tripwire

WHITE PAPER

Nine Steps for Maturing Beyond Checkbox Compliance

Avoid Audit Fatigue with a Unified Compliance Strategy

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

A common mistake many organizations make is approaching cybersecurity as a series of actions taken in order to check the right compliance boxes. If this sounds familiar, it's likely that you've witnessed something similar to the cycle of crisis-driven audit preparation, a suspenseful audit, remediating based on those findings, and waiting until the next hurried audit preparation phase returns.

Security leaders are positioning themselves for a win when they aim to figure out a new, more effective approach to meeting their goals that goes beyond this disjointed compliance cycle and ultimately results in mitigating security risk more effectively.

By successfully executing these nine steps, you'll no longer continually have to react to and manage the audit preparation crisis du jour. Instead, you can institute and rely upon regular, defined activities to complete the heavy lifting of preparing for a successful audit long before it occurs. Completing the nine steps requires business stakeholders, IT management, and security teams to all mutually support the same goals.

Compliance is a Process, Not a Project

Trying to achieve and maintain compliance as a stand-alone project has a number of significant operational challenges, some of which can create a negative organization-wide impact. For example:

- Cybersecurity is often organized and designed to minimally interfere with business and IT operations, but this setup creates barriers to meeting compliance goals
- Although the security team is held accountable for the effectiveness of controls to meet compliance goals, the effectiveness of these controls relies upon other business and IT management to adequately prepare for and correctly interpret compliance audit requirements
- Security holds the accountability, but not the organizational authority to prioritize and execute design and implement the required IT controls
- Security often discovers too late that business and IT management were not as prepared for the audits as was represented, resulting in last-minute, emergency preparation work
- Business, IT and information security management must perform heroics to generate proof of compliance, often creating new documents and presentations from scratch in response to auditor questions
- The business may fail an audit test, requiring remediation work, audit retests, fines, loss of auditor confidence in your security program, and potential loss of personal trust in the security manager

Nine Steps to Building a Compliance Program that Works

The objective of these steps is to ensure that your entire organization's activity conforms to the expectations of industry auditors. This includes identifying organizational goals, classifying risks, implementing required controls, and being able to test those controls in an automated manner. And when compliance reports are generated well in advance of the audit, there's a far higher likelihood that there will be time to complete any needed remediation.

1. Align with the tone at the top

Ensure that compliance activity is clearly managed from the top down. Stakeholders at all levels need to understand the importance of compliance and be able to clearly communicate the risks of non-compliance to those they manage.

The goal of this step is to propose to organizational leaders a way to break the disjointed compliance cycle by placing more effective controls on the audit environment. Our challenge is to define and communicate what needs to be done in a way that is palatable for leaders to champion within the organization. After all, security teams can't succeed without support from management.

The first step in changing the audit control environment is helping IT leaders understand that they share accountability for security and compliance outcomes with their security managers. The next step is to reach agreement about the changes to the audit control environment that must be made.

2. Create a set of merged security and compliance goals

Document IT governance goals and risks to achieving them, and confirm that all appropriate teams do their part to help achieve them. In order for them to hold someone accountable, these goals must be stated in a way that's achievable, measurable and verifiable.

Document IT governance goals and risks to achieving them. In order for them to hold someone accountable, each of these goals must be stated in a way that

Nine Steps for a Unified Compliance Strategy

1. **Align with tone at the top**
2. **Create a set of merged security and compliance goals**
3. **Define ideal goal indicators**
4. **Understand your information flow**
5. **Agree on control ownership, roles and responsibilities**
6. **Define the control tests so business process control owners will agree with the results**
7. **Schedule and conduct regular control tests**
8. **Organize metrics and remediation reports**
9. **Detect and respond to significant changes to the control environment**

is achievable, measurable and verifiable. For a goal to be achievable, we must describe what an audit scenario looks like when the goal has been accomplished. We cannot simply state these goals as: "Achieve compliance with regulation XYZ." Instead, we state the risk and then state the information security goals required to mitigate it.

By creating this merged set of goals , the IT leaders will ideally support the next steps and will also recognize how security can closely support business compliance goals, help with the efficiency and effectiveness of operations, and assist in creating well-defined objectives.

3. Define ideal compliance goal indicators

Develop ideal indicators that demonstrate that your compliance goals are being met.

There are many different approaches to achieving the desired outcomes of any given business process control. However, some approaches require considerably more audit work than others to verify their effectiveness. In general, the more subjective judgment required by management, the more testing and sampling audits must do. Consequently, the goal here is to design controls to allow as much objective measurement as possible. Change and access controls can be designed to ensure audit preparation and testing are as efficient as possible.

In this approach, the business process owner agrees in advance on the method by which the correctness of the file contents should be determined, such as a series of automated tests that compare the authorized set of values for the attributes against the current set of values. Any discrepancies or exceptions let us know when unauthorized changes have been made.

4. Understand your information flow

Do an end-to-end business process walk-through to document where sensitive information enters and exits the organization, where it is stored, and where reliance is placed on technology to prevent and detect control failures.

In the previous step, we created ideal information security goal indicators, where we favored reliance on the measurement of information attributes instead of relying on administrative activity and supervisory controls. By specifying the required attributes, we gain an end-to-end view of information flow and can enforce accountability to specific outcomes rather than to a set of procedures and processes.

Conduct an end-to-end business process walk-through to understand and document:

- Where sensitive information enters, transits, is stored, and exits the organization
- Specific risks to organizational goals and information flow
- Where reliance is placed on technology to prevent and detect control failures

By constructing the end-to-end information flow through a business process, we often reveal business use of information on desktops and cloud computing environments. When we view information control requirements in the context of information flow, merely distinguishing between authorized and unauthorized access requests within a single application is insufficient.

5. Agree on control ownership, roles and responsibilities

Clearly define roles and responsibilities for audit compliance activities at the process-owner level.

Next, agree on or assign the process owner for each of these controls. These owners are responsible for implementing and regularly auditing, in an automated manner, each of the controls within their area of responsibility. The goal is for them to regularly review these automated audit reports and remediate issues as part of daily operations as opposed to scrambling to generate the reports before the auditors show up.

Once we identify each business process control owner, these owners must define a standard configuration for each of the IT assets he or she is responsible for in the information flow. This includes detailed descriptions and technical specifications of the software needed to safeguard information and detect potential intrusions. The standard configuration also includes file object attributes, configuration settings, encryption key configurations and other parameters used by management. Each standard configuration must be automatically monitored for deviations.

Go Faster with Better Brakes

Compliance controls are often seen as a hindrance—something that gets in the way of business and slows everything down. But think of it this way: As a control, what are the brakes on a car designed to do? Of course the default answer is that they're there to stop the car. But more accurately, the brakes are not there simply to stop the car but to allow it to go *faster*—safely. The same thing can be said of security and compliance controls: They aren't there to prevent you from doing business. Rather, they're there to allow you to do business securely.

6. Define control tests so process owners will agree with the results

Make sure that evidence that demonstrates compliance goals have been met can be generated in an automated manner on demand.

It's important to determine and take deviation measurements when configurations deviate from a known standard configuration. These deviation

measurements can be used to build a remediation task list, and any known deviations should be shared with auditors.

Why would we share this evidence with an auditor? It's true that disclosing this need for remediation can be used as evidence for audit findings. However, the audit report will likely note that remediation is in progress and that the percent of inventory that is out of compliance is being reduced by these remediation efforts. By disclosing this evidence, the audit will conclude with much less time and effort by IT staff than if the auditors had to devise information security tests to detect these deviations. By coordinating information security management and IT governance processes, IT does not need to spend any extra staff time to gather information for auditors to pass an audit.

7. Schedule and conduct regular control tests

Conduct tests of control effectiveness frequently enough to be able to rely on them regardless of variances in audit scope and timing.

Once security management and business process control owners agree that a given standard configuration provides adequate security and that configuration monitoring can be automated, these decisions must be validated with respect to actual practice.

The attribute measurements of the controls must be tested frequently enough to capture any changes to the standard configuration that would present risk to the information flow. In an environment that processes millions of transactions per minute, the time threshold within which vulnerabilities should be detected will be very short. In an environment that infrequently processes transactions of value, detection of an inadequate information security configuration may be performed less frequently.

8. Organize metrics and remediation reports

Track the completion of required remediation work, ideally to be completed well in advance of the audit.

Organizations have differing approaches to taking an information inventory. However, the information inventory is only complete if it includes the set of information inventory definitions that cover any area of the business that contains any type of information flow. Some organizations use their corporate business unit structure as the basis for the classification scheme of their information inventory. Other organizations may share so many IT services that it is more convenient to classify information inventory at the IT service level.

Each information inventory item may contain multiple information flows. For example, a single information inventory item may include alternative Internet-accessible options for data delivery, internal information flows for business processes, and other internal information flows for administrative use. Each of these should be defined in terms of the existing IT infrastructure as well as the roadmap that supports them.

9. Detect and respond to significant changes to the control environment

Gain the situational awareness to know when the information flow or control environment has significantly changed, requiring these steps to be redone.

Changes that impact information flow should pass through a higher level of review and may result in changes to the scope of the information flow. An environment in which control over information flows can be set at the organization level and audited on-demand allows automated monitoring of both access and configuration by process control owners, as described in Step 3.

Even in an organization where the accountability for compliance goals is well-defined and managed with metrics, process owner control over information flows continues to require scrutiny from a security perspective. This continued scrutiny is critical because any change to the configuration of any device within the information flow may put business goals at risk.

Moving from Crisis Management to Routine Preparation

Individually, each of the nine steps constitutes a compliance best practice. Collectively, these steps enable control over the end-to-end information flow in any given infrastructure. However, it is unrealistic to think that any given security manager has the time or resources to manually perform each step. The key to quickly and easily preparing for an audit is to determine which control activities are routinely used in compliance and information security audits, and to automate the management of tasks that make up those activities.

As security managers, if we execute Steps 1 through 9 and verify the effectiveness of our controls with a configuration control solution like Tripwire® Enterprise, audit preparation becomes a much easier process.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

WPMBCC1a 2005