policies, that is, we need tight change control – we need to make sure everything continues to remain in a compliant state.

What exactly is a Governance Policy in IT Terms? **...contd.**

"being ITIL aligned won't make your organization compliant with your requisite standards and policies, but it will go a long way to ensuring that you have the structure in place to do so"

From an IT strategy and Auditor standpoint, there is a need for reassurance that there are sufficiently robust and detailed procedures in operation to enforce adherence to the standards required by the policy. For instance, all personnel in the IT department must demonstrate they understand and follow procedures for making changes to system configurations.

This is another reason why the adoption of ITIL is gaining pace in as much as it provides probably the most complete framework available defining processes for running an IT Service Delivery operation. Again, being ITIL aligned won't make your organization compliant with your requisite standards and policies, but it will go a long way to ensuring that you have the structure in place to do so.

One of the problems in running an IT Service Delivery operation is that the only constant is change. At a system level, there are requirements to ensure security patches are updated just to stand still but of course, new applications will be introduced at some stage while existing application will need to be regularly updated, and then server, network and storage infrastructures will always be changing too.

So compliance is a constant, every day driver in everything that IT does.

Some Compliance Audit FAQs

So do we need to check every device in our estate?

Potentially, yes – an auditor won't examine every single device as it just isn't practical to do so, and therefore they will typically use a statistical sample of your estate. Assuming that keeping your fingers crossed that they only check compliant devices isn't an acceptable strategy, it is vital that all devices are compliant in advance of an audit.

And herein lies one of the first uncomfortable truths about compliance – nothing but a comprehensive and pervasive approach is going to be acceptable. If the aim of a policy is to ensure that critical data is absolutely secure and tamper-proof, it stands to reason that any access point to that data is going to need to be 'locked down'.

Are there any ways to reduce the burden?

One strategy to reduce the burden of maintaining systems to be compliant is to segregate networks. For instance, an Electric Company required to be compliant with the NERC CIP standards for cyber security will physically isolate their core control system network from their general business/administration network and thereby limit the scope of any audit for NERC CIP compliance to a subset of devices only.

Alternatively some retail organizations side-step PCI DSS requirements by effectively by-passing their internal systems – any payment card transaction is encrypted as soon as it enters the system and is then handled and processed in its entirety using a third-party data center.

Some Compliance Audit FAQs **...contd.**

Benefits of ITIL and Other Formal IT Process Framework Adoption

First-fix rate: Initial fix attempts are 45 percent more likely to be successful in top performers than in medium performers, 56 percent more likely than in low performers

Source: IT Controls Performance Study, IT Process Institute (www.itpi.org)

One point to bear in mind is that organizations using NNT software to help enforce compliance all report an overall improvement in the quality of their IT Service Delivery capability.

Taking a pervasive approach to becoming a compliant organization may look like the hard way but working to a defined policy for configuration and change management will ultimately transform an organization into a more effective and professional operation (and using NNT software it can be a much easier journey than you might have imagined)

'Locked Down, Hardened, Whitelisting, Malware protection?

The 'Locked Down' PC or server – easier said than done. What do we want to achieve? Only authorized personnel are able to use the system and have access to data and files as permitted. And we certainly don't want any malware to get onto the system.

Firewalling and Intrusion Protection operating at the network perimeter is essential but must be also be complemented by Firewalling and Anti-virus measures at the desktop.

As we all know, AV packages only deal with post-'Day Zero' malware i.e. a new virus has to be identified before it can be included in AV packages and that means there is always a time period where a virus is 'in the wild' where protection does not yet exist, so we need other measures.

Personal firewalling goes some way to contain virus spread within a network but the more effective approach to protection is to use application/process whitelisting technology.

Whitelisting takes a much simpler premise for protection from malware than Anti-Virus, literally a black and white view of the world. If an application or process isn't specifically known as safe then it is assumed it is harmful and prevented from running. In other words, a whitelist of processes and applications is referenced for what is defined OK and anything else not listed is blacklisted by default.

Whitelisting technology is specifically advocated by PCI DSS as an effective measure against malware.

Effective Steps Pre and Post Audit

"nothing but a comprehensive and pervasive approach is going to be acceptable"

You may only be audited once a year, but your obligation in the true spirit of the matter is to maintain systems compliant with all policies 365 days a year.

So the first and most effective step to take to both ease the burden on IT resources and drive a round-the-clock commitment to compliance is to automate. A means of automating an IT infrastructure audit in real-time that will also track changes to system configurations will greatly simplify your compliance workload. We began by making a statement that no software toolset will make your organization compliant, but exploiting the best technological solutions available will bring significant value.

Pre-Audit Assessment – A fast and simple way to assess your starting point

Can you exploit any opportunities to segregate systems to reduce the scope of an audit from every system to a smaller subset?

NNT Change Tracker Enterprise employs a Compliance Engine – a checklist of all configuration settings and attributes that need to be in place for a system to be considered compliant with whichever policy is being assessed. Significantly, Change Tracker Enterprise covers all servers, desktops and network devices.

Pre-defined compliance templates, known as Trackers within NNT Change Tracker Enterprise identify the complete checklist of security settings, mandatory and illegal processes and services, and filesystem and registry settings. Settings are then compared against a Policy Template and a report generated to show whether a system is compliant or not, and if so, where remedial action is required.

Although this approach will provide you with a checkpoint on how far adrift your systems are from being compliant we always recommend organizations embrace fully an 'always compliant' mantra.

Adopting a pervasive approach to change management and configuration control means all personnel will be required to immerse themselves in the correct procedures and processes, which after all is a requirement for most regulatory standards. Furthermore your Auditors will be looking for your organization to be fully 'signed up' to compliance and operating very much to the spirit of the policy, as well as to the letter.

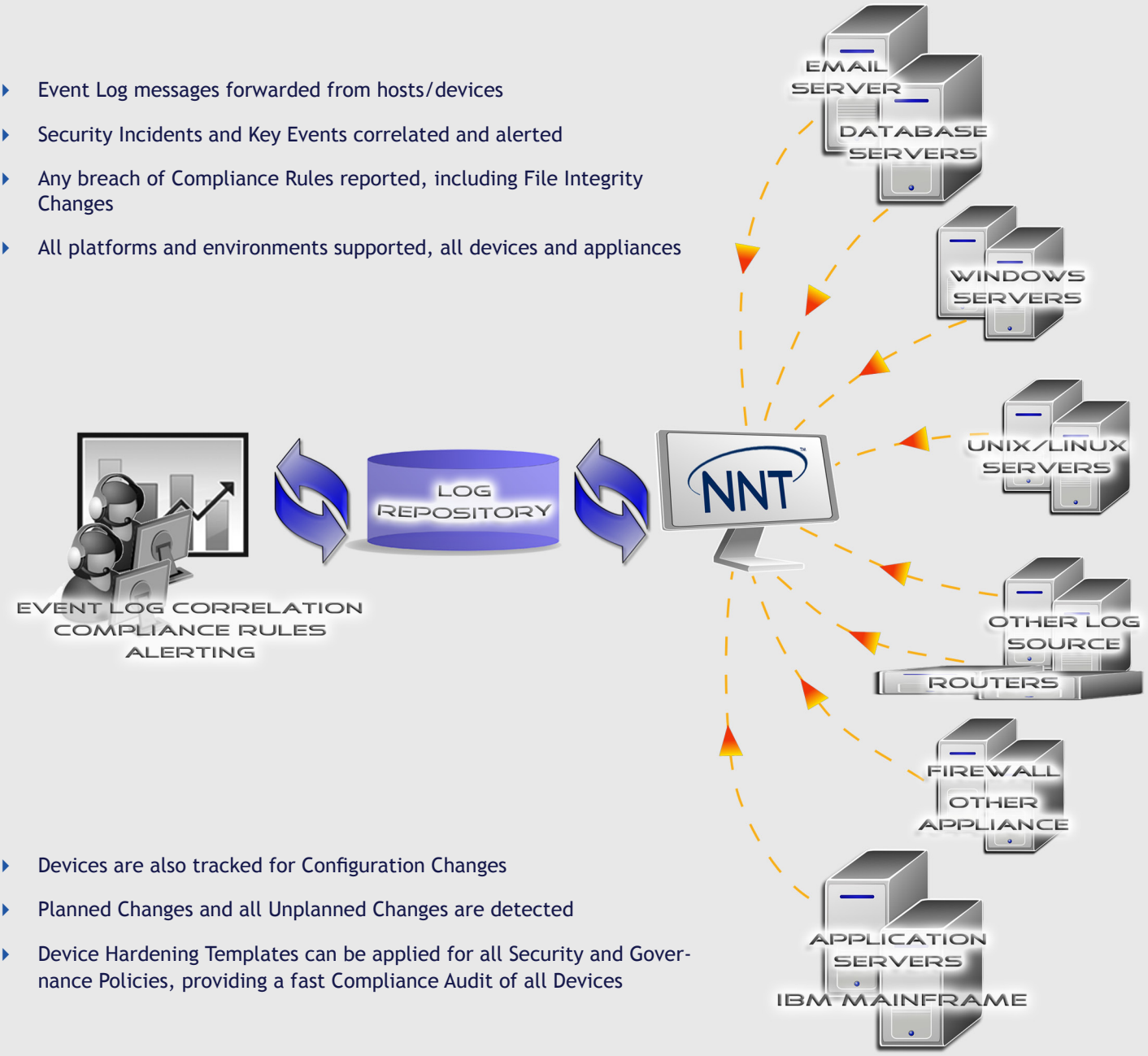
'In Service' Compliance Assessment – The Change Management Process

A key benefit to take from NNT Change Tracker Enterprise is that this is a system designed from an IT Operations standpoint. Devices being tracked for compliance are monitored continuously and are therefore constantly assessed for any deviations from their compliant state.

Of course, if nothing changes then your systems will remain compliant, but assuming you operate in the real world, then there will be near-constant change through software updates and patches, and the need to accommodate the incessant organizational demands for IT to support business growth and change.

What Do NNT Provide?

- Event Log messages forwarded from hosts/devices
- Security Incidents and Key Events correlated and alerted
- Any breach of Compliance Rules reported, including File Integrity Changes
- All platforms and environments supported, all devices and appliances



- Devices are also tracked for Configuration Changes
- Planned Changes and all Unplanned Changes are detected
- Device Hardening Templates can be applied for all Security and Governance Policies, providing a fast Compliance Audit of all Devices

Conclusion - The NNT View

In summary, the key message is that, whilst becoming compliant may be difficult enough, maintaining compliance is even harder. You need the right processes and procedures. You need the right infrastructure. You need a team who all understand and follow your processes at all times.

A lapse at any time could be enough to leave your organization non-compliant and exposed. Whenever we are providing consultancy to organizations with compliance standards to meet, we always remind them that the goal is not just to pass the audit – that is actually the easy part - because an Auditor will give you time to correct any deviations. The mindset required is that you need to be compliant for every minute of every day, because a hacker or malicious employee won't give you a second chance.

To this end, there is no alternative but to put in place an automated change tracking system that constantly audits all systems for configuration changes.

NNT PCI DSS Compliance solutions cover the following

- configuration hardening
- change management
- event log correlation
- file integrity monitoring

NNT Change Tracker and Log Tracker Enterprise - Compliance Clarified

- Audit Configuration Settings - The core function of NNT Change Tracker Enterprise is to first understand how your IT estate is configured
- Compare Audited Settings Against Policy - Configuration settings are assessed for compliance with any policy or standard relevant to your organization and deviations highlighted
- Continuously Monitor Configuration Settings - Configuration attributes are then monitored continuously for all changes, both from a compliance standpoint and from a general change management/control standpoint
- Change Management Process Underpinned - Authorized changes which have been approved via the formal change management process are reconciled with the original RFC to ensure the correct changes were implemented accurately
- The Change Management 'Safety Net' - All unplanned changes are flagged up for review immediately to mitigate security integrity or service delivery performance
- SIEM Event Log Correlation - Centralize and correlate event logs messages from all windows, unix/linux, firewall and IPS systems

TO REQUEST A FREE TRIAL OR DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT info@nntws.com

About NNT

NNT build the world's best solutions for tracking and managing change, managing and protecting users, maintaining system performance and ensuring availability across the entire enterprise.

Understanding and managing the day to day changes within your environment is critical to establishing and maintaining reliable service. NNT Solutions are affordable and easy to use.

NNT help you establish and maintain a 'known and compliant' state for your IT systems. Including: PC, Network, Software, Host Machine and Database.

www.nntws.com

UK Office - Spectrum House, Dunstable Road, Redbourn, AL3 7PR
Tel: +44 8456 585 005

US Office - 3000 Immokalee Rd, Suite 9, Naples, Florida, 34110
Tel: (Toll Free) 800 604 1746

Glossary of Compliance terms

Basel II - European oriented standards governing solvency levels of banks

Bill 198 - specific to Canada – governs integrity of financial reporting

CobiT - The IT Governance Institute's Control Objectives for Information and related Technology, a set of best practises in IT originated to help audit and develop an IT governance model for an organization's IT infrastructure

CoCo – Code of Connection, UK Government security standards and procedures for connections to the Government Secure Intranet

COSO – Acronym for Committee of Sponsoring Organizations of the Treadway Commission, a committee formed by a group of US accounting and auditing institutions to develop a framework for internal control and governance of financial reporting

GLBA - US originated legislation known as the Gramm-Leach-Bliley Act governs the formation of financial services conglomerates

GRC – acronym for Governance, Regulation, Compliance

HIPAA - US oriented standards based on the Health Insurance Portability and Accountability Act, within this context relates to the requirement to keep patient data private

ITIL – IT Infrastructure Library, widely accepted and implemented UK Government-originated framework of best practises in IT management and service delivery

NERC CIP - IT Security framework to support reliable operation of the Bulk Electric System used in the US and some Canadian provinces, designed to protect core IT control systems

MiFID - Markets in Financial Instruments Directive, wide-ranging financial instruments market governance requires detailed records to be retained for 5 years to prove 'best execution' of any trades

PCI DSS - Payment Card Industry Data Security Standard, originated by a consortium of payment card companies in response to the wide range of threats they had encountered within the market and as such have created one of the most broad and multi-dimensional security policies designed to protect cardholder details from misappropriation

SOX - US originated legislation as a response to WorldCom accounting scandal, the Sarbanes Oxley Act governs integrity of financial reporting and specifically makes company board members accountable for any irregularities