QUALYS®

WHITE PAPER

OPERATIONALIZING SECURITY & POLICY COMPLIANCE

A Unified Approach for IT, Audit and Operation Teams

Table of Contents

ON DEMAND SECURITY

Five Major Priorities for Information Security

Based on its latest survey and the results from previous years, Ernst & Young has identified five major priorities for information security where progress has been made, but where there is an ongoing need for continuous improvement. These are:

- ***Integrating information security with the organization:*** embedding information security into the mainstream of the business with increased visibility and resources.
- ***Extending the impact of compliance:*** shifting attitudes from compliance as a distraction to being an enabler, bringing advances in risk-based security for organizations.
- ***Managing the risk of third party relationships:*** recognizing the challenges, issues and actions needed to manage the risks with global suppliers and outsourced partners.
- ***Focusing on privacy and personal data protection:*** taking a proactive and comprehensive approach to mitigating the risks related to privacy and personal data protection.
- ***Designing and building information security:*** using externally imposed compliance deadlines and security incidents as a catalyst for proactive investments in stronger capabilities and defenses.

Ernst &Young
"Compliance Pays Off in Information Security," as reported by Scoop Independent News

I. Overview

At the heart of all data transactions is a trust between buyer and seller, employer and employee, corporation and shareholder. We trust that the relationship between the owners of personal data, the corporations that hold it in custody, will be protected—that data will not be manipulated, given to, or taken by unauthorized third parties.

In a recent article entitled Information Security: The Stealth Fiduciary Obligation, author Al Krachman suggests that "directors and officers have a fiduciary duty to maintain the highest standards of information security for their companies, and that security failures of a material nature may not only be actionable by shareholders, but also reportable events for certain public companies."

Unfortunately, intentional or not, that trust is violated when information is lost, compromised or manipulated. The complexities of our data relationships make the risk of this happening very high and in some instances, due to the notoriety of the incident, regulatory mandates have been put in place to ensure that corporations take a more active role in maintaining the fiduciary responsibility for data entrusted to them.

What follows is a detailed discussion of the internal and external regulatory challenges now faced by organizations, the scope of these challenges, and of the ways in which they can be addressed through better business processes and automation. The solution proposed allows organizations to raise the bar with regard to data security, while adding needed efficiencies to current processes.

II. A Proliferation of Regulatory Challenges

Compliance with regulatory mandates and internal security policies is critical to the success of any enterprise. The past decade has seen an unprecedented wave of scandals that have destroyed entire enterprises, leaving customers, shareholders and employees holding the bag. Because information access is now ubiquitous, sensitive corporate and personal information must be protected and prevented from falling into the wrong hands.

To prevent repeated corporate scandals, protect the integrity of enterprise-owned information and ensure customer privacy, new laws and regulations have emerged governing a variety of enterprises. Some of today's most prominent security mandates include:

SOX – The Sarbanes-Oxley Act of 2002 requires strict internal controls and independent auditing of financial information as a proactive defense against fraud—with potentially serious civil and criminal penalties for noncompliance.

HIPAA – The Health Information Portability and Accountability Act of 1996 requires tight controls over handling of and access to medical information to protect patient privacy

GLB – The Gramm-Leach-Bliley Act of 1999 requires financial institutions to create, document and continuously audit security procedures to protect the nonpublic personal information of their clients, including precautions to prevent unauthorized electronic access.

NIST SP 800-53 – National Institute of Standards and Technology Special Publication 800-53 defines management, operational and technical security controls for the information systems used by U.S. federal agencies, including guidelines within 17 different control areas to protect the confidentiality, integrity and availability of systems and the information they host.

California SB 1386 – Known as the Security Breach Information Act, this state law governs organizations that serve customers residing in California and store confidential data about those customers on computers, or transmit such data over networks. The law requires proactive protection of private data for Californians, and provides a model for electronic privacy legislation that has been enacted in 30 other states.

UK Data Protection Act of 1998 – The eight principles of the Data Protection Act state that all data must be processed fairly and lawfully; obtained and used only for specified and lawful purposes; adequate, relevant and not excessive; accurate, and where necessary, kept up to date; kept for no longer than necessary; processed in accordance with individuals rights as defined in the Act; kept secure; and transferred only to countries that offer adequate data protection.

That's just a sampling of the many federal, state and international regulations that apply to specific industries and government agencies today, and the regulatory environment will only become more complex in the years to come. In addition, enterprises typically maintain a large, evolving body of internal policies designed to protect the company's information resources, employees, customers and brand reputation.

III. Applying IT Governance Frameworks to the Compliance Challenge

Many organizations faced with multiple compliance requirements are now taking a more mature approach to this problem by adopting IT governance frameworks that can cover a large percentage of regulatory compliance mandates. Three of the most widely employed frameworks are:

COBIT 4.0 – Published by the IT Governance Institute (ITGI) COBIT® 4.0 emphasizes regulatory compliance. It helps organizations to increase the value attained from IT and enables alignment with business goals and objectives. COBIT offers the advantage of being very detail oriented, which makes it readily adoptable across all levels of the organization. It also makes use of the Capability Maturity Model Integration (CMMI) as a way of assessing the status of security processes.

ISO 17799:2005 (ISO 27001) – This is an international standard for the management of IT security that organizes controls into ten major sections, each covering a different topic or area. These are: business continuity planning, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer operations and management, asset control, and security policy.

NIST 800-53 – This publication from the National Institute of Standards and Technology is a collection of "Recommended Security Controls for Federal Information Systems." It describes security controls for use by organizations in protecting their information systems, and recommends that they be employed in conjunction with and as part of a well-defined information security program.

An added benefit of adopting control frameworks is the creation of repeatable processes for compliance and security processes. This has typically led to the ability to better cope with multiple regulatory compliance mandates and an overall reduction of compliance costs. However, the issue of cross-team processes and communication remains unaddressed.

> *"Many organizations are spending more than they need to on IT-related compliance work, because they haven't clearly defined the scope of what's necessary and sufficient for disclosure….However, the organization also must consider how IT support for compliance activities can be provided on an enterprise-wide basis for all compliance needs, rather than just implementing "point" solutions for specific needs (such as Sarbanes-Oxley attestation)."*
>
> **Gartner, Inc.**

IV. Accountability and the Stakes of Noncompliance

Legitimate businesses really have no option but to adopt policies and technologies to ensure compliance with relevant regulations and policies, and to document both the compliance measures and the results for audit purposes. In this increasingly complicated regulatory environment, the relationship between a company's IT department and the rest of the business is changing dramatically.

Failure to manage compliance with regulatory mandates and internal policies imposes serious legal and security risks to the company. Protecting customer data from loss, ensuring the integrity of financial data, and preventing leaks of intellectual property as well as private employee data have become top priorities. As top-level executives have come to recognize the stakes, they're increasingly holding IT managers accountable for enforcing and documenting compliance with regard to electronic systems and networks. When it comes to evaluating the performance of the IT staff, compliance metrics and audit results are now as important as system uptime and performance statistics.

V. Divided Teams with Many Tools: The Problem of Ad Hoc Compliance Management

In a digital world, the obvious response is to automate as much of the compliance and documentation process as possible. Without automated solutions, the burdens of compliance threaten to overwhelm the organization with spiraling costs and risks.

But historically, the available automation tools have been rudimentary and immature at best, ranging from complex products targeted at specific areas of compliance or specific parts of the security team, to simple collections of spreadsheets. Often, generic configuration and risk management solutions are pressed into service to support highly individualized compliance functions—with a lot of manual labor or programming effort required to collate generic data into regulation- and policy-specific compliance data. This often leads to "results" that are inaccurate and hard to replicate/prove on a regular basis due to the manual processes used.

Adding to the problem of ineffective tools, compliance enforcement and documentation is a business process that is still relatively new. Different business units focus on different aspects of the total problem, using the limited tools at hand. For example, a typical enterprise may have three different IT teams assigned to compliance tasks, including:

A security and vulnerability management team is tasked with identifying vulnerabilities in applications, databases and the IT infrastructure before they can compromise enterprise, employee or customer security. This team asks, "Where are the vulnerabilities in our IT environment?"

An IT operations team, typically made up of teams of operating system and application administrators, is tasked with "fixing" various problem issues discovered on systems. This team asks, "What vulnerable or noncompliant systems need to be fixed?" It then undertakes the actual work of fixing them in order of priority.

An audit team is tasked with defining compliance standards, evaluating conformance to those standards, and documenting both compliance and exceptions for the benefit of external auditors and other stakeholders. This team asks, "Are we meeting regulatory standards and baselines, and are we complying with internal policies?"

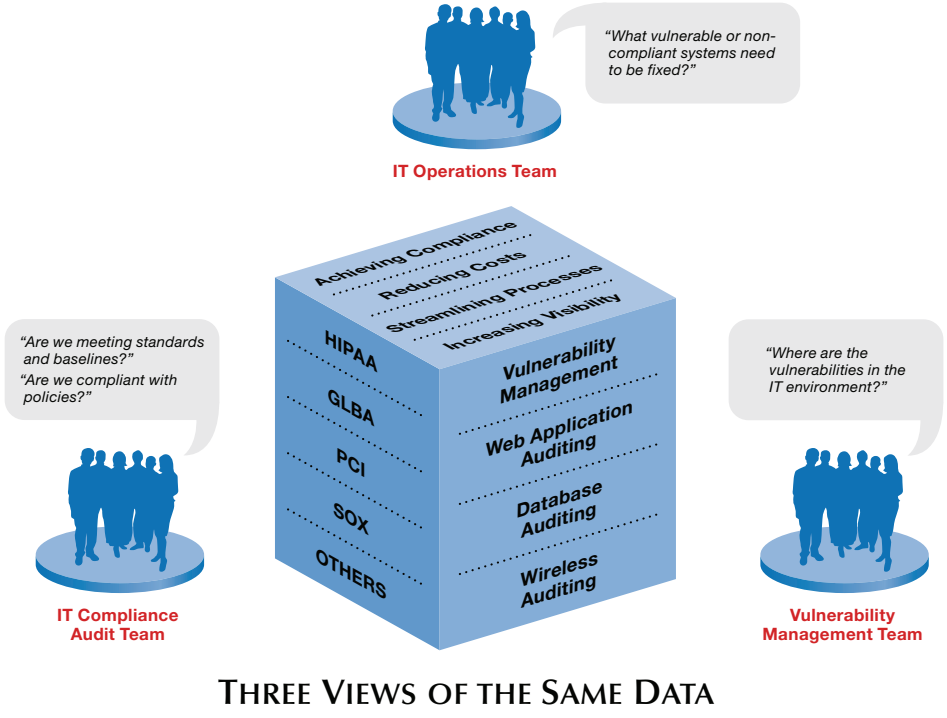

Figure 1: Three Views of the Same Data

As in the Hindu fable of the blind men and the elephant, these three teams look at the same large body of data, but their viewpoints are fragmentary and limited. One team has the elephant by the tail, another by the trunk, and the third by the ear. In fact, the situation is even more disjointed than the fable suggests, since the body of data itself is fragmented by the use of multiple, non-integrated data collection and reporting tools.

"Compliance is an all-encompassing set of activities that cross business and IT groups —everyone is affected in some way. The numbers show that technology is now playing an increasingly significant role in the integration of those compliance requirements into existing business processes."

John Hagerty
AMR Research

With no coherent, big-picture way of viewing compliance data across the organization—or across different regulatory requirements—compliance teams are increasingly caught in inefficient, ad hoc processes. Compliance tasks are often redundant between one regulatory sphere and the next, and across compliance teams. In addition, the use of point solutions that assist only one of these three IT teams in addressing overlapping security and compliance needs makes the problem of fragmentary data and redundant work even more burdensome.

What's needed is a converged solution supporting the entire compliance process that combines policy management with configuration scanning based on defined policies and remediation, all with granular task-based access control. In the next section a more in-depth view of the roles of the IT teams and their responsibilities will be explored.

VI. The Big Picture: The Scope of Compliance Activities and the IT Team

To map out the requirements of a successful compliance solution, the responsibilities of all three compliance-related teams must be taken into consideration. Let's first take a look at traditional overlapping responsibilities of each.

We can break down all compliance activities into a series of tasks that can be roughly grouped under the categories of definition, discovery, evaluation and remediation. Assigning these tasks to the three groups we've identified, the tasks map as follows:

Compliance Activities By Category

	COMPLIANCE AUDIT TEAM	VULNERABILITY MANAGEMENT TEAM	IT OPERATIONS TEAM
DEFINE	– Create policy – Maintain policy		
DISCOVER	– Set compliance scan schedule	– Run compliance scans	
EVALUATE	– Review compliance scan reports – Assess metrics	– Assess scan data against policy – Assess scan data against known threats	– Assess vulnerabilities against policy – Maintain hosts in compliance with IT security policy
REMEDIATE	– Report findings – Provide remediation analysis	– Report findings – Provide risk analysis	– Prioritize & remediate confguration-based vulnerabilities

Figure 2: Compliance Activities by Category

Even though each team has unique responsibilities, there's obviously a lot of overlapping responsibility within their respective roles. At the same time, there's a lot of overlap in compliance requirements for different regulatory mandates and internal policies, which leads to unnecessary spending to deploy and manage one-off solutions for each individual area of compliance. These overlaps provide an opportunity to consolidate policy controls and compliance data—reusing policies, controls and compliance data whenever possible to accommodate the needs of each compliance team and the requirements of each regulatory mandate and each security policy.

For example, an organization's password policies have relevance across SOX, HIPAA, GLBA, NIST and other external mandates, as well as to internal security processes. Likewise, controls over user access and permissions have relevance for SOX, GLBA, NIST and internal processes. Patch policy is relevant to SOX, NIST and internal IT management. And all of these policies and controls have relevance for the activities of the compliance audit, vulnerability management and IT operations teams.

VII. Requirements for a Converged Solution

How can an organization take advantage of these overlapping areas to centralize and simplify compliance management while saving time and money in the process? We've already identified the role of each IT team in the compliance process and some of the required solution elements to support each team's role. To create convergence, solution elements should include:

A single, electronic library of policy and compliance standards and controls

As organizations develop best practices for regulatory and policy compliance, they need to reuse compliance policies and controls wherever possible, applying intelligent filtering and analysis to meet the requirements of each team and compliance task. That means implementing a library of policy and compliance information that spans operating systems, applications, and both external and internal compliance processes.

For example, many businesses have discrete strategies for controlling malware, limiting the deployment of peer-to-peer software, controlling the deployment of applications that could prove harmful to the IT environment, and other compliance and security needs. In a recent implementation, one enterprise was utilizing 57 different, paper-based standards for dealing with all the different operating systems and applications in use. A more efficient and effective compliance model would collect all these standards and controls in one electronic library, where they can be efficiently accessed, updated and shared by different compliance teams for different purposes.

How to Succeed in Security Compliance: Automate and Audit Often

In a recent study, researchers at the IT Policy Compliance Group examined the relationship between IT security spending and successful regulatory compliance in 876 organizations. Among the study's recommendations are that companies allocate 10% of overall IT spending on security systems, and that they audit frequently—companies that conduct monthly system audits are far more successful at achieving compliance than those that only audit annually.

The report also concludes that organizations are better served spending their security dollars on systems and services that facilitate audits—including configuration and change management applications, user-access control systems, anti-virus and reporting tools—rather than on additional external contractors and consultants. Organizations with the fewest compliance problems are spending 9% more to automate audit functions and 11% less on contractors and outside services.

For more info: **www.itpolicycompliance.com**

Multipurpose compliance checks

Instead of building and maintaining compliance checks for each regulatory and internal business requirement, companies need to adopt a "build once, deploy many times" strategy. With a few variances, a single core group of compliance checks can provide support across most or all of an organization's compliance obligations. For example, user password policies, user access privileges, account management and other types of checks can be designed to satisfy all internal and regulatory requirements, eliminating the burden of management redundancy and allowing compliance teams to focus their efforts on the few remaining unique compliance requirements.

Change control

Policy checks typically have a lifecycle, with the number of checks and the specific requirements of each changing over time as business needs change and new systems come online. To accommodate these lifecycles and support compliance documentation, the compliance system needs to include a change control mechanism that provides an audit trail including the date of any change, author of the change, and any required change approval.

Audit against an established IT gold standard

To ensure policy compliance, new systems can be checked both prior to deployment and continuously once the systems are operating in the production environment. To provide efficient support for both methods, IT can create a "gold standard" or baseline for a specific host configuration, testing all other hosts of that type against the gold standard. For businesses that regularly deploy servers from a test environment into a production environment, this approach allows for certification of the host configuration, ensuring that a compliance baseline has been met and reducing risk in the deployment phase.

Once hosts have been deployed in the production environment, the appropriate detective controls should be used to measure policy compliance on an ongoing basis. Determining compliance usually involves querying a data set that represents the configuration of the operating system and applications on one or more hosts, and comparing the query results to the expected results as documented for the relevant compliance policy. Here again, having an established gold standard can provide invaluable support. Policy-driven control testing, as defined by specific controls, can represent hundreds of very specific queries of host configuration data sets for thousands of hosts compared to the expected query results.

Exception control

Day-to-day operations may often require temporary or role-based exceptions to the blanket policy. For example, a company's security policies may include a restriction against running an FTP service on any server. But certain employees in the enterprise, at certain times, may have a temporary need to use FTP.

Such a policy exception and the ensuing workflow must be allowed and documented in a way that formally acknowledges the company's acceptance of the risk involved in permitting the exception. This is especially important when compliance controls are audited by third parties—such as internal or external auditors—who may not otherwise understand the business reasons for deliberately violating the policy.

Consolidated management, reporting and issue tracking

In consolidated management, reporting and issue tracking, the main goals of a converged compliance and vulnerability management solution are achieved. Ideally, you have one system for the entire enterprise that allows you to:

- ***Manage multiple compliance requirements,*** including all relevant external regulations and internal security policies. The solution should provide a continuous, automated view of host configuration with data updated on every host scan.

- ***Generate reports*** that support each compliance team's needs, including compliance metrics and audit results. All reports should draw upon one data set for all compliances, ensuring consistency and completeness.

- ***Issue and track service tickets*** to ensure that issues are promptly reported to and resolved by the appropriate asset owners. This capability should be a built-in feature of the solution in order to eliminate the time lag—or even the black hole—that often occurs when issues trickle down through the organization from IT to a department manager, to the responsible party.

"Through 2007, companies that choose one-off solutions for each regulatory challenge they face will spend 10 times more on IT solutions for compliance than their counterparts that take a sustainable programmatic approach. The pressure of meeting SOX deadlines may have led many CIOs to implement one-off projects and miss opportunities to secure long-term benefits for their businesses. This will, in some cases, mean more budget will be spent to advance these projects in 2008 and 2009."

Gartner, Inc.
"Gartner Survey Shows Spending for Compliance and Corporate Governance to Account for 10 to 15 Percent of an Enterprise's 2006 IT Budget"

VIII. Architecture for a Converged Solution

A converged solution needs to support all of the pieces of the compliance process, with the right tools all applied in the right order for the right teams. An illustration of the converged solution architecture and process flow is shown below.

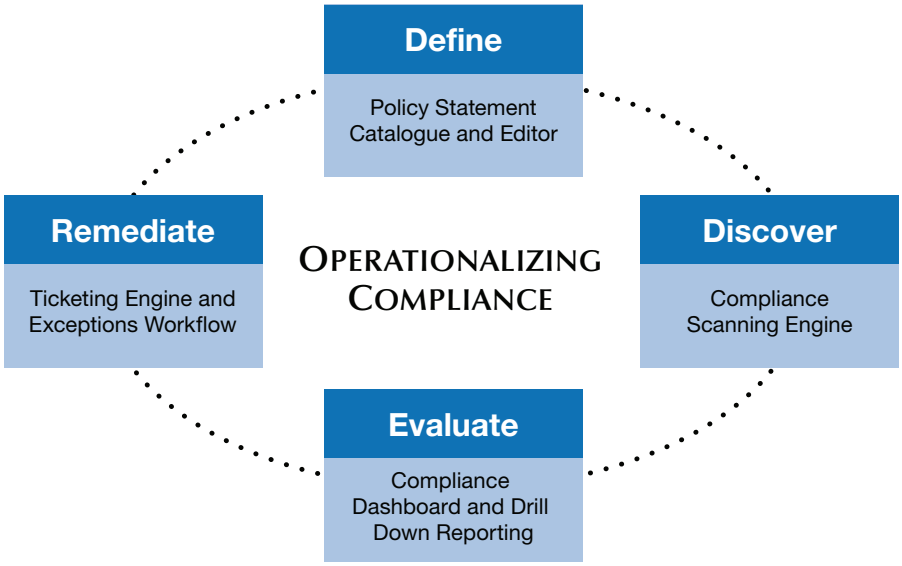

Figure 3: Operationalizing Compliance

VIIII. Why Software-as-a-Service (SaaS) is best suited for Compliance

We have identified the problems associated with using compliance point solutions that address only one segment of the IT team's needs, and that may be further limited by each team's geographic location. All teams within IT need a unified compliance approach that supports the specific role of each team while supporting the segregation of duties between them. The benefits of the SaaS approach, which is the foundation of Qualys' award-winning vulnerability management and policy compliance system, include:

- ***A Trusted Third Party*** that yields reliable data. Because all host compliance data and policies are securely stored by QualysGuard® and not subject to manipulation, auditors trust the integrity and accuracy of the information and resulting QualysGuard reports.

- ***Deployment and Scalability*** is extremely important when diverse compliance teams are scattered across the globe. SaaS is best suited to support geographically dispersed teams that may be responsible for compliance for the entire enterprise or only one small part. Scheduled compliance scans can be run against specific parts of the enterprise at specific times, allowing for continuous scanning for compliance issues. SaaS removes scalability as a total cost of ownership (TCO) concern, and compliance becomes as ubiquitous as the web browser.

> *"Compliance is having demonstrable, repeatable security processes to keep the auditors happy."*
>
> Dave Bixler
> **Siemens**

- ***Agent-less*** solutions speed deployment and cost less to manage over time. Remediating configuration compliance issues is not complicated by having to remediate problems with the software agents that collect compliance data. Hosts that have malfunctioning software agents cannot be considered in compliance reports.

- ***Subscription-based SaaS*** model allows the customer to control the compliance solution without the "sunk-costs" associated with purchasing, licensing and supporting software based products. The entire service is priced per host and there are no hidden costs. This is in stark contrast to solutions that comprise a management console, data collection agents, databases, add-on modules for compliance reporting and in some cases, a separate product that manages selective compliance policies. Simplified deployment, a reliable gold-standard of reporting, and overall lower TCO are primary benefits of the subscription-based SaaS approach.

- ***Role-based Access*** to data is critical to an organization made up of IT teams that all have some role to play in the compliance process. The roles played by all compliance teams—IT operations, security and vulnerability management, internal audit and policy management—need to be supported. Even an external audit firm could be granted a view of compliance reports to gauge compliance status over time and streamline the consulting engagement.

X. Look to Qualys for Converged Compliance Leadership

Qualys understands the challenges organizations face as different teams and asset owners throughout the organization struggle to achieve and document compliance in an ever-changing regulatory and compliance landscape. That's why Qualys approaches vulnerability and compliance management as a global issue that crosses your enterprise's organizational boundaries—and that encompasses an ever-growing and changing web of overlapping requirements.

QUALYS®
www.qualys.com

USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
T: +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 München
T: +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
T: +33 (0) 1 41 97 35 70

ON DEMAND SECURITY