WHITEPAPER: FORTIFY COMPLIANCE

The Benefits of Compliance Automation

Paul Duval, CISSP
Compliance Specialist
Prevalent Networks

PREVALENT networks

1. Executive Summary

This paper highlights some of the compliance challenges that various organizations face as well as the best practices for rising to those challenges.

Compliance to the multitude of new and ever-changing external regulations as well as internal policies or control objectives can be a burdensome and expensive process, often fraught with inconsistency, redundancy, manual errors or undetected gaps. This is further complicated by the expanse of IT systems and electronic data that must be accounted for and protected. Additionally, IT resources are typically pulled away too frequently from their primary activities to measure or validate compliance in their environments.

The IT compliance panorama has expanded over the last several years in terms of breadth and organizational involvement and more companies are embedding GRC - Governance, Risk Management and Compliance - within their business functions and are looking for the best risk and compliance software products to assist them. [1]

As compliance to federal regulations, best-practice frameworks, or internal policies or standards is not a one-time process, automating the process establishes a foundation for ongoing compliance, and provides best-practice to ensure a company's processes, information; reputation and bottom line are protected and enhanced.

[1] In February, 2008, Gartner Research published a report titled "Critical Capabilities for IT GRCM Tools" in which they assessed various risk and compliance management software tools, such as Symantec's Control Compliance Suite, CCS. They were scored based upon their ability to meet critical capabilities such as controls and policy mapping, IT controls self-assessment, automated computer controls and mapping, IT compliance dashboards, and IT risk assessment in three use-case scenarios: Self-Assessment, Audit Support, and Automated General Computer Controls. www.gartner.com Report ID: G00155061

2. Regulatory Compliance Landscape

Until recently, IT compliance had typically been a self-imposed, internal IT function to ensure that systems were configured or patched properly. Now, IT compliance is often driven by external regulations and requirements for companies to demonstrate effective processes and controls across a broad range of areas. They must assess and show that they practice due care, adhere to strong security and technology controls practices, and protect their own information as well as that of their customers.

Additionally, many organizations must also demonstrate compliance to not one, but multiple regulations, with varying degrees of either redundancy or subtle distinction. For example, a public healthcare company might be regulated by Sarbanes-Oxley (SOX), Health Insurance Portability & Accountability Act (HIPAA), and Payment Card Industry (PCI).

There are also other drivers for compliance, beyond regulatory requirements. Some companies might not be regulated, but want to ensure they follow best-practice frameworks for their IT organization and security, such as CobIT (Control Objectives for IT) or the International Organization for Standardization (ISO). Others might simply want to improve security or ensure alignment with their own policies and standards. Some may have seen a competitor or similar company in recent headlines concerning a data breach or security event and want to strengthen their own controls so as not to suffer a similar impact to their reputation.

Below is just a sampling of regulations and their associated industries:

Sample Regulations	Targeted Industry
PCI DSS	All merchants who accept payment cards (including online, mail, and phone orders) need to comply with the Payment Card Industry Data Security Standard.
FISMA	The Federal Information Security Management Act of 2002 requires federal agencies to provide information security for their information technology assets.
SOX	The Sarbanes-Oxley Act of 2002 requires public companies to implement controls to safeguard financial data.
GLBA	The Gramm Leach Bliley Act requires IT controls for financial companies to keep customer financial information private and confidential.
HIPAA	The Health Insurance Portability and Accountability Act of 1996. Regulates the security and privacy of patient records and other health information.
COPPA	The Children's On-line Privacy Protection Act requires companies with general-audience Web sites – who collect data from children to implement safeguards.

Whatever the drivers for compliance may be, there can be many challenges with implementing it and doing it well.

3. Challenges and Pitfalls

Keeping up with new regulations (whether newly enacted or updates to existing) and demonstrating compliance to them is a challenging and costly process for most organizations. There are ever-growing numbers of regulations & mandates which lead to increased costs and complexity for covered organizations. New technologies or solutions can lead to new exposures, vulnerabilities and threats. These threats in turn lead to new laws, then new regulations, and eventually new policies within an organization. This all leads to new compliance requirements and additional costs to ensure them.

In many organizations, risk and compliance are managed as separate activities. Without an integrated approach to understanding an organization's risk and compliance objectives together, there can be a gap between what the risks are to the organization and what compliance is actually doing to reduce those risks.

In many organizations, IT is often called upon to handle compliance tasks and IT resources are pulled away from their core responsibilities, which can result in compromise of service levels or support of IT within an organization. This can be especially arduous when trying to demonstrate compliance to multiple regulations via several audits throughout a given year.

Some companies opt to develop their own in-house solutions to manage compliance. These usually end up with simplistic databases, voluminous collections of spreadsheets, and weak reporting capabilities. Such solutions essentially rely on manual methods, ad-hoc reviews and lack of consistent approach across departments within a business. This makes information gathering difficult and time consuming and leads to incomplete or inconsistent results. Reconciling results from multiple areas and systems can also be burdensome and error-prone and often cannot give management timely and accurate visibility into IT compliance status and clarity for next steps and monitoring progress towards improving results.

As a result of these challenges, one of the biggest pitfalls to compliance is that many organizations treat compliance as a one-time event or exercise and perform it only once or at a very limited frequency. As compliance can be a complex, de-centralized, time consuming process, most companies do not gauge their compliance with enough, or any, frequency. Increasing the frequency of audits or checks has been shown to dramatically improve compliance results, reduce risk and improve a company's profitability. In fact, the most recent research conducted by the IT Policy Compliance Group shows that improvements to data protection and compliance are paying big dividends among firms with the most mature governance, risk management, and compliance management practices and increasing the frequency of audits or checks has a direct effect on improving results. [2]

[2] The May 2008 Annual Report on IT Governance, Risk and Compliance demonstrates that those firms with mature compliance practices had consistently higher revenues than all other firms; much higher profits than all others; better customer retention rates; dramatically lower financial risks and losses from the loss or theft of customer data; significantly reduced financial impact from business disruptions caused by IT disruptions; and much lower spending on regulatory audit. www.ITpolicycompliance.com

4. Benefits of Automation

Research has shown that those organizations that conduct more frequent compliance checks or audits have the best security and compliance results [3] and the best way to conduct frequent assessments is through the use of an automated toolset. Using an automated solution not only reduces the time it takes to conduct compliance assessments, it provides management with more visibility and control of their IT assets and compliance posture and affords continuous monitoring of an organization's compliance posture.

The best automation tools delineate the various regulations or frameworks and their associated control statements to allow companies to map their policies or control objectives – providing a clear landscape for the company to identify and proactively control its compliance.

Automation tools can also provide hundreds of pre-defined standards with which to evaluate systems against controls in specific regulations and frameworks. The ability to schedule and perform automated checks for server configuration settings as they specifically apply to Sarbanes-Oxley, for example, is powerful and immediately valuable.

Running automated, scheduled checks of systems:

- ✓ Saves time, avoiding lengthy manual checks of individual servers to a plethora of configuration settings.
- ✓ Saves money, reducing costs by providing one solution for compliance to multiple regulations, frameworks or standards rather than separate, one-off initiatives thereby reducing redundant assessment efforts and eliminating unnecessary controls.
- ✓ Provides consistency – ensuring all systems are evaluated against the same standards in a repeatable and measurable way.

Additionally, automated compliance solutions can enable non-IT personnel to conduct technical and non-technical checks of controls to standards – keeping precious IT resources where they need to be.

Automated compliance solutions can also assist with non-technical checks, and can automate self-assessments for non-programmatic areas that traditionally have relied on paper-based solutions such as:

- The creation and dissemination of corporate policies or mandates
- Creating on-line questionnaires and workflows to measure acceptance of polices and standards
- Assign risk-based weighting to questions and responses to properly identify and handle risk

[3] Ibid.

5. Conclusions

Using automated tools and the right personnel, compliance can provide a sustainable and well-documented path to ensuring a well-controlled and secure environment, which in turn can reduce risks and complexity, protect an organization's reputation and make it more profitable.

Automation Benefits:

- Enables high-frequency of audits/checks to sustain compliance.
- One solution to manage compliance to multiple regulations, frameworks, standards or policies.
- Reallocate resources effectively and reduce time required to validate compliance.
- Ensure consistent checks and results.
- Provides visibility into IT compliance posture.

Prevalent Networks recommends implementing risk and compliance software offerings that can provide the following:

- Map an organization's control statements to policies, frameworks and regulations.
- Publish policies and gather evidence of acceptance.
- Identify gaps and manage exceptions to policies.
- Conduct risk assessments for technical and non-technical aspects
- Identify systems and run automated technical checks of standards against them.
- Readily identify and manage user entitlements to system resources.
- Provide compliance dashboards and reports.

Automating compliance is a business enabler, which reduces time and resources; maps to internal and external regulations and standards; streamlines the complexity of compliance monitoring and ensures effective and continuous controls over an organization's technology assets and practices.

[Fortify] Compliance

[Fortify] Compliance is a methodology designed by Prevalent Networks to deploy and support Symantec's Control Compliance Suite (CCS). Prevalent Networks has worked closely with Symantec to create the [Fortify] Compliance methodology to help ensure project success.

To receive additional information regarding how [Fortify] Compliance by Prevalent Networks, can benefit your organization, Please contact your dedicated Prevalent Networks account manager. Call us at 877-PREVALENT (773-8253).