QUALYS®
ON DEMAND SECURITY

GUIDE:

Avoiding 7 Common Mistakes of IT Security Compliance

Table of Contents

Summary

Compliance is a key driver for deployment of IT security controls, and many organizations are pursuing automation to improve accuracy and lower costs of fulfilling requirements. Automating controls is not just laudable – it's essential for finding and fixing a myriad of vulnerabilities that enable criminals to breach enterprise IT, disrupt electronic business processes, and steal confidential business and customer data. But automation alone is not a panacea for compliance. Organizations must also associate deployment of automated security solutions with common sense operational strategies to ensure success.

At the most basic level, there is no single standardized framework or terminology that explicitly defines what your organization must do for compliance. Instead, there are many frameworks with conflicting requirements. Terminology is often vague or interpreted differently within organizations and between geographic regions. Ambiguity abounds due to lack of a universal philosophy of compliance. A big challenge for security professionals is navigating this ambiguity, especially when financial auditing terms such as Governance, Risk and Compliance (GRC) are loosely applied to IT security solutions. Let the buyer beware! This guide describes seven typical mistakes of IT security compliance and how you can use these lessons to help your organization achieve its compliance goals.

1) Decentralized Policy Management

Many companies, especially global organizations have had multiple silos of policy content that evolved over time without the benefit of a common compliance framework, terminology and definitions. Consequently, different regions in an organization have different policies that do not conform to a unified standard. For example, a risk score might be calculated one way in the EU and another in the US, which complicates consistent documentation of compliance. It's not expected that every region would share identical policies, especially since regulatory requirements for one area often differ substantially from another. But when regional policies are developed in a vacuum, it increases the cost of an enterprise compliance program.

Your organization should centrally coordinate all compliance policies to help control costs. Centralized policy management will also help your organization in the selection of compliance software used to automate global compliance processes.

2) Failure to Define Compliance

An efficient and successful compliance program requires common definitions for vocabulary used by regulations, your vendors and consultants. Lack of common definitions can lead to confusion, inefficiency, waste, or penalties and fallout resulting from non-compliance. Make clear distinctions, such as:

- **Policy.** Is it a high level text-based concept or a collection of technical settings?
- **Compliance.** Technical-only, or does it include manual task completion? Statements about compliance should include exceptions, which allow an auditor to accept risk and make a control pass.
- **Standard.** Is this a high-level statement, a regulatory requirement, or an industry-driven concept?
- **Control.** Is this a high-level statement, a technical requirement, or a product? A control statement should include the rationale for its use (e.g. "To prevent a malicious user from accessing sensitive information in these accounts.").
- **Framework.** A technical architecture, guidelines for development of strategy, or an industry-specific document (e.g. NIST Special Publication 800-53 for US federal, the PCI Data Security Standard for retail, or Control Objectives for Information and related Technology [COBIT] for IT security governance)?

Articulating clear definitions for all relevant terms of compliance is essential to ensure the success of your organization's compliance efforts.

> *"Gathering IT security and configuration data for compliance purposes is a daunting task and quite expensive for a distributed organization like ours. QualysGuard enables us to collect security and compliance information from all of our global IT assets without having to deploy agents and to leverage this data across multiple compliance and regulatory initiatives. This enables us to drastically reduce the cost of compliance reporting while gaining an accurate view of our security and compliance posture."*
>
> Victor Hsiang, Director of Security Architecture
> **TransUnion**

3) Tactical Instead of Strategic Response

Beware the risk of kneejerk reactions to regulations, which can lead to tactical mistakes in compliance. The guiding strategy for every regulation should be specification of scope with the "letter of the law." For example, after Sarbanes-Oxley (SOX) became law, many companies subject to its requirements chose a "quantity over quality" approach and created a large number of controls. SOX requires controls affecting systems related only to financial reporting, but some organizations adopted controls affecting the entire enterprise. Consequently, technical staff was unable to keep up with workload and effectively deal with the risks that affected compliance.

Strategic definition of scope with specific regulations will make your organization's compliance efforts more efficient and effective.

4) No Pre-implementation Testing

In an effort to automate the harvesting of IT compliance data, some organizations purchase software without adequately testing it to ensure the result is what they need. Often these information security tools cost more than $1,000 an agent per system. One energy company spent $2 million on a solution right after the Enron scandal, only to drop it within two years because it did not provide the intended result. In addition to testing for functionality, your organization should test for conflicts with existing business processes. For example, a hospital installed an agent-based system into production without adequate testing. It subsequently discovered a conflict with an internal application that prevented nurses to log in after a shift change. As a result, patients missed receiving medication and some critical systems were unavailable for hours.

Test IT security products before you buy to prevent trouble and ensure success with compliance.

5) Treating the Audit as a Nuisance

An IT audit of business functions can identify waste and help to streamline business processes. This is beneficial to an organization but common staff sentiments are that audits are a necessary evil, do audits only as required (e.g. once a year or quarter), and invest as little as possible in the audit process. In other words, many organizations go through the motions of an audit only for the sake of appearance. It's worse when staff prefers convenience over security. HPUX administrators at a large pharmaceutical company once told a consultant when they learned an audit was eminent, they would harden the systems a week before and revert to the original state after the auditors left. That company later paid large penalties for violations of compliance. This is a good example of how an audit only certifies security compliance in a snapshot of time.

Another challenge is being unaware of what IT assets exist and need protection. To rectify this situation, organizations should deploy a device discovery solution that automatically catalogs all devices and configurations on the network.

Having asset, configuration and vulnerability information available on demand is vital for knowing what to protect, what security solutions to deploy, and to ensure compliance. Having device, configuration and security data on demand also helps to support a safer "perpetual audit" environment, especially if a network or systems administrator changes topology without notifying the security staff.

6) Lack of Team Buy-in

Lack of buy-in is a perennial issue in every organization. It's particularly bad for security compliance because IT administrators have been known to do things "their way" irrespective of organization process and protocol. Over confidence in their technical ability can lead to an attitude of being above the rules – even to the point of erasing evidence. For example, an IT administrator in one organization was well aware of the organization's prohibition on downloading files from peer-to-peer sites. To circumvent this, the administrator used VMware environments as a temporary download station to receive files in violation of policy. Presence of pirated content placed the organization in jeopardy.

Educating staff about the benefits of policy and obtaining their commitment to comply are essential for obtaining and maintaining organization compliance.

> *"Regulations such as the Sarbanes-Oxley Act and Basel II have pushed compliance to the forefront of the executive's agenda. In this environment, security managers must tie their vulnerability management and security auditing practices to broader corporate risk and compliance initiatives."*
>
> Andreas Wuchner-Bruehi,
> Head of Global IT Security
> **Novartis AG**

7) Ignoring Hidden Costs of Solutions

In calculating your organization's required budget for compliance, be sure to look under the hood for hidden costs that vendors do not always note in their sales pitches and responses to RFPs. Automation of security solutions is a key ingredient to keeping hidden costs low, but even this does not always save as much as you think. For example, agent-based security solutions often require large amounts of upkeep and maintenance. This cost can rise sharply if agents must be maintained on every endpoint and network IP. Solutions that are hosted on in-house servers and databases require installation and ongoing maintenance. Staff requires education on security solutions, how to deploy and use them, and to provide ongoing maintenance. The technical staff must also stay up-to-date on technologies behind solutions that are hosted in house, for these can quickly fall out of currency. Finally, IT security managers must provide constant oversight to ensure that security applications do not fall into a neglected state and remain in productive operation.

Analyze all aspects of compliance to discover their hidden costs. Hosting IT security and compliance applications in house usually adds to the total cost of compliance.

Comply with Confidence

The QualysGuard Policy Compliance on demand solution helps organizations to solve the challenges of compliance and avoid the common mistakes described above. It is an agent-less and scalable audit technology that automates the harvesting of configuration data from IT assets. It automatically identifies violations of an organization's stated control objectives as related to compliance. The technical controls library is based on CIS and NIST. The service supports the following categories, technologies, frameworks, and compliance initiatives:

Categories

- Security management
- Authentication
- Access control
- Services network security
- Antivirus/malware
- Integrity/availability
- Application control
- Encryption

Technologies

- AIX 5.x
- HPUX 11.iv1
- HPUX 11.iv2 ('Q2)
- Linux Red Hat Enterprise 3/4
- Linux Red Hat Enterprise 5
- Microsoft SQL Server 2000 ('Q2)
- Microsoft SQL Server 2005 ('Q2)
- Oracle 10g
- Oracle 11g
- Oracle 9i
- SUSE Enterprise Linux 9/10
- Solaris 10
- Solaris 8
- Solaris 9x
- Windows 2000
- Windows 2000 Active Directory ('Q2)
- Windows 2003 Active Directory ('Q2)
- Windows 2003 Server
- Windows Vista
- Windows XP Desktop

Frameworks & Regulations

- SCIS – AIX v 1.0.1: 2005
- CIS – HPUX v 1.4.1: 2007
- CIS – Oracle 9i, 10g v 2.0: 2006
- CIS – Red Hat Ent. Linux 2.1, 3.0, 4.0 v. 1.0.5: 2006
- CIS – Red Hat Ent. Linux 5 v. 1.0 & 1.1: 2008
- CIS – SUSE 20 2.0: May 2008
- CIS – Solaris 10, Rel. 11/ 06 & 8/07 v. 4.0: 2007
- CIS – Solaris 8, 9 v. 1.3.0 : 2004
- CIS – Windows 2000 Server, L2 v. 2.2.1 : 2004
- CIS – Windows 2003 Server v. 1.2: 2005
- CIS – Windows XP v. 2.01: 2005
- COBIT 4.0 Published: 2005
- COBIT 4.1 Published: 2007
- FFIEC ver. 1 Published: 2006
- HIPAA 45 CFR Parts 160/164, Subparts A/C: 1996
- ISO 17799 Published: 2005
- ISO 27001 Published: 2005(E)
- IT Infrastructure Library (ver. 2) Published: 2003, rev. 2005
- IT Infrastructure Library (ver. 3) Published: 2007
- NERC ver. 1 Published: 2007 vol. 1
- NIST 800-53 ver. 1 Published: 2006

QualysGuard Policy Compliance deploys immediately, is automated and easy to use, is accurate, scalable, enables quick reaction, and provides flexible automated reporting, built-in exception management, improved security, and cost-effective compliance.

About Qualys

Qualys, Inc. is the leading provider of on demand IT security risk and compliance management solutions – delivered as a service. Qualys' Software-as-a-Service solutions are deployed in a matter of hours anywhere in the world, providing customers an immediate and continuous view of their security and compliance postures. The QualysGuard® service is used today by more than 3,500 organizations in 85 countries, including 40 of the Fortune Global 100 and performs more than 200 million IP audits per year. Qualys has the largest vulnerability management deployment in the world at a Fortune Global 50 company. Qualys has established strategic agreements with leading managed service providers and consulting organizations including BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, SecureWorks, Symantec, Tata Communications, TELUS and VeriSign.

For more information, please visit ***www.qualys.com***.

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
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
United Arab Emirates – Qualys FZE • P.O Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

ON DEMAND SECURITY