QUALYS®

WHITE PAPER

# USING QUALYSGUARD TO MEET SOX COMPLIANCE & IT CONTROL OBJECTIVES

ON DEMAND SECURITY

> *"CobIT 4.0 is a significant improvement on the third release, making it more relevant, filling some gaps and adding clarity. Most importantly, it better aligns with good and best practices in the management of IT and so increases the possibility that its use will result in a better-managed IT environment and, specifically, improve risk management. Therefore, we continue to recommend that enterprises use it to challenge their established IT governance procedures and to improve the controls they have in place."*
>
> **CobIT 4.0 Is a Good Step Forward**
> Simon Mingay
> 29 December 2005

Meeting new regulatory compliance requirements can be a struggle for any company. The concerns about "where do I start?" and "can I leverage existing processes to meet these new requirements?" are obvious questions with not-so-obvious answers. Guidance provided by the Public Company Accounting Oversight Board (PCAOB) is embedded in long and complex documents known as "Audit Standards"; unless you are a seasoned audit professional, much of this guidance can easily be misinterpreted or misunderstood. Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) requires the management of public companies to assess the effectiveness of an organization's internal control over financial reporting and annually report the result of that assessment. In order to satisfy this requirement, SOX mandates that affected organizations use a recognized internal control framework. Actually, it makes specific reference to the Committee of the Sponsoring Organizations of the Treadway Commission (COSO), which is accepted by many enterprises as the "standard" internal control framework. The "CobiT" Control framework has basically become the standard for IT general computing controls (GCC's) and is mapped back to the five focus areas of IT governance and respective COSO control domains.

The Sarbanes-Oxley Act of 2002 has fundamentally changed the business and regulatory landscape for all companies publically traded in the US. SOX is intended to instill confidence back into the investor community after several corporate scandals resulted in the loss of billions of dollars in invested capital. SOX does this by increasing corporate governance requirements through measures that will strengthen internal checks and balances and ultimately, provide transparency, as well as elevated corporate accountability. It is important to emphasize that section 404 does not require senior management and business process owners to merely establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis. Most would agree that the reliability of financial reporting is heavily dependent on a well-controlled and secure IT environment. Accordingly, organizations must consider addressing IT controls in a financial reporting context. The QualysGuard Vulnerability Management Service maps to many of these controls.

CobiT, administered by the Information Systems Audit and Control Association (ISACA), is a high-level yet comprehensive framework for managing risk and control over IT assets, comprising four domains, 34 IT processes and 318 detailed control objectives. Unlike COSO, CobiT includes controls that address operational and compliance objectives, but only those related to financial reporting have been considered in the development of this document. CobiT provides an actionable framework by which an entity can achieve compliance with SOX, when this framework is strategically implemented, to reduce identified risk areas to acceptable levels.

The following tables outline some specific activities in CobiT that map to the QualysGuard Vulnerability Management service benefits for each section. In support of the items below, "PO3" represents one of CobiT's 34 IT processes.

| | | | COSO Component | | | | |
|---|---|---|---|---|---|---|---|
| Company Level | Activity Level | CobIT Area | Control Environment | Risk Assessment | Control Activities | Information & Communication | Monitoring |
| **Plan and Organize (IT Environment)** | | | | | | | |
| ✔ | | IT strategic planning | ✔ | ✔ | | ✔ | ✔ |
| ✔ | | Information architecture | | | ✔ | ✔ | |
| | | Determine technological direction | | | | | |
| ✔ | | IT organization relationships | ✔ | | | ✔ | |
| | | Manage the IT investment | | | | | |
| ✔ | | Communication of management aims and direction | ✔ | | | ✔ | ✔ |
| ✔ | | Management of human resources | ✔ | | | ✔ | |
| ✔ | | Compliance with external requirements | | | | ✔ | ✔ |
| ✔ | | Assessment of risks | | ✔ | | | |
| | | Manage projects | | | | | |
| ✔ | | Management of quality | ✔ | | ✔ | ✔ | ✔ |
| **Acquire and Implement (Program Development and Program Change)** | | | | | | | |
| | | Identify automated solutions | | | | | |
| | ✔ | Acquire or develop application software | | | ✔ | | |
| | ✔ | Acquire technology infrastructure | | | ✔ | | |
| | ✔ | Develop and maintain policies and procedures | | | ✔ | ✔ | |
| | ✔ | Install & test application software & technology infrastructure | | | ✔ | | |
| | ✔ | Manage changes | | | ✔ | | ✔ |
| **Deliver and Support (Computer Operations and Access to Programs and Data)** | | | | | | | |
| | ✔ | Define and manage service levels | ✔ | | ✔ | | ✔ |
| | ✔ | Manage third-party services | ✔ | ✔ | ✔ | | ✔ |
| ✔ | | Manage performance and capacity | | | ✔ | | ✔ |
| | | Ensure continuous service | | | | | |
| | ✔ | Ensure systems security | | | ✔ | ✔ | ✔ |
| | | Identify and allocate costs | | | | | |
| ✔ | | Educate and train users | ✔ | | | ✔ | |
| | | Assist and advise customers | | | | | |
| | ✔ | Manage the configuration | | | ✔ | ✔ | |
| | ✔ | Manage problems and incidents | | | ✔ | ✔ | ✔ |
| | ✔ | Manage data | | | ✔ | ✔ | |
| ✔ | | Manage facilities | | ✔ | | | |
| | ✔ | Manage operations | | | ✔ | ✔ | |
| **Monitor and Evaluate (IT Environment)** | | | | | | | |
| ✔ | | Monitoring | | | | ✔ | ✔ |
| ✔ | | Adequacy of internal controls | | | | | ✔ |
| ✔ | | Independent assurance | ✔ | | | | ✔ |
| ✔ | | Internal audit | | | | | ✔ |

### *CobIT Domain - Planning and Organization*

| CobIT Mapping | QualysGuard Benefits | COSO Component | | | | |
|---|---|---|---|---|---|---|
| | | Control Environment | Risk Assessment | Control Activities | Information and Communication | Monitoring |
| P03 – Determine Technological Direction | QualysGuard can help to determine the needs for other additional products in the security architecture. | | | | | |
| P04 – Define the IT organization and relationships | QualysGuard can be used to define the relationships between security teams (VM to Desktop Support) through the use of the remediation capabilities. | ✔ | | | ✔ | |
| P05 – Manage the IT Investment | Trending information from QualysGuard can help to determine the need for IT investment (system and/or software upgrades) over time. | | | | | |
| P08 – Insure Compliance with external organizations | QualysGuard reports can assist organizations in meeting compliance with SOX, GLBA, and HIPAA among other regulations by discovering devices in the IT environment that may be vulnerable or improperly configured. | | | | ✔ | ✔ |
| P09 – Assess Risks | QualysGuard provides customers a method of assessing risks within their environment based on CVSS and by allowing each customer to create an individualized value matrix for devices in the architecture. | | ✔ | | | |

### *CobIT Domain - Acquire and Implement*

| CobIT Mapping | QualysGuard Benefits | COSO Component | | | | |
|---|---|---|---|---|---|---|
| | | Control Environment | Risk Assessment | Control Activities | Information and Communication | Monitoring |
| AI4 – Develop and Maintain procedures | QualysGuard introduces a structure (our six-step approach) for the management of vulnerabilities, from discovery to remediation. These steps are the groundwork for needed for the creation of organizational IT processes and procedures. | | | | | |
| AI5 – Install and accredit systems | The QualysGuard solution allows for the creation of a “gold standard” for the security of a particular host. This can be used to accredit a system’s configuration prior to deployment. | ✔ | | | ✔ | |
| AI6 – Manage Changes | The remediation features in the QualysGuard solution can be used for the management of changes, such as patches, to update or reconfigure network- or user-based IT resources. | | | | | |

### *CobIT Domain - Delivery & Support*

| CobIT Mapping | QualysGuard Benefits | COSO Component | | | | |
|---|---|---|---|---|---|---|
| | | Control Environment | Risk Assessment | Control Activities | Information and Communication | Monitoring |
| DS5 – Ensure System Security | QualysGuard qualifies the classifications of what systems' "vulnerabilities," include, to help to ensure understanding of the interrelationships in security remediation. | | | ✔ | ✔ | ✔ |
| DS9 – Manage the Configuration | QualysGuard scans can indicate that hosts may not be configured correctly, which may also result in a reduced level of system security. | | | ✔ | ✔ | |
| DS10 – Manage Problems and Incidents | QualysGuard's built-in ticket remediation system can assist in the management of problems and root cause analysis of security incidents. | | | ✔ | ✔ | ✔ |

### *CobIT Domain - Monitoring*

| CobIT Mapping | QualysGuard Benefits | COSO Component | | | | |
|---|---|---|---|---|---|---|
| | | Control Environment | Risk Assessment | Control Activities | Information and Communication | Monitoring |
| ME2 – Monitor and Evaluate Internal Control | QualysGuard provides an automated method of testing all technically defined controls. Companies impacted by SOX compliance are required to perform periodic self-assessments related to the effectiveness of internal controls placed in Production. Taking into consideration that this is an ongoing process, QualysGuard can greatly reduce the cost and human resource overhead associated. | | | ✔ | ✔ | ✔ |
| ME3 – Ensure Compliance with External Requirements | QualysGuard Vulnerability Management and Policy Compliance reports can be used as evidentiary support for meeting regulatory and contractual requirements and expectations. | | | ✔ | ✔ | |

In addition to its use as a vulnerability management and remediation tool, QualysGuard maps to many of the areas of the COSO framework and can be used to demonstrate compliance with Sarbanes-Oxley Act of 2002, Section 404.

For those companies using the CobiT framework for overall IT governance, QualysGuard functionality provides a method of meeting specific CobiT governance requirements. The table below outlines the QualysGuard capabilities that map to the specific control objectives.

| CobIT 4.0 Controls | CobIT Sub-Control | QualysGuard Capabilities |
|---|---|---|
| PO 9 Assess and Manage IT Risks | PO9.3 Event Identification | • Identifies vulnerabilities.<br>• Asses Risk – support for CVSS.<br>• Identifies device misconfigurations.<br>• Information available on demand. |
| AI6 Manage Changes | AI6.4 Change Status Tracking and Reporting | • The incorporation of a remediation management system within QualysGuard allows for tracking of changes to systems.<br>• Action logs available for viewing and (with QG 4.7) download for tracking changes to QualysGuard Activities.<br>• Scan and report notifications available via email. |
| | AI6.5 Change Closure and Documentation | • Action logs available for viewing and (with QG 4.7) download.<br>• Multi role support segregation of duties (SoD).<br>• Scan and report notifications available via email. |
| DS2 Manage Third-party Services | DS2.4 Supplier Performance Monitoring | • Many customers have purchased Qualys to monitor third party service providers. Audits SLA compliance for those who've outsourced IT infrastructure patching maintenance. |
| DS5 Ensure Systems Security | DS5.4 User Account Management | • QualysGuard can assist in meeting this requirement by auditing for unused accounts (QID 105234).<br>• QualysGuard can provide audits of user rights and privileges. |
| | DS5.5 Security Testing, Surveillance and Monitoring | • Automated QualysGuard scans using credentialed access can test for compliance and accreditation of systems. This can be accomplished through the use of specific templates containing level 1 and 2 vulnerabilities. |
| | DS5.6 Security Incident Definition | • QualysGuard threat, impact and solution data is well defined as part of Qualys reporting.<br>• CVSS is supported for indicating impact level. |
| | DS5.9 Malicious Software Prevention, Detection and Correction | • Report templates containing specific Qualys QIDs represent and identify Trojans, back-doors, key loggers and rootkits on systems and can be used as part of an overall strategy for DS5.9. |
| DS8 Manage Service Desk and Incidents | DS8.3 Incident Escalation<br>DS8.4 Incident Closure<br>DS8.5 Trend Analysis | • QualysGuard Remediation specifically supports all DS8 controls allowing for vulnerability remediation assignment and control.<br>• Reports are available to support remediation trend analysis.<br>• Export to third part ticketing system is supported. |
| DS9 Manage the Configuration | DS9.3 Configuration Integrity Review | • Specific Qualys QIDs represent system configuration detections that include software inventories. These can be compared to user defined baselines.<br>• QualysGuard can perform system software audits. |
| DS10 Manage Problems | DS10.1 Identification and Classification of Problems<br>DS10.2 Problem Tracking and Resolution<br>DS10.3 Problem Closure<br>DS10.4 Integration of Change, Configuration and Problem Management | • QualysGuard Remediation specifically supports all DS10 controls allowing for vulnerability remediation assignment and control.<br>• Reports are available to support remediation trend analysis.<br>• Export to third part ticketing system is supported. |
| ME2 Monitor and Evaluate Internal Control | ME2.1 Monitoring of Internal Control Framework<br>ME2.1 Monitoring of Internal Control Framework | • QualysGuard supports vulnerability trending and benchmarking reports to control the IT environment.<br>• QualysGuard supports exception control through the ignore vulnerability function on a host-by host basis. This information can be made available across users.<br>• QualysGuard provides subscription based timely security notifications about emergency threat detections. |
| | ME2.7 Remedial Actions | • Qualys supports remediation change management and process control.<br>• Remediation can be assigned specific individuals.<br>• Tracking reports are available. |
| ME3 Ensure Regulatory Compliance | ME3.3 Evaluation of Compliance With Regulatory Requirements | • Information gathered through QualysGuard scans can assist with compliance with many regulatory compliances.<br>• User access rights to files and folders, File permissions, Patches, Malicious Software, Host event log settings, and other security setting information is relevant for HIPAA, Sarbanes-Oxley, NIST 800-53, and other regulatory compliances. |

**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 35 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, 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
**Hong Kong – Qualys Hong Kong Ltd.** • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 2824 8488

ON DEMAND SECURITY