# How to Avoid a Compliance Nightmare

## An IT Security Leader's Story

NNT™
SECURITY THROUGH SYSTEM INTEGRITY

# Table of Contents



NNT™
SECURITY THROUGH SYSTEM INTEGRITY

# INTRODUCTION

It's getting to be that time. Audit season is just a few months away and you have over 3,000 assets about to be heavily scrutinized by the poker-faced external audit team, who might as well just show up wearing FBI jackets for the amount of tension they induce.

You're in charge of an IT estate that's failed to secure approval for the last two years and things are to the point now where if this shave gets any closer, it will be the sword of Damocles that provides it.

But it gets worse. The solution you currently have in house, the one that desperately needs addressing to correct the previously identified shortcomings, is performing terribly, and being poorly supported by the vendor. Now isn't that convenient!

You need File Integrity Monitoring (FIM) that works, systems configured to an acceptable benchmark, and critically, you need them all to stay that way with auditable proof that you're in control of all production changes made to your 'in scope systems'.

It's the stuff of nightmares….and likely a rabbit hole you've been down before.

Fortunately for you dear reader, this particular nightmare, while all based on real events, is at least for the time being restricted to the words contained herein. However, if this scenario feels in any way familiar, then please read on…

This scenario is precisely where Jerral Sapienza former Project Manager for a large corporation found himself in.

Jerral has been a leader in cybersecurity, security operations, and risk mitigation/compliance for more than two decades, working with Fortune 100 companies, B2B service organizations, and state and local government entities to build, maintain and document compliant, resilient IT operations running at the speed of business. He has also partnered with NNT to help many of these businesses streamline and simplify their compliance alignment and mitigation.

Having worked to get the prevailing solutions to a point where the delivery of the artifacts required to confidently address the looming audits would be achieved but consistently pulling up short. Jerral found himself in the unenviable position of having to decide whether to persevere or to admit defeat and look for an alternative solution.

In this instance, he decided not to continue to waste good money on products that have previously proven to underperform and elected to adopt a new solution to the problem, provided proudly by New Net Technologies (NNT).

> *We were delighted to have been selected to both replace a competitor and at the same time acquire a new customer, but nonetheless the size of the task was hard to ignore and the stress under which the team we were delivering to was under was palpable to say the least.*
>
> - Kirby Lott, VP of Sales at NNT.

What unfolded was a riveting story including a healthy mix of good process, careful consideration for the prioritization of task, user management, proper setting of expectations, blind fear, grit and determination, and ultimately a decent sized dose of 'hang on tight and don't look down'!

Here is a helpful Q&A transcript with Jerral Sapienza. For more information on this project or insight into effective cybersecurity provisioning, please visit our website at www.nntws.com

# MISTAKES MADE - LESSONS LEARNED

1

## Looking back on your experience, is there anything that you feel you could have done differently?

There will always be many things that could have been done differently... but "to do" items aren't always within our control. Wisdom is often one of the most usefully infectious methods of propagating support within projects. But participative wisdom isn't something we can parcel out and distribute or inoculate. It requires active buy-in from team members in the form of an innately driven desire to achieve the same outcome we're "selling".

So: What to do differently? Be ready for more of the pitfalls; be an active learner, capable of pivoting immediately to other options where required; invest less in being right and more in being successful over time; trust and believe your teams can succeed; plan; execute; track; repeat. Be willing to retrace your steps if necessary, but do everything in your power to gracefully move consistently and creatively forward so that you never have to!

### A few starter adages for motivation and insight:

- Success can be learned, but it cannot be taught.
- Give a team fishes & they eat for a day; teach a team to fish and they eat for a lifetime.
- The pain of planning is usually easier than the pain of failing: Fail to Plan = Plan to Fail.

- One can never know too many people: projects usually succeed not just through hard work and boots on the ground. Relationship and communication cannot be overstated.
- There is no substitute for Executive Sponsorship of your compliance project. Unless and until people at every level of an organization are aware how the project benefits their work, their salary, how they spend their time... they do not yet have the motivation to participate.
- Projects will almost always fail when people who don't know each other are tossed together, into a plan they have never seen, to accomplish an unspoken goal for a regulatory compliance framework they don't understand, using tools they have never touched. And yet, more than half of compliance projects running today probably fit most of this bill.

# EMBRACE THE POWER OF PROCESS

2

## How important to the success of this project was the creation of process and what if anything did that process contain?

**The process cannot be overstated. It is, in short, execution of the PLANNING phase. The process usually includes three basic parts:**

1. Step-by-step or summary guidance extracted from the plan, provided to team members.
2. Forms to document (and re-document interactively) success/gaps within the Plan.
3. Communication with the various teams, stakeholders, process owners, technicians involved in process collection via meeting agenda; email updates; status reporting; metrics.

Every company will have a different process, but there are commonalities within them all, including:

- Diagram / document the in-scope environment for the audit/assessment engagement
- Divide the environment into logical chunks to 'consume' over course of the engagement
- Create an inventory of in-scope assets (or refer to an existing CMDB, if available)
- Create a directory of people associated with various teams, divisions and assets

- Create a shared depository (SharePoint, file share, etc.) where assets are collected, tracked and reviewed
- Create intake/data collection and guidance documents to outline requirements, options, processes, and expectations from technical teams. This helps avoid having to say the same things multiple times, as you step through a group of assets to review, add, track.

*(Be willing and ready to update your forms with lessons learned as to how badly your form is misunderstood by people using it! Humility in the face of chaos is a good thing! : )*

- Create a communications roster to help streamline people connections and ensuring their valuable time is not wasted as you muddle through all the pieces (i.e. project plans; meeting times, list of meeting participants, meeting agenda, updates, reporting, metrics)
- Create three types of tracking documents as you progress through the assessment:

1. **General** tracking document shared with teams across the company
2. **Private** much more detailed tracking document you maintain with your private notes I.E: gaps; roadblocks; ways you'll attempt to overcome/tackle things next
3. **Auditor** tracking doc (designed so it can be shared with external auditors)

**Be very careful** *not to inadvertently share the wrong document with the wrong people, since doing so can cause political storms which can significantly set back your project with in-fighting and finger-pointing, not to mention damaging your trust and reputation!!*

## Suggestions for administratively enforcing the separation of documents:

- Use linked spreadsheets: The main source of entry will be the private view, a password-protected secure doc. Using the linking function, columns extracted from this sheet can then auto-populate the other two views into separate sheets for other purposes.
- Use Color coding within the master sheet: shade sensitive data private columns in light red/pink; Shade general comments in light green; shade auditor columns in light yellow. Carefully build doc links to export only the correct columns into each of the other views.
- When updating teams with the new information, do so by sending out URLs / LINKs to the updated docs, not sending the documents themselves through email. This allows you much greater control to make on-the-fly updates if you should notice you've got something wrong, or need to revoke or reformat and update entirely. Name the links accordingly. Private and Auditor views should be password protected (with separate passwords, of course). Depending on the sensitivity of data in the "General" view, it may also require a password to better control its distribution. Of course, NONE of these documents should under any circumstance be put on public internet sites. They should be on internal or intranet company-controlled IT file share depositories.

# THE LIGHT AT THE END OF THE TUNNEL

3

## What were the biggest challenges that you had to overcome in this project? As we now know, this story happens to be a positive one as audits were passed. What for you were the critical elements of success?

There is simply no substitute for a good Project Manager who knows the organization and knows how to plan, execute, and track. Probably the two most common challenges in any compliance project will be A) too short a timeline; and B) politics and turf wars where in-fighting, resource restrictions, and a general misunderstanding of the audit goals fester.

Both of these challenges can usually be overcome by ensuring senior management completely understands and supports the engagement, and by appointing a competent well-established project manager to oversee the project.

A timeline (tied closely with a work breakdown structure (WBS)) is essentially a logical arrangement of well-defined, ordered bite-sized chunks of project work that is assigned to people who can get the job done within the number of calendar days parceled out. It is very rare that a timeline is ever deemed sufficient by everyone on a project team. That's why we need a well-established and competent project manager to help ensure its sanity and order.

The best project managers thrive by making order out of chaos (and there is no shortage of chaos in a compliance project). But a PM can only thrive and succeed when they know the environment well, and, preferably, have some history with the technical teams and management involved. That way, a project manager will know who to prod (when and how firmly), and can repeat this cattle-drive/juggling act over and over again, for the duration of the project.

Politics and in-fighting at their core, are essentially fear and argumentation hormones oozing into social interaction (or lack thereof) when a group of people are tossed together to get a job done. The larger the company, the more inevitable that politics rears its head as a project stumbling block. But again, the most effective way to ensure politics doesn't impede or derail a project is to ensure your best available project manager can be assigned to the job. Project managers don't just thrive on chaos because they like to live in primordial goo. They thrive there to solve a puzzle and bring about a new flow and natural order.

A PM can best solve political in-fighting and turf wars by building on established relationships with the people involved, and/or applying their keen perceptive awareness of how people operate. PMs usually keep things moving by wheeling and dealing and tactfully nudging a project forward, artfully communicating a vision of common solution as in everyone's best interest.

Most politics/in-fighting can be nipped in the bud when the right people are kept on or kept off resource lists for a given project (choose your people carefully) and when a sufficiently high-level executive sponsor signs on and communicates vocal support for the project.

# TAKE A PAGE OUT OF MY BOOK

4

## What advice would you give to anyone faced with a similar dilemma?

The most basic advice for IT Teams taking on PCI, HIPAA, GDPR, NIST, FISMA, HiTech, or any other compliance mitigation woes is:

1. Don’t take shortcuts!
2. Don’t use inferior security tools.
3. Time is money.  Don’t waste either one going down the wrong path.
4. Commit upfront to ensure SPONSORSHIP, PLANNING, and PROCESS!!

Compliance projects take time and effort. But luckily you don’t have to re-invent the wheel.

You can save time, money, and effort by partnering with New Net Technologies (NNT) and using their amazing Change Tracker tool to take a massive weight off your shoulders when it comes to automating the asset compliance reporting process.

Change Tracker is designed to help your organization document the initial compliance baseline for all of your assets, and report on-going compliance status as devices continue to function in the real production world, subject to application, device, and O/S updates and changes along the way. It even knows how to ignore global recurring changes associated with O/S updates and planned changes that affect groups of assets.

Your objective should be to maximize your compliance effort by doing what you do best: You know your organization, people, business, applications, and customers. And let NNT do what it does best: change tracking, compliance reporting, and baseline change reporting within a sleek, friendly interface to access its powerful reporting capabilities.

When you commit to building the launch platform, Change Tracker takes off from there to help you fly high, successfully achieving your compliance goals for years to come.

## Here's what steps you will need to take to build that launch platform:

1. Executive Sponsorship of your compliance effort, communicating the company's need to reach this compliance milestone for technical teams, business owners, and customers alike.
2. Partner with the NNT Team to help design your NNT Change Tracker environment, based on the size of your organization and how many assets are in-scope for protection and reporting.
3. Organize a plan for stepping through compliance review and mitigation (NNT can provide a basic plan you can customize with your organization's specific details).
4. Document names, roles, contact info and time zone/location of management, technical owners, process owners, and business/compliance owners involved in your project.
5. Locate, build, and/or update network diagrams, application and architectural diagrams, device inventory, data flow diagrams of all assets in-scope for this compliance review. *Auditors require these diagrams, inventories, maps and data flows later in the process anyway. So, locating or building them early on gives you a head-start for later steps, while also providing working documents to improve planning and communication along the way.*
6. Take time to build some basic forms to use during your onboarding process. Having these in place and aligned with your process flow will keep things moving (NNT's Support Team can provide you with some basic starter forms you can then customize for your project).

NNT's Support Team can provide you with some basic starter forms that you can then customize your project, including:

- **Process overview document** to outline the basics of what is this compliance project, why it's happening; what are the basic steps of the process; estimated timeline of the steps; what information is required by each team; who is the technical contact to best assist.
- **Device inventory** for this team's devices. Things like O/S, device name, device role; device location; device interfaces; primary IP; other IP functions; Descriptive notes.
- **Status and Reporting forms** (Color-coded header bands: Red for internal-only; Green for general; Yellow for Auditors).
- **Recurring Meeting Agenda** to help organize communication delivery and discussion (depending on the intensity of scope at various stages in the project, different kinds of meetings may recur weekly, daily or on a periodic basis).
- **Change Tracker User Access forms** (guides you first to collect and document your company's security policy, to provide to teams requesting access, such that user access process remains compliant with security policy, re: request and approval process; AD or local accounts; username format; password format requirements; portal timeouts; account renewal and expiration, etc).
- **Device Role or O/S Baselines** (where applicable, your company may require certain device types or roles to be compliant with company minimum baseline requirements. Once collected, you can engage NNT Professional Services to work with you to create new NNT Change Tracker baseline templates to track devices matching baseline criteria. Note that out-of-the-box, NNT Change Tracker provides baseline templates for a variety of O/S and Compliance reporting; NNT's Support Team can create for you any custom templates you wish, matching requirements set forth within your organization's security policies).

# CONCLUSION

Costs associated with data security or privacy breach are real and substantial in today's interconnected networks, operating at the speed of business. Regulatory frameworks abound, with non-compliance very expensive. Steps we take to secure our networks and protect our customers' data matter.

One of the simplest, most cost-effective and efficient solutions available is to partner with NNT and their Change Tracker product to help ease the burden of compliance baseline tracking and reporting.

No compliance solution happens without some effort. But it doesn't have to be costly or complicated. I've outlined the actual steps we took to succeed, partnering with NNT and Change Tracker, significantly simplifying our overall compliance mitigation journey, and streamlining the effort to maximize value and productivity along the way.

You, too, can experience this same compliance success story when partnering with **NNT**!

# How NNT Helps with Continuous Compliance and Assurance

- Built-in compliance policies – Compliance policies and regulations change constantly. NNT has predefined policies that can be applied in a matter of seconds to determine if systems are in compliance
- Complete, Closed-Loop Compliance Automation – Automate the process of compliance validation and provide descriptive details on how to rectify if compliance drift has occurred
- Give management and auditors the confidence they need with reports that can be generated within minutes that show evidence of compliance testing, results and remediation
- Get total visibility into all changes and detect and validate changes – Track every change made across the IT environment and expose unauthorized changes through reconciliation with expected changes
- Reduce the cost of compliance with automation – Streamline the audit process by removing the need for internal audit staff to spend countless hours gathering evidence to present to external auditors with automation. By enabling workflow automation that monitors and tracks security risks, organizations know they are in compliance in real-time

*Continuous Compliance and Assurance* is an ongoing process of proactive risk management that delivers predictable, transparent, and cost-effective results to meet information security goals.

| NNT Capabilities | PCI-DSS | NERC CIP | SOX | HIPAA | NIST 800-53 | NIST 800-171 | CMMC | MAS TRM | IRS 107 | 20 CSC | COBIT | ISO 27001 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FIM (Intelligent Change Control) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Continuous Configuration Control | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Hardware & Software Asset Inventory | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vulnerability Assessment (Unlimited IPs) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Audit Log Analysis | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Remediation | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | | | | |

NNT™
SECURITY THROUGH SYSTEM INTEGRITY

## Contact us


US - (844) 898-8362, UK - 01582 287310

info@nntws.com

www.newnettechnologies.com


**Schedule a free consultation** **Request a Demo**