

The Tripwire logo consists of the word "tripwire" in a white, lowercase, sans-serif font, set against a solid orange rounded rectangular background. A thin red line curves under the text.

TAKE CONTROL.

Managed Compliance

STREAMLINING MULTIPLE COMPLIANCE MANDATES
WITH VISIBILITY, INTELLIGENCE, AND AUTOMATION.

The text "WHITE PAPER" is in a white, uppercase, sans-serif font. To its right is a white circle with a vertical line extending upwards from the top of the circle, which then turns left and then down to form a bracket-like shape pointing towards the "Managed Compliance" text above.

Introduction

Any IT security and compliance professional would probably answer, “Yes,” to the following questions:

- Are your organization’s compliance costs out of control?
- Do you need solutions and practical advice to simplify and streamline compliance and security efforts?
- Do you face compliance with multiple compliance initiatives?
- Are you under pressure from more rigorous compliance requirements and more frequent audits?

They might not be able to answer this question, though: Do you understand the real intent of the numerous federal security compliance mandates, industry regulations and standards, and state data breach notification laws?

This paper discusses these important issues and provides IT security and compliance professionals a roadmap and practical advice for implementing an approach to compliance that helps overcome these issues.

Perfect Storm of Compliance and IT Security Demands

Companies today are up against the “perfect storm” when it comes to IT compliance and security. Cyber threats are more numerous, sophisticated and complex than ever. To protect against these threats, federal and state governments and industry groups continue to issue new regulations and data and system protection standards that companies must adhere to. In addition, existing regulations and standards continue undergoing updates, which typically make compliance requirements more prescriptive and rigorous. Simply enough, all companies face more risk, and as a result, they now have more compliance activities to manage. For many, this perfect storm feels impossible to ride out—it’s too expensive, it’s never-ending, and the requirements are complicated to understand and implement.

To weather this perfect storm, companies will need to implement automated security solutions; adopt and update policies, procedures, and manual security practices; and successfully navigate the numerous security and internal control requirements included in the multiple laws and regulations they’re subject to.

A Brief History of Major IT Compliance Regulations and Standards in the US and Other Countries

US federal regulations started the major trend in IT compliance, with the introduction of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), designed to ensure that the health care industry protects patient data. In 1999, the Gramm-Leach-Bliley Act (GLBA) was enacted to ensure that financial institutions secure sensitive customer data. Next came the Federal Information Security Management Act of 2002 (FISMA) to protect sensitive data in government agencies. That same year, Sarbanes-Oxley (SOX) was enacted, specifying internal controls publicly traded companies must have in place to prevent accounting fraud.

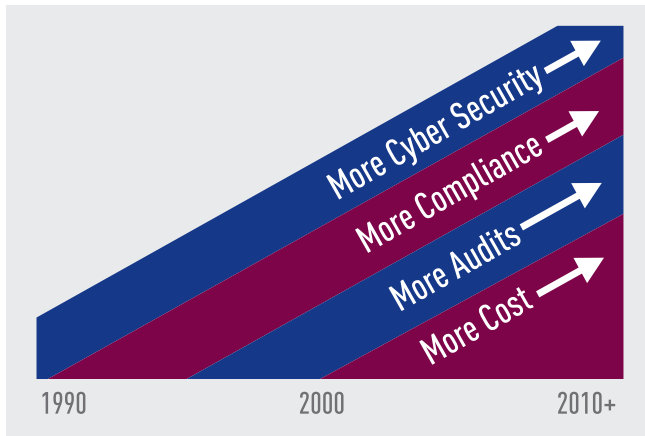
In 2004, the major card brands released the Payment Card Industry Data Security Standard (PCI DSS) for companies that handle credit or debit card data. This law extends well beyond the boundaries of the US, impacting any entity that captures, transmits or stores credit card data.

More recently, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 specified new privacy and security mandates for health care organizations. And over 46 states have enacted state data breach notification laws for all companies that collect consumer information that is not publicly available.

Other countries have experienced a similar surge in major IT compliance mandates; for example:

- European Union Data Protection Directive in 1995;
- United Kingdom Data Protection Act in 1998 and Financial Services and Markets Act 2000;
- Canadian Government Operation Security Standard: Management of Information Technology Security (MITS) of 2004;
- Financial Instruments and Exchange Law in 2006 (AKA FIEL or JSOX) in Japan; and

- International Organization for Standardization (ISO) 27002, originally referred to as ISO 17799, was subsequently renumbered ISO/IEC 27002:2005 in July 2007 to bring its name into line with the other ISO 27000-series standards. The standard is entitled Information technology—Security techniques—Code of Practice for Information Security Management.



The Future of IT Compliance Regulations and Standards

The cyber threats that these laws, regulations, and standards are intended to address are real and can have an immediate and significant effect on the company. As a result, these compliance mandates are not going away; in fact, Congress has several new bills pending¹ that add to these existing mandates. If enacted, these new bills will require all companies to:

- Increase their security focus;
- Undergo more frequent and prescriptive compliance and security audits;
- Use only licensed and certified security professionals in IT security and compliance efforts; and
- Adopt automated and continuous monitoring of controls to detect, report, respond to, contain, and mitigate security incidents.

A More Challenging Environment for Compliance

A number of factors have combined to make the compliance environment even more challenging. Security compliance mandates are getting more prescriptive and harder to meet. For example, the HITECH Act strengthens the civil and criminal enforcement of HIPAA rules and adds new mandates for encryption and access controls. Similarly, version 2.0 of the PCI DSS adds more emphasis on encryption and locating cardholder data.

In addition, the IT infrastructure and operating environment is getting more complex, with many implementing virtualization, cloud computing, mobility, wireless, and other newer technologies. At the same time, the adversaries who attack this more complex technology environment have become more sophisticated and polished in their attack methods. For example, patient adversaries may make minor changes over a long period to minimize their visibility while eventually opening a security hole. They may also erase data to cover their tracks.

Budgets and time present further challenges. Companies now spend significant capital or operating budget on risk management, security and compliance. Typically, this expenditure is on equipment and software, personnel, and facilities; continuing education on security and technology for personnel and consultants; and time staying informed on current security regulations and standards and the cyber threats they address.

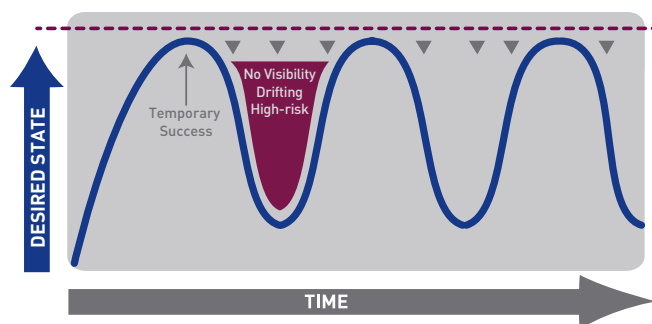
Yet in this environment where budgets are spent on compliance and security related activities, most companies:

- Face shrinking or flat budgets;
- Have limited security or compliance expertise;
- Undergo more rigorous and frequent audits; and
- Risk experiencing security events, fines, and other negative financial impacts.

Different Approaches to Compliance

Traditionally, companies take a “check box” approach to compliance that provides assurance of compliance and security for a single point in time by conducting periodic, mostly manual assessments. This approach may be effective for meeting some compliance objectives and even passing an audit; however, it is time consuming, resource-intensive, and fails to address the inevitability that changes and security events occur between audits. This approach can’t help companies achieve a continuous known and trusted state and provides a false sense of security. The increasing compliance demands and security threats only serve to magnify these issues.

TRADITIONAL METHOD

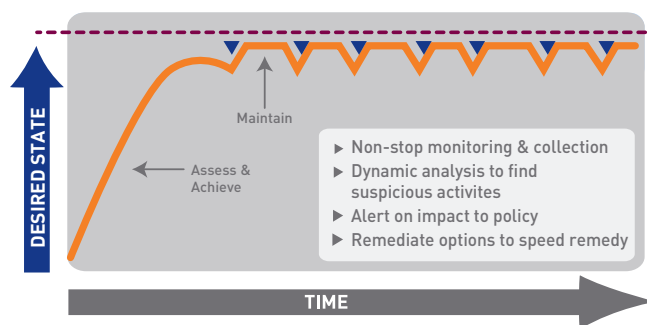


(Fig. 1) Traditional, periodic assessment approach to compliance.

But even if these solutions did capture data about changes and security events between audits, a company can experience millions if not billions of change and security events a day. Realistically, no IT organization could sift through these events to determine which event or combination of events may represent a threat to data or systems. Without this ability to distinguish good or benign change from a potential threat, all that data just generates a lot of noise, and companies can only react to issues after they discover them—typically after damage has already occurred.

‘KNOW-NOW’ REAL-TIME METHOD

To avoid this reactive mode, organizations need an intelligent, automated solution that provides visibility to activity on the entire IT infrastructure, helps manage compliance across multiple mandates, detects events of interest that are outside the established norm, and manages change at the device level and for the entire IT infrastructure. And they need this information as the events occur, with minimal manual effort.



(Fig. 2) Know-now, real-time approach to compliance.

A PRUDENT MANAGED COMPLIANCE PROGRAM WILL HELP THE COMPANY TO:

- Proactively identify and assess risks
- Implement appropriate cost-effective controls
- Self-assess compliance with applicable compliance mandates
- Know when legal and regulatory updates occur
- Provide meaningful reports to the board, executive management, and auditors on compliance status

By implementing these managed compliance best practices, companies can more effectively mitigate risk to critical information and systems, fulfill multiple compliance requirements, and ensure that their risk management expenditures are more closely aligned with their actual vulnerabilities. In short, they evolve beyond a check box compliance validation strategy to a continuous compliance culture of performance that meets the true intent of compliance—real-time security and risk management.

Managed Compliance: A Practical Approach

Not long ago the world of IT security and compliance was delegated to one person or a small group of technology or compliance staff in the back office. Clearly compliance is no longer a back-office responsibility, and the cost of compliance—and noncompliance—is too great to ignore. Companies need to take a smarter, simpler, and more cost-effective alternative to the current approach to compliance: Managed Compliance.

Aligning the right people, processes, and technology to establish visibility, intelligence, and automation allows companies to adopt a successful managed compliance strategy. Managed compliance provides this blend of the right people and processes with a culture of continuous “know-now” security and risk management

BENEFITS FROM USING THE RIGHT AUTOMATED COMPLIANCE SOLUTION WITH MANAGED COMPLIANCE

- Ensures decision-makers are well informed.
- Establishes appropriate policies and procedures that govern employee behavior related to compliance and information security.
- Discovers, enforces, and addresses behavioral and compliance shortcomings.
- Provides just-in-time audit and forensics compliance and security event data.
- Manages change over time including changes in compliance mandates, changes in staff, changes in the IT environment, and changes in the nature of present threats.
- Identifies unauthorized configurations and other conditions that increase the risk of intrusion or other security events by monitoring host and network conditions.
- Helps assure a continuous state of compliance and provides situational awareness and security needed for control of the IT infrastructure by deploying intelligent log management, security event management, and configuration management solutions.
- Accurately and quickly identifies, classifies, escalates, reports, and guides responses to vulnerabilities and security events by analyzing the results of monitoring.

When done right, a managed compliance strategy simplifies compliance and audit efforts and creates a more secure environment. It also helps decision-makers go beyond a check box compliance strategy to meet the true intent of the compliance mandates—to protect sensitive data and critical systems. In addition, managed compliance allows companies to reduce the overall cost of compliance activities while increasing security.

The end result is an ongoing process of IT auditing and resolution that maintains the kind of stable, trustworthy operations required by today’s businesses, regulators, auditors, and customers.

Getting Started with Managed Compliance

Most organizations struggle with how to begin their managed compliance initiative. The most successful approach tends to be one that is simple and cost-effective. When starting a managed compliance initiative, organizations should consider the following five steps.

STEP 1. OBTAIN SECURITY AND COMPLIANCE BEST PRACTICE EXPERTISE AND RESOURCES.

Expertise and resources are important. Organizations need to leverage in-house personnel and resources, hire, or contract for the necessary experience. Many smaller and mid-sized organizations have little security and compliance experience or expertise, which puts them in the unfortunate position of having to get up to speed before planning and executing the compliance initiative. Tapping into the existing domain expertise of an outside resource is one solution. In addition to helping with the planning and tactical execution of the risk management activities, an outside resource also provides the credibility and “political independence” necessary to drive real cultural change across the entire organization.

STEP 2. QUANTIFY THE EFFECT OF COMPLIANCE AND EACH SECURITY EVENT.

Quantifying the effect of compliance and a security event on your company's operations, reputation, and brand; customer trust and loyalty; legal exposure (e.g., enforcement, civil money penalties and other fines); and financial gain or loss is critical. Quantifying these effects helps prioritize risks, identify risk that may create a competitive advantage or disadvantage, and determine the cost versus benefit of possible controls.

STEP 3. COST-EFFECTIVELY BUILD A SECURITY AND COMPLIANCE MANAGEMENT PROGRAM.

The size of the investment in security and compliance does not guarantee success. The organization's executive team must agree upon a company-wide security and compliance strategy and prioritize the most critical areas of risk. Once this occurs, the organization can execute a phased roll out of its managed compliance program. This phased rollout allows adoption of a risk-based budget approach and funding the managed compliance activities over time, not as a large up-front capital expenditure.

STEP 4. ADDRESS SPECIFIC AND IMMEDIATE SHORT-TERM RISK.

Addressing these risks enables the organization to perfect its managed compliance approach, while gaining valuable results. Once the organization is confident it has the right resources, expertise, and management support for funding, it can tackle the other critical risk areas to:

- Document risks;
- Identify critical IT functions;
- Implement risk-based and cost-effective controls;
- Monitor controls and remediate gaps in control effectiveness;
- Analyze and report on security and compliance status; and
- Audit effectiveness of controls and compliance.

STEP 5. AUTOMATE AND STANDARDIZE BEST PRACTICES FOR MANAGED COMPLIANCE.

Technology solutions can add significant value to jumpstarting successful initiatives for managed compliance with:

- Comprehensive knowledge of specific types of risks, probabilities, and severities;
- Automatic updates that account for changes in the cyber threat and compliance landscape;
- Analysis of common cyber risks and compliance issues across business units or other critical areas;
- Policies to guide upper management and employees.
- Controls and vulnerability management; and
- Automated monitoring, alerting, and reporting.

Successful managed compliance requires all business units to work together while replacing the traditional manual audit processes and operations with strategic partners and experience, automated solutions, and prudent practices for security and compliance. Once a company adopts these recommended practices, it is positioned favorably for its next audit and can ensure continuous security of its infrastructure and data while complying with multiple compliance mandates.

To ensure these changes take place smoothly, all companies must make a shift in the organizational culture so that:

- Management has visibility across the network from the device level to the entire business unit level to know what risk must be managed;
- Security personnel are armed with the intelligence to identify real and material threats from an ocean of "business-as-usual" activities; and
- Automated capabilities are deployed to enable a proactive response to threats with continuous:
 - o Monitoring
 - o Analysis
 - o Risk identification and mitigation
 - o Alerting of material events
 - o Response
 - o Assurance of system and data integrity and reliability
 - o Remediation

Where to Go From Here

Implementing a managed compliance approach that includes automated solutions that provide the necessary visibility, intelligence and automation to succeed in this approach can give organizations a way to weather out today's perfect storm of compliance and cyber threats. To help organizations review solutions that support Step 5, this paper includes a simple due diligence checklist that organizations should consider. Whether an organization is exploring how to leverage the right technology to help comply with the increasing requirements and cost of security compliance mandates, or is simply planning to replace an outdated manual process with more visibility, intelligence and automated capabilities, these questions can serve as a quick reference guide.

HOW DOES YOUR COMPANY APPROACH COMPLIANCE TODAY?

Do you:

- Have to comply with multiple security compliance mandates?
- Perform annual (or less frequent) point-in-time audits?
- Use automated audit and reporting tools?
- Have visibility across your infrastructure to know what is happening at all times?
- Have intelligence to know which changes or events are suspect and may put your infrastructure and data at risk of compromise?
- Use automation to help categorize high-risk changes and events, remediate certain conditions, and meet compliance reporting requirements?

About ReymannGroup, Inc.

ReymannGroup, Inc. provides finance, healthcare, energy, retail and manufacturing, and local and state government subject-matter expertise. The firm helps companies evaluate their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with legal and regulatory requirements. ReymannGroup provides customers with independent, highly qualified professionals, authors of regulations and books, and subject matter experts familiar with industry regulations and best practices. For more information, please visit www.reymanngroup.com and www.verticalenabler.com.

¹ Example bills pending include: Cyber Security Act; Cyber Enhancement Act; Information and Communications Enhancement Act or (ICE) Act (AKA, FISMA II); Data Breach Notification Act; and Data Accountability and Trust Act or (DATA).

Due Diligence Checklist

1. HOW AUTOMATED IS THE SOLUTION?

- Is it an automated compliance solution?
- What additional manual effort is required?
- Does it look for changes and events throughout the entire infrastructure, all network and end-point devices, operating systems, applications, and databases?
- Will it identify and evaluate configuration changes against policies to “know-now”:
 - » Are you still within policy?
 - » Was the change authorized?
 - » Are you compliant and secure?
- Does it generate out-of-the-box policies for critical regulations and standards such as HIPAA, PCI DSS, GLBA, CIP Cyber Security Standards, SOX, and ISO? This is an important step to help you cost-effectively report on compliance and establish a central set of IT controls. These out-of-the-box policies should apply to both physical and virtual environments and include frequent updates and configuration assessments. This immediate “know-now” security and compliance capability will help you to harden the IT systems and make achieving, maintaining, and providing proof of continuous compliance and security easy.

2. HOW INTELLIGENT IS THE SOLUTION, E.G., HOW WILL IT:

- Distinguish a “material change” (e.g., compromising your security & compliance) that requires immediate attention from business-as-usual changes?
- Address all security compliance frameworks (e.g., HIPAA, GLBA, PCI DSS, CIP, SOX, etc)?
- Securely record a history of IT changes to enable:
 - » Audit preparedness and regulatory compliance?
 - » Improved security by alerting key personnel when anything changes on vital information systems?
 - » Single points of control to provide visibility across the entire information infrastructure to quickly identify, diagnose, and verify changes, as well as restore systems to a “known and trusted” state, if necessary?
 - » Respond rapidly to alert on and remediate a material incident such as system disruption from an unauthorized change?
 - » Reporting on errors, performance problems, fraud, and forensic information to management?
- Proactively assess current configuration settings against established internal policies and external industry benchmarks such as the Center for Internet Security (CIS)?² By assessing an IT configuration against a policy, IT learns what settings are compliant and what are not.
- Detect all changes? Once the organization achieves a known and trusted state, you must maintain it. Companies need intelligent solutions to detect all change across the entire IT infrastructure—applications, databases, servers, active directories, virtual environments, middleware and network devices—and alert IT to any unauthorized or non-compliant change.
- Establish step-by-step remediation to get out-of-compliance configurations into a compliant state? You should be able to continuously address vulnerabilities one-by-one across the network and virtual environments until your organization moves into a known and trusted state.
- Provide intelligent visibility of the appropriate log data from across the network to monitor for material security events?

3. HOW IMMEDIATE IS THE NOTIFICATION TIME WHEN A MATERIAL CHANGE IS DETECTED? YOU ARE LOOKING FOR A “KNOW-NOW” CAPABILITY.

ABOUT TRIPWIRE

Tripwire is a leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Thousands of customers rely on Tripwire's integrated solutions to help protect sensitive data, prove compliance and prevent outages. Tripwire® VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and security event management solutions, is the way organizations can proactively achieve continuous compliance, mitigate risk and improve operational control through Visibility, Intelligence and Automation. Learn more at www.tripwire.com and @TripwireInc on Twitter.

