



**Sarbanes-Oxley  
Compliance Reports**  
Security and Audit Directors  
Live For

# Sarbanes-Oxley Compliance Reports

## Security and Audit Directors Live For

### Contents

Executive Summary .....	3
REPORT #1: Compliance Evaluation for Sarbanes-Oxley and COBIT .....	4
REPORT #2: Compliance Evaluation for All systems.....	5
REPORT #3: Security Assessments for System Permissions Given to Users (Entitlement Report) ..	6
REPORT #4: Security Assessment for Modifications to Critical System Files .....	7
REPORT #5: Security Assessment for Users and Groups with Elevated Rights to the Database ...	8

## Executive Summary

While complying with regulations is one of the top issues facing businesses today, many IT security executives are confused about what specifically they must do to achieve compliance. As a result, they can easily allocate either too much or too little staff time, money and outside consulting resources pursuing a seemingly elusive goal.

As many companies discovered this past year, costs for demonstrating compliance with Sarbanes-Oxley can be staggering. Spending on Sarbanes-Oxley will exceed \$6 billion in 2005 according to AMR. Of this amount, \$2.6 billion goes to pay for internal personnel devoted to compliance, while another \$1.7 billion is being spent on consultants and external auditing firms.

From an IT security perspective, the key to Sarbanes-Oxley compliance is in the documentation, monitoring and management of a compliance control structure for your specific enterprise environment. While managing and monitoring technical controls is just one part of SOX compliance, it is an expensive and labor-intensive component.

The good news is that technical controls including policies and controls can be automated or enforced across the IT infrastructure. Technical controls, for example, would include a company's password policies, as well as the secure configuration and protection of system servers.

Unlike any other vendor, Symantec offers proven, practical IT security compliance solutions that remove the barriers limiting your ability to cost-effectively demonstrate and continuously monitor Sarbanes-Oxley compliance.

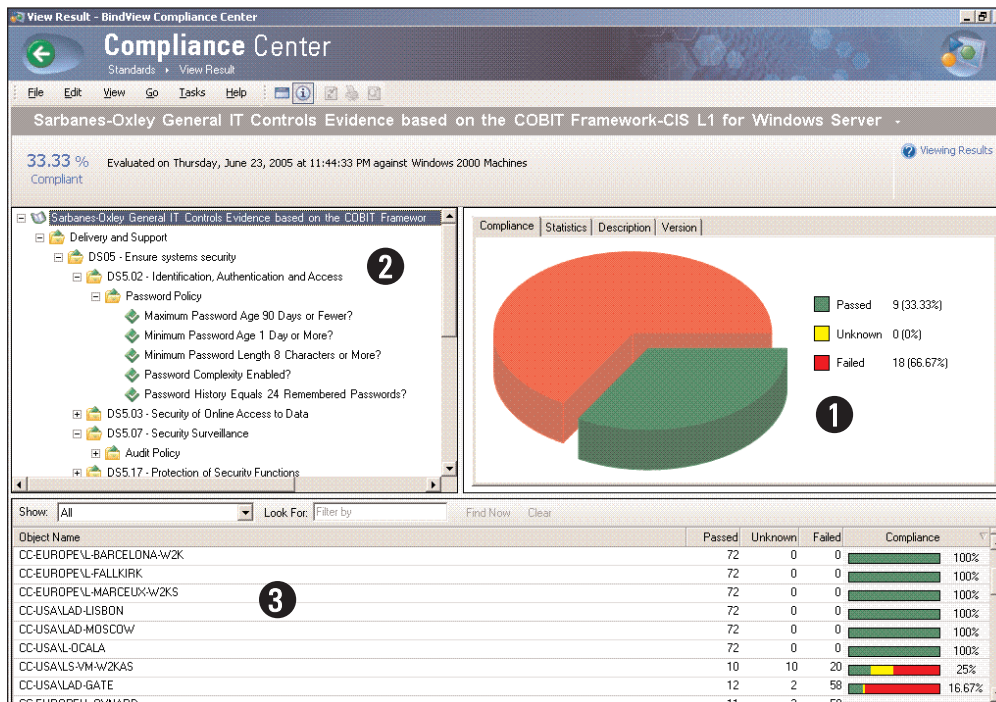
Symantec's powerful viewing and reporting capabilities in Compliance Center enable you to audit and maintain Sarbanes-Oxley compliance to standards in a fraction of the time required by manual methods. Symantec can streamline, automate, and sustain compliance at reduced cost with easy-to-produce and understandable console views and reports that include:

1. Compliance Evaluation for Sarbanes-Oxley and COBIT
2. Compliance Evaluation for All systems
3. Security Assessments for System Permissions Given to Users (Entitlement Report)
4. Security Assessment for Modifications to Critical System Files
5. Security Assessment for Users and Groups with Elevated Rights to the Database

## REPORT #1

### Compliance Evaluation for Sarbanes-Oxley and COBIT

Many organizations have reverted to COBIT as a standard for Internal IT Controls for Sarbanes-Oxley. Symantec Compliance Center helps you demonstrate Sarbanes-Oxley compliance through a collection of automated checks that map directly to the COBIT framework. This mapping translates the technical details of your security compliance program into a common language used by internal and external auditors and other stakeholders when evaluating Sarbanes-Oxley compliance. As seen below, compliance requirements can be analyzed at the COBIT domain level, or at the individual Control Objective level.



1] When running the COBIT report view, you can receive an overall compliance score or you can receive a compliance score for each requirement in a control objective.

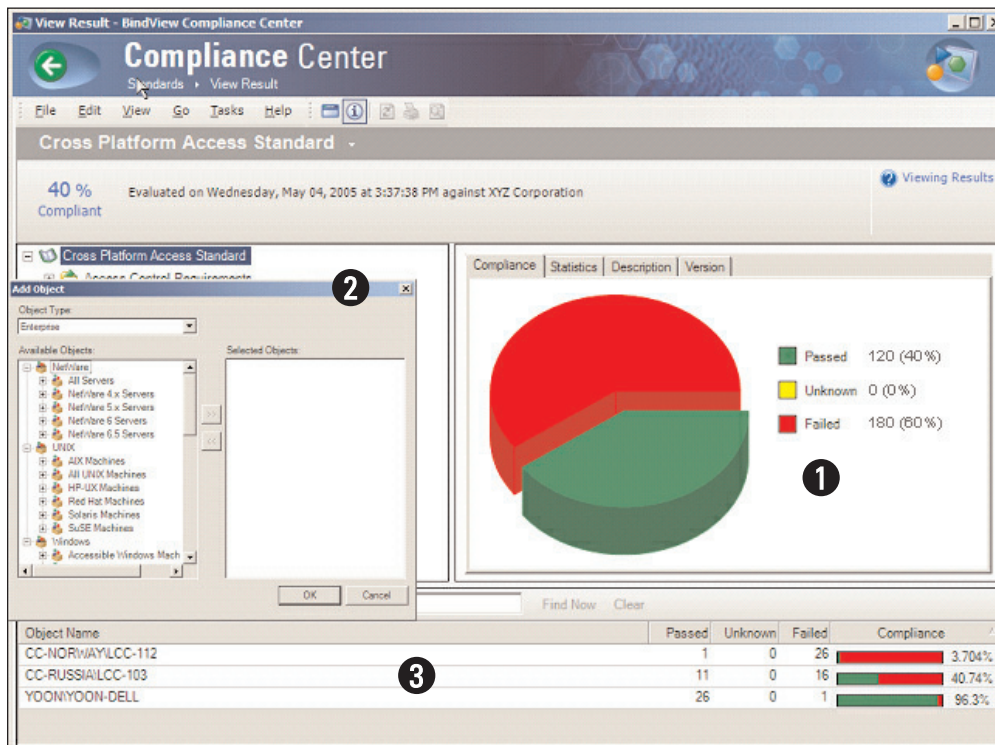
2] COBIT is divided into four general domains with detailed control objectives supporting each high level control objective. Here you see the detail requirements contained within the "Ensure Systems Security" objective, and the "Identification, Authentication and Access" objective within Compliance Center.

3] The lower part of the summary report shows systems that have failed the COBIT report view, ranking the worst systems first. This view can also be customized to show all systems, or only the passed or failed systems.

## REPORT #2

### Logging and Data Collection

Most senior executives do not typically have an accurately summarized and aggregated glimpse into the effectiveness of the organization's internal IT controls. Many receive detailed spreadsheets that are incomprehensible to them and too time-consuming to review. In other cases, IT staff must spend hours in manually rolling up the data for viewing by senior management. Symantec can help reduce the cost and complexity of complying with Sarbanes-Oxley by aggregating the granular results of IT controls and making them available via reports appropriate for a high level audience. Compliance Center helps you assess, monitor, and report on your security status across multiple platforms, making high-level compliance reviews of the entire enterprise easier and more efficient, whether you are gathering and analyzing data for end users or for audit personnel to reduce billable hours.



1] A security or audit director can quickly view a single compliance score covering multiple platforms across the enterprise. Compliance Center reporting supports all major operating systems including Windows®, UNIX®, Linux® and Novell®.

2] Systems can be grouped based on priority, by function, or by geography. Compliance Center makes it easy to create custom groups or collections of systems to fit your environment.

3] The lower part of the summary report shows systems that have failed your overall compliance requirements, ranking the worst systems first. This view can also be customized to show all systems, or only the passed or failed systems.

Keep in mind that Compliance Center can also provide a detailed evaluation of any single system, including a detailed checklist of non-compliant items and a fix report with instructions for how to correct these items. In addition, Compliance Center offers a convenient method for managing exceptions.

**REPORT #3**

**Security Assessments for System Permissions Given to Users (Entitlement Report)**

Symantec provides extensive granularity in implementing SOX controls. For example, accurate Access Control or Entitlement reporting is a crucial area for the COBIT control objective, "Ensuring Systems Security." Under this control objective, a process to periodically review and confirm access rights is required. Symantec Access Control reports take into account not just explicit rights of users and groups but also account for effective privileges through group memberships and cascading rights. Symantec's ability to perform such analysis accurately and with minimal intrusiveness is a key differentiator.

**1]** As illustrated in this report, BindView bv-Control® for Windows® allows you to gather direct and inherited permission data for users and groups with access to the financial directories, and report and export that data for more detailed analysis such as to ensure separation of duties.

**2]** Access security control should be based on the individual's demonstrated need to view, add, change or delete data. This report documents the level of access to financial systems for each user or group, clearly identifying end-user exposure at the operating system level. See report #5 to identify end-user exposure at the application level.

**3]** This report also shows users and groups in the accounting department that have access to the financial directory with full control of the information. Management should review this list periodically to ensure that users and permission levels are appropriate.

<b>1 Entitlement – By Directory – Basic Permissions</b>		
<b>Account Name</b>	<b>Effective Permissions</b>	<b>Group Members</b>
COUNTINGSRV1		
C:\Financials directory		
AD-DOMAIN\Administrators	[Full Control] <b>2</b>	AD-DOMAIN\Administrator AD-DOMAIN\Domain Admins AD-DOMAIN\Enterprise Admins AD-DOMAIN\HSAdmin361971 AD-DOMAIN\HSAdmin482685
AD-DOMAIN\Accounting	[Full Control]	AD-DOMAIN\MStewart AD-DOMAIN\CSmith AD-DOMAIN\HGray AD-DOMAIN\KCountess AD-DOMAIN\LHuffman <b>3</b>
Everyone	Read Execute Delete	[N/A]
C:\Accounts Payable directory		
AD-DOMAIN\Administrators	[Full Control]	AD-DOMAIN\Administrator AD-DOMAIN\Domain Admins AD-DOMAIN\Enterprise Admins AD-DOMAIN\HSAdmin361971 AD-DOMAIN\HSAdmin482685
AD-DOMAIN\Accounting	Read Execute Delete	AD-DOMAIN\MStewart AD-DOMAIN\CSmith AD-DOMAIN\HGray AD-DOMAIN\KCountess AD-DOMAIN\LHuffman
AD-DOMAIN\Controller	Read Execute Delete	AD-DOMAIN\MStewart AD-DOMAIN\CSmith

**REPORT #4**

**Security Assessment for Modifications to Critical System Files**

"Manage Changes" is a control objective under COBIT that examines how an organization modifies system functionality to help meet business objectives. Establishing baseline standards and then monitoring changes to these standards to ensure that any changes are appropriate and approved is an important component to sustain compliance to SOX and other regulations. Monitoring systems to ensure that all changes are authorized and perform as designed is important to establish integrity of the systems that store your financial data. Symantec baseline reports show only objects that have changed from a previous report—saving you time and improving accuracy when comparing report results from one time frame to another.

1] Ensuring system security includes monitoring changes to critical infrastructure files. This report monitors critical system files and identifies when files have been changed, deleted or added. Changes in these files can indicate that a system has been compromised by a hacker, a worm, or a virus.

Symantec baseline reporting lists only those files that have been altered, saving you time and resources for researching masses of data to detect and validate changes to your critical infrastructure upon which financial applications depend.

1 Modifications to Critical System Files						
Status	File Name (With Path)	File Version	Checksum	Size (Bytes)	Last Modified Date/Time	
Machine Name: W 2K3-DC						
Changed	C:\WINDOWS\SYSTEM32\playx.dll	Old Value: 5.2.3790.0 New Value: 5.2.3790.163	Old Value: 237,198 New Value: 258,814	Old Value: 219,136,0000 New Value: 221,184,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 5/7/2004 3:08:32 PM	
Changed	C:\WINDOWS\SYSTEM32\psockx.dll	Old Value: 5.2.3790.0 New Value: 5.2.3790.163	Old Value: 99,580 New Value: 79,723	Old Value: 54,784,0000 New Value: 55,296,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 5/7/2004 3:08:32 PM	
Changed	C:\WINDOWS\SYSTEM32\uctldll	Old Value: 5.4.3790.0 New Value: 5.4.3790.14	Old Value: 130,737 New Value: 129,891	Old Value: 97,280,0000 New Value: 115,808,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 8/25/2003 6:06:50 PM	
Changed	C:\WINDOWS\SYSTEM32\engine.dll	Old Value: 5.4.3790.0 New Value: 5.4.3790.14	Old Value: 234,058 New Value: 194,348	Old Value: 178,688,0000 New Value: 182,880,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 8/25/2003 6:06:50 PM	
Changed	C:\WINDOWS\SYSTEM32\msidl	Old Value: 2.0.3790.0 New Value: 3.1.4000.2435	Old Value: 2,179,232 New Value: 2,313,499	Old Value: 2,160,128,0000 New Value: 2,890,240,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 5/4/2005 2:45:32 PM	
Changed	C:\WINDOWS\SYSTEM32\sisexec.exe	Old Value: 2.0.3790.0 New Value: 3.1.4000.1823	Old Value: 108,616 New Value: 143,546	Old Value: 69,120,0000 New Value: 78,848,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 5/4/2005 2:45:36 PM	
Modifications to Critical System Files						
Status	File Name (With Path)	File Version	Checksum	Size (Bytes)	Last Modified Date/Time	
Changed	C:\WINDOWS\SYSTEM32\slsp.dll	Old Value: 2.0.3790.0 New Value: 3.1.4000.1823	Old Value: 51,093 New Value: 27,080	Old Value: 50,176,0000 New Value: 15,360,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 5/4/2005 2:45:36 PM	
Changed	C:\WINDOWS\SYSTEM32\ndden32.dll	Old Value: 5.2.3790.0 New Value: 5.2.3790.173	Old Value: 58,054 New Value: 26,742	16,896	Old Value: 3/25/2003 7:00:00 AM New Value: 6/16/2004 7:21:03 PM	
Changed	C:\WINDOWS\SYSTEM32\ntide.exe	Old Value: 5.2.3790.0 New Value: 5.2.3790.184	Old Value: 123,032 New Value: 140,014	Old Value: 103,424,0000 New Value: 104,448,0000	Old Value: 3/25/2003 7:00:00 AM New Value: 6/16/2004 6:31:38 PM	
New	C:\WINDOWS\SYSTEM32\000102_tm.p.dll	2.0.3790.0	2,179,232	2,160,128	3/25/2003 7:00:00 AM	
New	C:\WINDOWS\SYSTEM32\pmp.sgd.dll	6.1.22.4	25,766	14,048	3/4/2005 8:30:28 PM	
New	C:\WINDOWS\SYSTEM32\ws03ms.dll	5.2.3790.332	16,848	2,560	5/13/2005 6:54:14 PM	

**REPORT #5**

**Security Assessment for System Permissions Given to Users (Entitlement Report)**

Sarbanes-Oxley requires periodic assessment of systems supporting the financial reporting process. Ensuring the quality and integrity of financial information is the foremost tenet of security compliance for SOX. With significant amounts of data residing in large relational databases, maintaining good security practices on these systems is critical to IT security and audit directors. Using bv-Control® for Oracle®, for example, you can validate the configuration of Oracle databases against internal security standards. You can assess separation of duties in the database and report on the level and extent of access to sensitive corporate data.

1] Excessive rights to database applications can provide a back door into those same applications even though access controls are established by an ERP system. This report shows a list of users with access to the vendor table in the Accounts Payable database and the level of privilege for each user. Inappropriate access to an Accounts Payable vendor table could lead to the creation of fraudulent vendor accounts or increasing the credit limit for a questionable vendor.

2] Management should review access levels on a regular basis to ensure the integrity of data, and confirm that permissions are appropriate. Symantec can also give IT the forensic information needed to support changing user permissions.

3] Good security requires strong passwords. In this example report you can see that several users are still using default passwords to access critical data.

**1 Privileges on the Accounts Payable Database Table**

Server Name	Database Name	Object Name <b>2</b>	Privilege Grantee	Privilege Name
Accounting_Server	BVCO9U	Vendor	AP_ADMINISTRATOR	SELECT
Accounting_Server	BVCO9U	Vendor	MANAGER	DELETE
Accounting_Server	BVCO9U	Vendor	MANAGER	INSERT
Accounting_Server	BVCO9U	Vendor	MANAGER	SELECT
Accounting_Server	BVCO9U	Vendor	MANAGER	UPDATE

**3 DEFAULT PASSWORDS**

Prepared by: AD\jchancha  
Sorted by: Ascending Server Name  
Filtered on: Is Default Password? Is True  
Scope: Default

Printed on 2/15/2005, 5:08 PM

Server Name	Database Name	User Name	Is Default Password?	Account Status
ORACLE	BVCO9U	OUTLN	Yes	Open
ORACLE	BVCO9U	OBSNMP	Yes	Open
ORACLE	BVCO9U	HR	Yes	Open
FINANCIAL DB	BVCO9	OBSNMP	Yes	Open
FINANCIAL DB	BVCO9	SCOTT	Yes	Open
FINANCIAL DB	BVCO9	HR	Yes	Open
FINANCIAL DB	BVCO9	OUTLN	Yes	Expired & Locked
FINANCIAL DB	BVCO9	ORDSYS	Yes	Expired & Locked
FINANCIAL DB	BVCO9	ORDPLUGINS	Yes	Expired & Locked
FINANCIAL DB	BVCO9	MDSYS	Yes	Expired & Locked
FINANCIAL DB	BVCO9	OLAPSYS	Yes	Expired & Locked
FINANCIAL DB	BVCO9	RMAN	Yes	Expired & Locked

## About Symantec

Symantec is the world leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, California, Symantec has operations in 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745-6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517-8000  
1 (800) 721-3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.  
01/06

10527722