IPLOCKS WHITE PAPER

February 2006

IPLocks Addresses Sarbanes-Oxley: A Regulatory Compliance Solution

2665 North First Street, Suite 110 | San Jose, CA 95134 | Telephone: 408.383.7500 | www.iplocks.com

TABLE OF CONTENTS

INTRODUCTION

The Sarbanes-Oxley Act (SOX)[1] is undisputedly one of the most important regulations that companies struggle to comply with. Discerning how and where to employ policies that enforce financial controls proves to be a daunting task. Even more troublesome, is understanding which controls need to be implemented in order to enforce processes and data integrity in the Information Technology (IT) subsystems and the applications that public companies rely on to automate financial processes. Although SOX does not dictate which controls are required, many companies have used the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Control Objectives for Information and Related Technologies (CobiT) frameworks as steps toward meeting SOX compliance. Since the accuracy of financial statements is directly associated with the security and control of financial data, IT must implement a strategy to ensure that the databases which provide information to financial applications have not been manipulated.

In this document, we will discuss the often overlooked but required area of database controls. Many of IPLocks' customers, who were initially comfortable with the implementation of strong business process enforcement, were surprised to fail an audit or find significant material weaknesses in their IT subsystems. Without an automated database security solution, important database changes and policy breaches could easily go unnoticed, affecting the reliability of financial data. The IPLocks Database Security and Compliance Solution provides vulnerability assessment, continuous monitoring, and auditing to aid companies in their compliance efforts by ensuring proper controls are in place and enforced *(Appendix A)*.

WHAT IS SARBANES-OXLEY?

SOX was created to protect investors by improving the accuracy and reliability of corporate disclosures. Motivated by corporate financial scandals, including those at Enron, Tyco International, and WorldCom, SOX reviewed outdated legislative audit requirements and mandated new, stringent financial reporting requirements for companies doing business in the United States. SOX is considered the most significant change to federal securities laws since the 1930s.

[1] Officially titled the "Public Company Accounting Reform and Investor Protection Act of 2002", but commonly called SOX, it was signed into law on July 30, 2002.

The act requires:

- Public companies to establish accounting oversight boards
- Financial auditors to be independent of the audited company
- Executives to be responsible and legally liable for correct financial reporting
- Disclosure of additional accounting practices and transactions

WHAT EFFECT DOES SOX HAVE ON INFORMATION TECHNOLOGY?

Since 2002, much has been written on SOX and the importance it places on internal financial controls, but very little on the role that IT must play in fulfilling these requirements. Most IT professionals would agree that the reliability of financial reporting is dependent upon a well-controlled, highly secure IT environment. Since the most critical business processes are automated through financial, ERP or sales automation applications, and the vast majority of business information resides within databases, an audit of processes and controls must also include an audit of the IT subsystems that provision and generate financial reports.

WHAT DOES COSO AND COBIT HAVE TO DO WITH SOX?

Professional organizations dedicated to examining the common causes of fraudulent accounting practices founded COSO in 1985.

CobiT is a framework for information security and control created by the Information Systems Audit and Control Association (ISACA). The process of converting abstract financial processes to IT systems control is contained in CobiT framework and is the de-facto standard used to address IT specific issues required to pass a SOX audit. This framework covers all areas of IT and each phase of the compliance lifecycle.

While SOX does not specifically dictate which controls or methodology to employ, most companies have adopted the "COSO Framework" for process controls and the "CobiT Framework" for IT controls as steps to aid in SOX compliance.

WHAT DOES THE DATABASE HAVE TO DO WITH SOX COMPLIANCE?

Since the majority of financial processes are automated within financial software, the review of processes and controls must also include a review of the logic, control, and access to the financial software, and its underlying systems. Every major accounting and financial software package relies on a database; the two are inextricably linked. The database not only contains all data processed within the application, but much of the logic and functional controls.

In order to comply with SOX, companies need to focus efforts on assessment, controls, and audits within the financial databases.

HOW DOES IPLOCKS HELP WITH SOX COMPLIANCE?

Achieving SOX compliance is top priority for companies who undergo annual audits. By monitoring and auditing all activities, the IPLocks Database Security and Compliance Solution assists companies in meeting regulatory requirements. Adding IT controls to automated business processes make IT more efficient, secure, and accountable. The IPLocks Solution offers several features that ensure proper controls are in place and consistent over time, thereby improving management and efficiency of strategic data sources.

SOX demands controls for people, process, and technology, and IPLocks provides those controls from the database perspective

DATABASE CONTROLS PROVIDED BY IPLOCKS

People	*Process*	*Technology*
Periodic verification of permissions, roles, and groups	**Alert to violation of business rules or controls**	**Check databases security settings**
Alert to changes in permissions	**Alert on change to process or stored procedure**	**Check database patch levels**
Alert to failed logins	**Alert when auditing is turned off**	**Check for unneeded database services**
Track changes in passwords	**Alert on suspicious content changes**	**Track changes to metadata**
Track OS and database users	**Track access and changes to sensitive data**	**Track change history**
Track activity against database objects	**Track access and changes to sensitive objects**	**Alert on unapproved application connections**
Provide separation of duties	**Verify a process or stored procedure executed**	
Show locked accounts		

CASE STUDIES

The following case studies are three real-world examples of the types of review, enforcement, audit, and reports that IPLocks provides its customers. These case studies demonstrate how the IPLocks Database Security and Compliance Solution enhances specific IT controls and verifies that these controls are consistent.

CASE STUDY A: INSURANCE AND FINANCIAL COMPANY

BACKGROUND

This customer is a global insurance and financial services company in the process of completing the second round of SOX compliance. The company has thousands of databases world-wide, many of which contain financial data used to produce financial reports. The customer needed to augment its current policy enforcement to include the database servers. The objective was to validate and monitor their database servers to verify policy enforcement. One challenge was to address this requirement consistently across several major geographically dispersed, databases servers.

A COMPREHENSIVE SOLUTION MEETING FUNCTIONAL COMPLIANCE REQUIREMENTS

Although several software vendors offered individual point solutions, IPLocks was the only comprehensive solution offering assessment, continuous monitoring, and auditing required to meet the functional compliance requirements.

A combination of native database features with custom developed in-house scripts were also considered, but the cost-savings, ease of deployment, and performance advantage offered by IPLocks provided a better ROI than a 'home grown' solution.

IPLocks was the only solution that provided the full range of security and audit across all required relational database platforms, including DB2 Mainframe, DB2 UDB, Oracle, and SQL Server.

REQUIREMENTS MET WITH IPLOCKS

Requirements	*Regulatory Requirements*
Verify authorized changes to structure of production databases (Add or alter).	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Supervision of local IT**
Alert any changes to structure to verify no unauthorized changes are made.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Centralized monitoring of operations, local monitoring of operations or security**
Track all changes to data in certain columns related to financial statements.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Monitoring, manage data**
Track all password changes (Who and When).	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Control activities and access**
Track and log database configuration changes.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage the configuration**
Periodic report on changes to stored procedures and functions.	• **SOX Section 404.b: Audit and review effectiveness of controls** • **CobiT: Manage changes, operational security**

chart continued, next page.

Requirements (Con't.)	*Regulatory Requirements (Con't.)*
Periodic review of user roles, groups and permissions.	• **SOX Section 404.b: Audit and review effectiveness of controls** • **CobiT: Adequacy of internal controls**
Periodic review of patch levels and configuration.	• **SOX Section 404.b: Audit and review effectiveness of controls** • **CobiT: Manage operations, independent assurance**

PROCESS AND IMPLEMENTATION

The SOX team identified each of the databases involved in financial reporting. Based upon previous risk analysis, the team knew it needed to enforce basic security requirements for their financial databases and user accounts *(Figure 1)*. The IPLocks Solution addressed these requirement by:

- Verifying that operational controls, configuration settings, and database security patches were applied on a periodic basis
- Tracking changes to permissions, user passwords, structures, and data

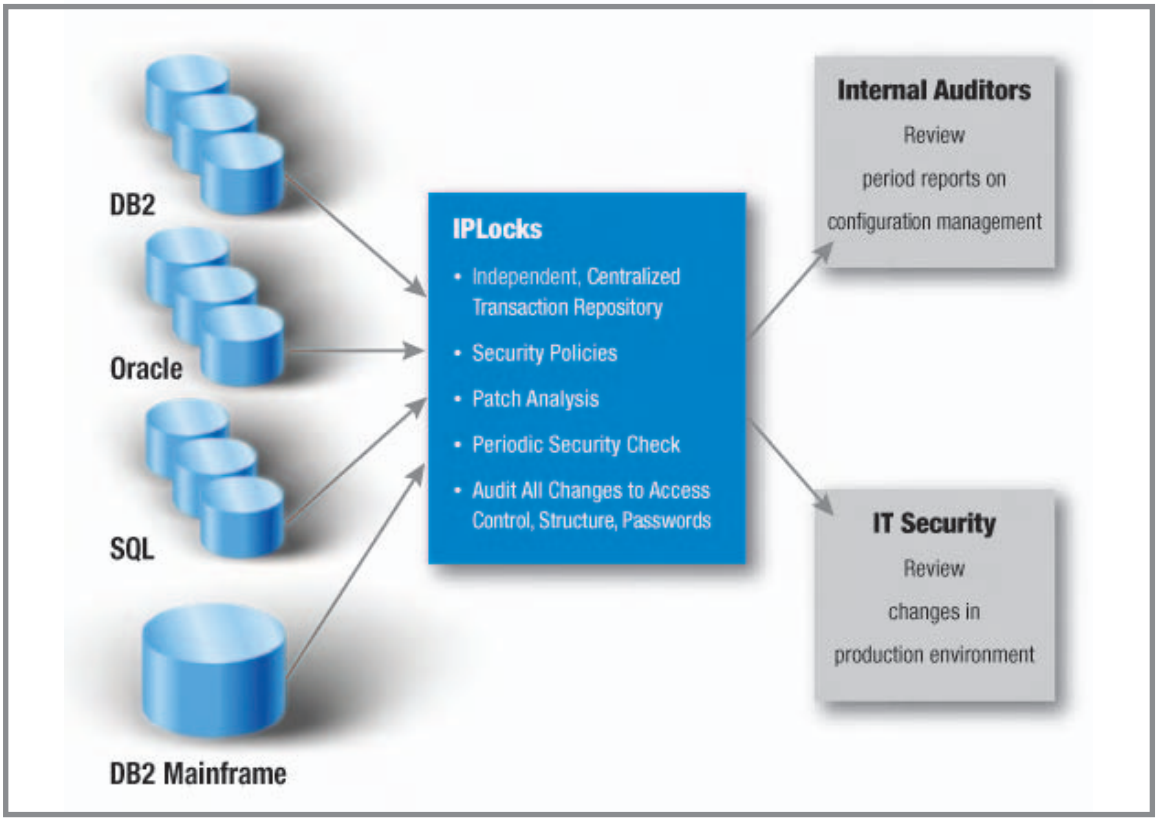

Figure 1: The IPLocks process for Internal Auditors and IT Security.

AREAS OF COMPLIANCE

SOX Section 404 and 302 outline management's responsibilities to effectively establish controls to financial data, and to certify financial statements.

SOX Section 404 outlines management's responsibility for:

- Building effective internal controls over financial reporting
- Detecting unauthorized acquisition
- Using or allocating assets
- Disclosing any associated material weaknesses potentially effecting financial statements

SOX Section 302 describes management's responsibility to certify all financial statements.

Specific CobiT recommendations for IT Services include:

- Controlling and verifying access
- Enforcing system maintenance
- Providing physical and logical security
- Ensuring data management
- Providing incident response

To meet these requirements, IPLocks assesses the basic security and configuration to ensure that industry best practices are being followed. The IPLocks Solution provides a gap analysis of all major relational database platforms used by financial, accounting, and business applications and illustrates specific areas of weakness prior to an audit. It provides a list of current patches that need to be applied for both system maintenance and security. IPLocks works with database vendors, security organizations, and auditors to compile a list of known best practices to ensure the database meets the minimum recommended guidelines.

A critical step in the compliance process is identifying relevant risks to the IT systems. Doing so requires the ability to monitor, detect, and record electronic information disclosures. The IPLocks Database Security and Compliance Solution fulfills SOX compliance by:

- Providing risk assessment under the planning phase of SOX compliance
- Identifying infrastructure and monitoring changes during implementation phases
- Helping with systems security
- Managing database configuration
- Monitoring process and controls
- Provides for an independent audit

EXAMPLES

The following illustrations show several customer required reports and alerts. Some of these reports are viewed periodically, while others require attention on an 'as generated' basis. In most cases, the setup steps involve turning on standard IPLocks policies and connecting to the desired database.

All reports contain a summary and detailed format. Policy violations are stored in the IPLocks repository and distributed via email or SNMP, providing centralized and distributed event notifications.

This sample report shows captured changes to a database structure *(Figure 2)*. By using a pre-existing rule from the Metadata Monitor, IPLocks reports the changes to the metadata. The summary list of alerts contain specific information, such as who issued what command, on what table, and when it was issued.

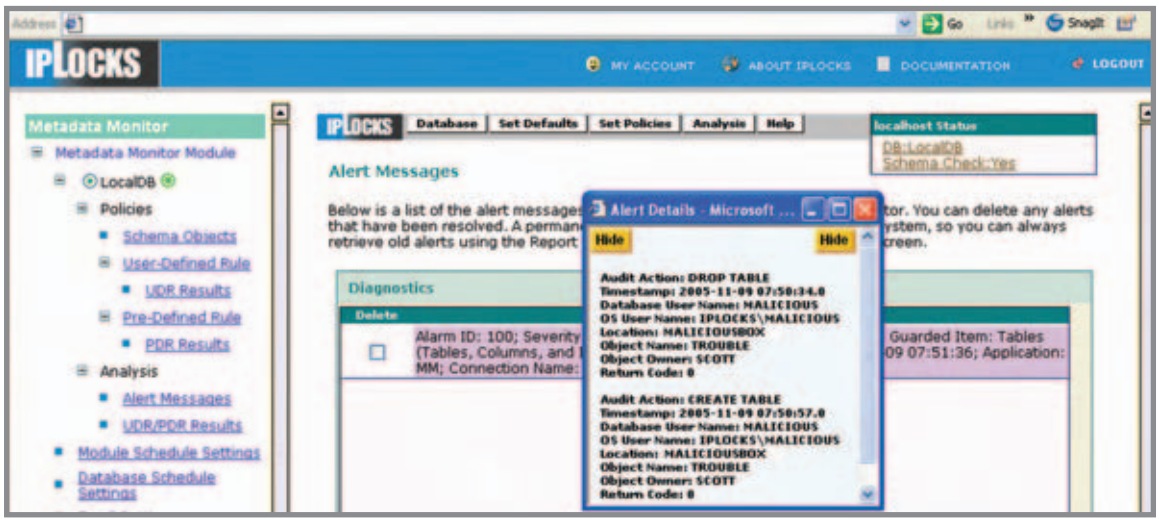

Figure 2: Metadata Monitor Alert.

In order to periodically assess the databases across the enterprise, the IPLocks Solution interrogates the database for configuration and patch level information. It then generates database and global reports on how well the configuration matches industry best practices *(Figure 3)*.

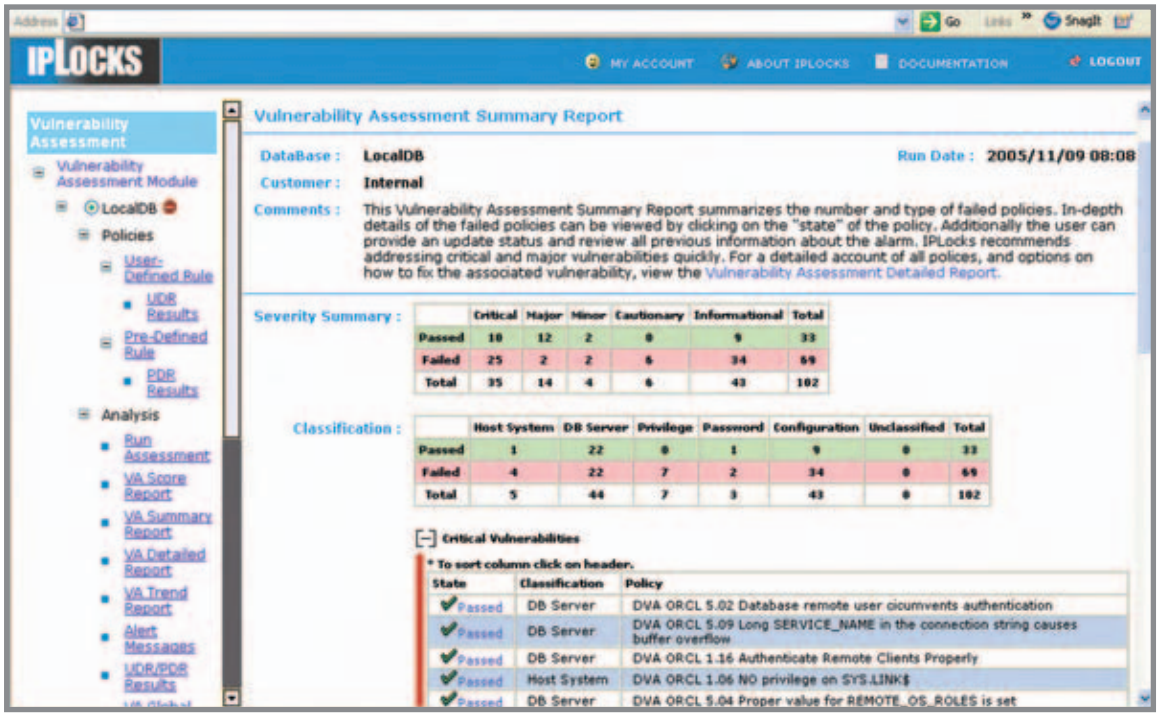

Figure 3: IPLocks Vulnerability Assessment Solution Sample Report.

CASE STUDY B: SOFTWARE VENDOR

BACKGROUND

This customer is a major software vendor using SAP and Oracle financial applications for their internal accounting systems. They run several different database platforms, including DB2 UDB, Oracle, and SQL Server, to support these applications. After completing the first round of SOX implementation, several deficiencies in policy enforcement and in the separation of duties between data collection and review were found.

CONSISTENCY, ASSURANCE, AND LOW OVERHEAD TRANSLATES INTO SIGNIFICANT ADVANTAGES

IPLocks offered several advantages that appealed to this customer:

- ***Consistent monitoring.*** The ability to monitor and produce reports on all databases that served financial applications.
- ***Assurance of timely reporting to management.*** The capability to alert on suspicious activity in near real-time, rather than in days or weeks.
- ***Implementation without risk to productivity.*** Although the customer was auditing all metadata and user changes, the overhead to their financial databases was less than 3% of CPU and network utilization. This was a major factor in their decision to deploy the IPLocks Solution.

REQUIREMENTS MET WITH IPLOCKS

Requirements	*Regulatory Requirements*
Show all changes to user permissions, roles or groups that would allow a user to exercise control outside of the developed policies.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage operations, manage changes, monitoring**
Ensure all of the changes to meta-data and users are seen to prevent an unapproved change.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage changes, monitoring of security**
List all changes to the structure of the production database to ensure the applications function normally.	• **SOX Section 404.b: Audit and review effectiveness of controls** • **CobiT: Manage operations, independent assurance**
Facilitate separation of duties between data collection and data review.	• **SOX Section 404.b: Audit and review effectiveness of controls** • **CobiT: Manage operations, monitoring**

PROCESS AND IMPLEMENTATION

The SOX team devised new policies, as well as a process for enforcing separation of duties, and sent them to analysts and database administrators (DBAs) for implementation. The analysts required data and reports from the database, but access controls prevented them from directly accessing the system. The DBAs' actions, including changes, required independent review and verification from tampering in controls, application logic, and database structures—all of which needed to be independently reviewed.

The delineation between creating and verifying reports provided the customer with the separation of duties that SOX required. IPLocks provided an independent record of events and enabled both parties to perform their respective roles. The reports were then presented to internal and external auditors, demonstrating that the controls were in place.

It was also required that this customer monitor database structural changes. Figure 4 illustrates how changes to the production financial system were monitored to ensure approved changes were made. These changes were independently verified, and the results stored for auditors to inspect.

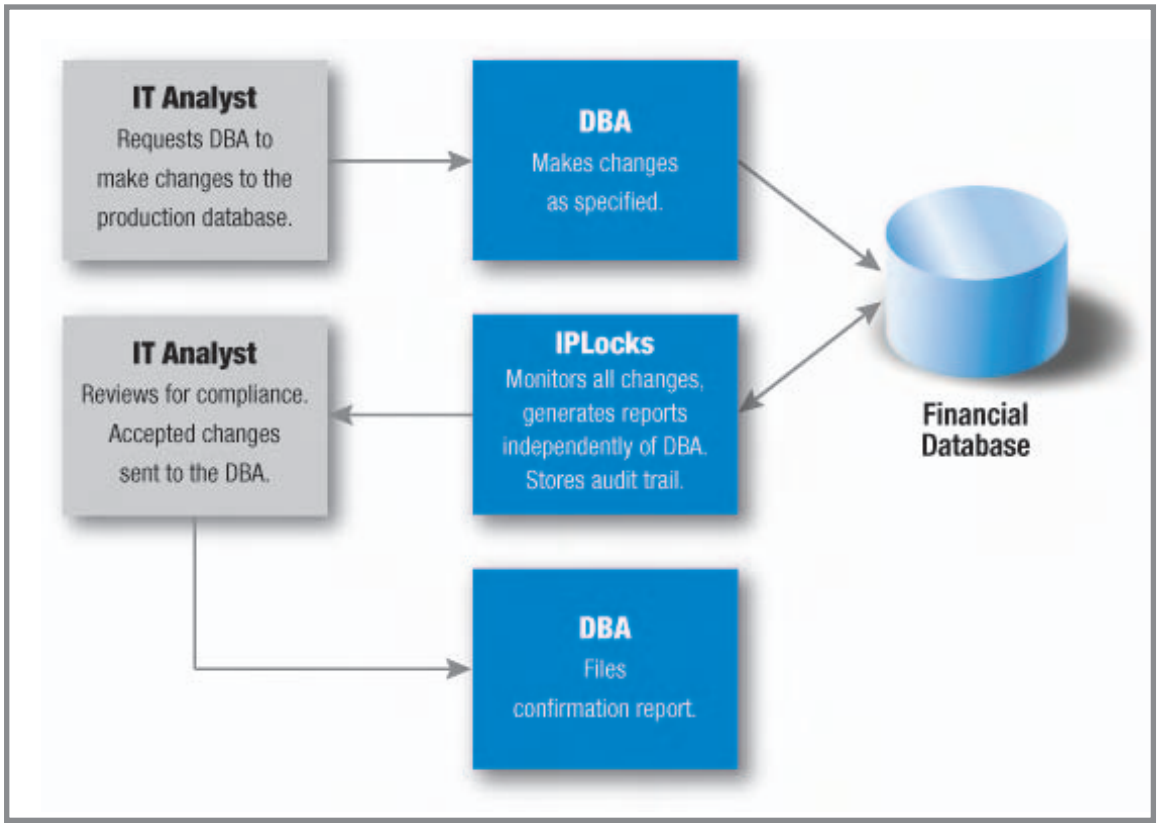

Figure 4: Change and Confirmation Process.

Another area of significant interest was Access Control verification. The IPLocks Database Security and Compliance Solution independently audits the changes to database permissions and creates several important reports for compliance. These included:

- A monthly review showing users of every group and role, providing a complete report on the access of each database used
- An alert report on changes in permissions, groups, or roles on the production database server

Both of these reports were sent to the regulatory officer to be reviewed for:

- Verification of changes
- Assurance that no one received access to data that they should not have
- The accounting of illegal iterative changes that are not part of the monthly report

The workflow looked like this *(Figure 5)*:

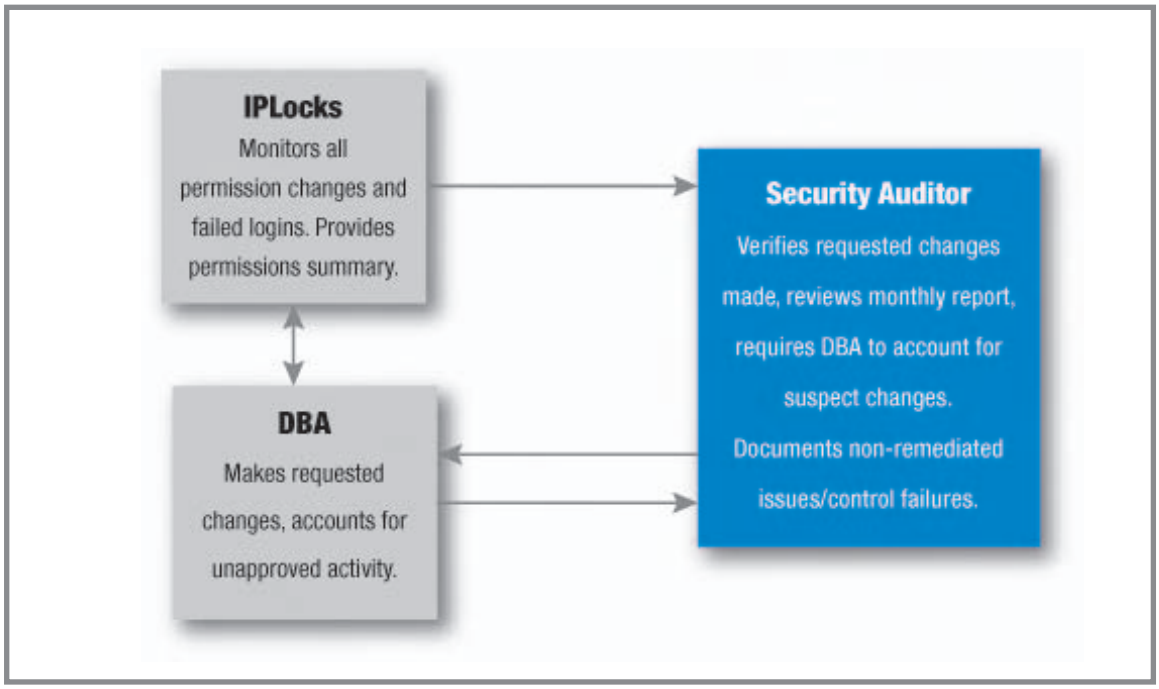

Figure 5: IPLocks Workflow Process.

AREAS OF COMPLIANCE

A critical step in the compliance process is identifying relevant risks to the IT systems. The IPLocks Database Security and Compliance Solution fulfills SOX compliance under the COSO and CobiT frameworks by:

- Providing risk assessment under this planning phase of SOX compliance
- Identifying infrastructure and monitoring changes during implementation phases
- Helping with systems security
- Managing database configuration
- Assisting with the delivery and support of a SOX strategy

Four of the thirty-four IT processes identified and mapped from COSO related to the continuous operational issues of monitoring and evaluating. Specifically, those four items are:

- Monitoring processes
- Assessing internal control adequacy
- Obtaining independent assurance
- Providing independent audits

It is advised under SOX Section 302 that auditors inquire about significant changes to the design or operation of controls over financial reporting. Examples of these include:

- Those who have gained access to reports
- Where data was collected from and when
- Consistency of data, functions, and structure
- Proof of the separation of duties

These rules may be enforced through access control, groups and roles, or they may constitute rules implemented as triggers or stored procedures that enforce data consistency. This may necessitate verification that certain rules have not changed over time.

The IPLocks Database Security and Compliance Solution was designed to continuously observe transactions and monitor database events. Monitoring establishes that policies have not been violated and that structures and rules remain intact. For example, the IPLocks User Behavior Monitor verifies that the approved user performed the appropriate transaction and that all business rules were followed.

The IPLocks Metadata Monitor tracks and alerts changes to database structures required for the Control Environment sub-grouping of the COSO standard.

IPLocks Permissions Monitor detects and alerts changes to user permissions that may violate separation of duty policies under Control Activity sub-grouping of the COSO standard.

EXAMPLES

The following example illustrates how IPLocks alerts on changes to the database schema *(Figure 6)*. The IPLocks Metadata Monitor generates reports and email alerts when changes to objects within the database are made. Adding a new table to the production environment generated the following alert:

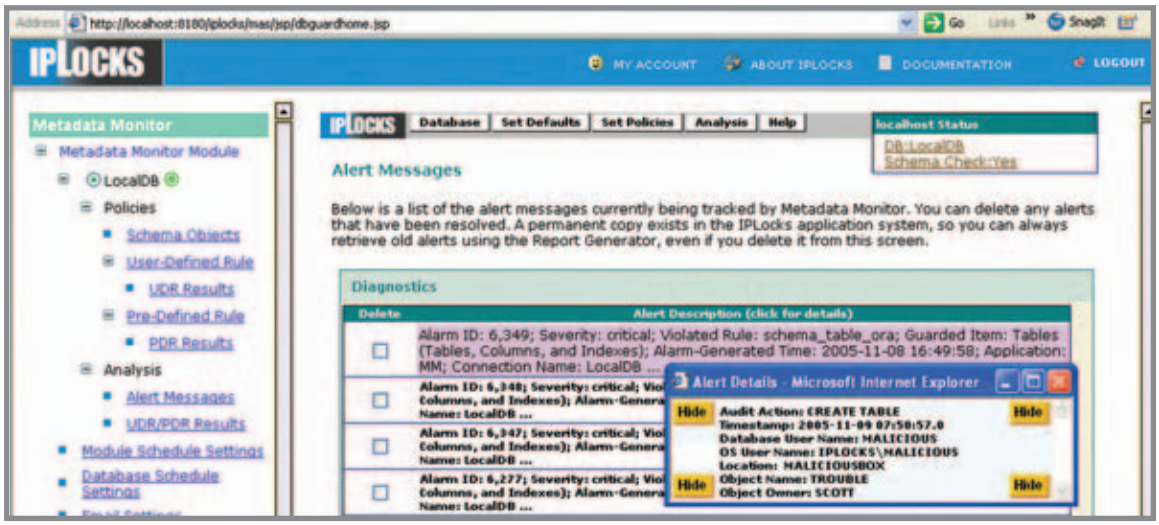

Figure 6: Metadata Monitor Alert Message.

Privilege Summary reports permissions for all users on the target database, whether assigned directly or indirectly. This summary can be viewed by user or by role. The output is as follows *(Figure 7)*:

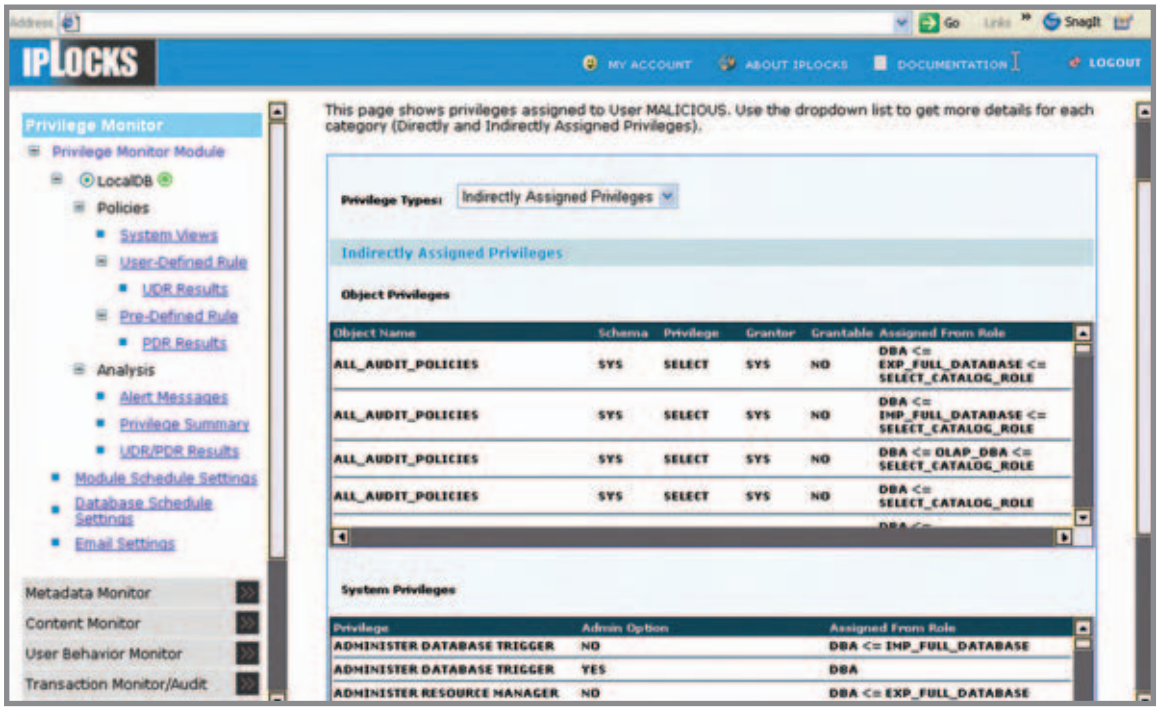

Figure 7: IPLocks Privilege Summary Report.

The IPLocks Privilege Monitor provides several pre-defined rules to track permissions-related changes in order to track user account creation and modification on the production database. The following example displays the "No 'alter user'" predefined rule and captures every command that alters a user account or grants a user additional privileges *(Figure 8)*.

Figure 8: Privilege Monitor Alert.

CASE STUDY C: FINANCIAL SERVICES FIRM

BACKGROUND

This customer is a public financial services firm running an ERP application for tracking sales and compensation. The company was primarily concerned with monitoring data changes in critical areas, as well as ensuring the privacy of data. They required a complete audit trail of changes to ensure that no data change would go unnoticed. The customer uses Oracle databases in a Real Application Clusters (RAC) configuration and specifically wanted to know who, what, where, and when the changes were occurring.

IPLOCKS AUTOMATES AUDITING PROCESS AND IMPROVES DATA ACCURACY

The customer discovered anomalous changes to data in their ERP database. As changes were being made from the database console, they went undetected by the network-based security tool. This material breach was later discovered by a database audit trail analysis, which consisted of a manual inspection of the audit logs. Since this manual breach discovery was tedious and time consuming, the company decided to implement an automated solution to discover future breaches and provide better log file analysis.

The IPLocks Database Security and Compliance Solution examined the company's transaction logs and system tables. This provided a complete picture of database modifications with which the company could accurately audit all transactions. IPLocks also keeps a verifiable copy of all required transactions thus providing for an independent audit. The accuracy of the data was considered more important than the minor performance impact to the target database platform.

REQUIREMENTS MET WITH IPLOCKS

Requirements	*Regulatory Requirements*
Immediately alert on permissions changes, including groups or roles.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage operations, manage changes, monitoring security**
Track all changes to salary and commissions columns.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage data, manage changes**
Validate data ranges of salary and commissions.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage operations, manage changes, manage data, monitoring**
Alert if auditing is shut off.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage operations, manage changes, monitoring, ensure security**
Audit transactions outside 'normal' business hours.	• **SOX Section 404.b: Audit and review effectiveness of controls** • **CobiT: Manage operations, independent assurance**
Detect the use of the Export command on Oracle database.	• **SOX Section 404.a: Establish and maintain controls** • **CobiT: Manage operations, manage changes monitoring**

AREAS OF COMPLIANCE

SOX Section 802 states, “Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any records, documents, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any department or agency of the U.S. ... or contemplation of any such matter or case, shall be fined ... imprisoned not more than 20 years, or both.”

If a company’s IT security is weak, controls can be altered or bypassed by malicious or negligent individuals. If the controls are bypassed, the resultant data is meaningless in terms of judging the effectiveness of the control. An assessment, however, would demonstrate whether the basic configuration and security had been altered.

While IT professionals are familiar with the applications and databases they manage, they are typically not SOX experts. By implementing the IPLocks Solution, this customer was able to achieve an automated compliance investigation which reported variances that needed to be addressed.

IPLocks provided an independent audit of transactions and activity for later review by capturing the data logs and copying relevant events to a secure, independent repository. IPLocks customizable reporting allowed the company to generate a report of successful and failed login activity, incidents of potential fraud, and security controls documenting the adequacy of security measures.

IPLocks also furnished a Privilege Summary Report listing user and group permissions which demonstrated the separation of duties and documented known deficiencies and weaknesses as required by SOX.

The IPLocks Reports included a trend analysis report which demonstrated sustained compliance to the auditor.

EXAMPLES

The following customer example demonstrates how IPLocks tracks access and modifications to specific columns in the database *(Figure 9)*. In this example, the customer is interested in tracking and reporting changes to the salary and commissions columns of the Oracle HR database. Through the use of the User Behavior Monitor, IPLocks reviews changes at the column level and filters out those events that do not involve sensitive data.

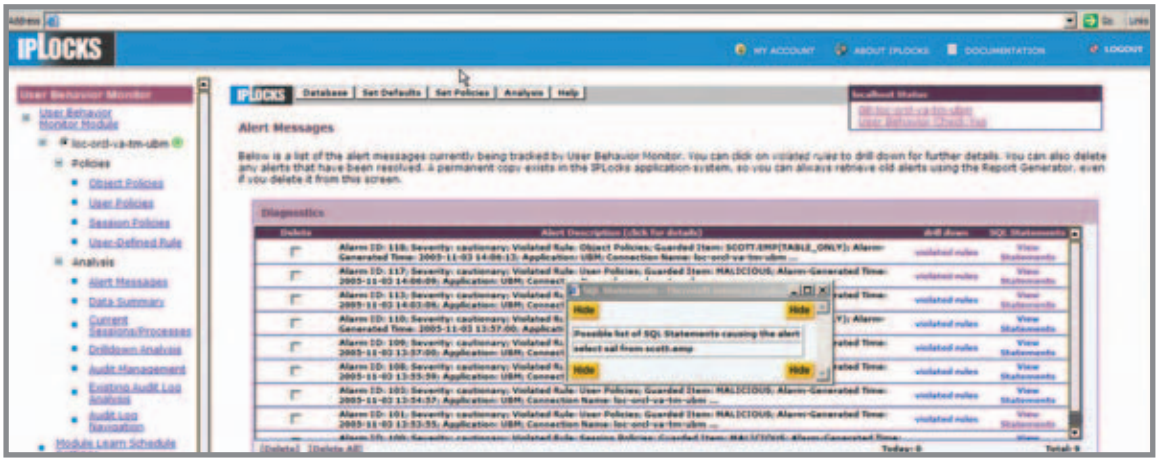

Figure 9: Column Level Monitoring.

Another way the customer protected sensitive financial data was to monitor specific columns in the database for unusual data entries. Since a complete audit was only conducted on a quarterly basis, the customer utilized IPLocks to be alerted to erroneous entries in a more timely manner. In this case, several columns were tracked with the IPLocks Content Monitor to alert on any changes involving monetary amounts that were outside the typical transaction size *(Figure 10)*. This dynamic content validation alerted the accounting department of potential issues and to take corrective action.

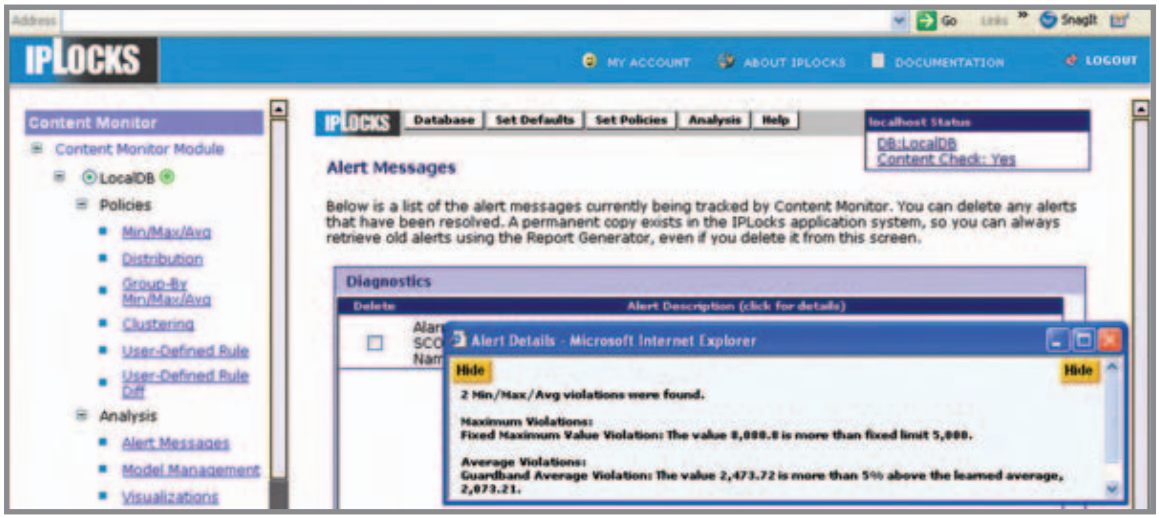

Figure 10: Content Monitoring.

SUMMARY

In accordance with the SOX requirement, IPLocks obtains an independent assessment that reports whether environmental controls are in place and activity is being monitored. With IPLocks forensic auditing, all database activity is recorded and stored in the IPLocks internal repository for later analysis and reporting. This provides an independent repository for activity with the ability to generate ad-hoc reports on activity, security, and data integrity. By collecting all activities on users, data objects, processes, and structure, IPLocks forensically provides proof of concept to auditors.

Beyond simple reporting and managing, IPLocks provides a data-centric view to managing intellectual property within the enterprise and the proactive capability to respond and resolve security and process enforcement problems as they occur. IPLocks works to ensure that business process and security best practices are implemented, enforced, and appropriate to the regulatory challenge. With our patented behavioral and content monitoring, IPLocks tracks the usage of business assets, differentiates appropriate from inappropriate activity, and takes action when policies are violated. IPLocks provides an essential key to successfully meeting Sarbanes-Oxley compliance by bundling people, process, and technology under a common policy umbrella.

APPENDIX A

IPLocks Relationship to CobiT	IPLOCKS SOLUTION *Vulnerability Assessment*			
	ASSESSMENT	**PRIVILEGE SUMMARY**	**MONITORING**	**AUDITING**
PLAN AND ORGANIZE				
Define a strategic IT plan				
Define the information architecture	●			
Determine technological direction				
Determine the IT organization and relationships				
Manage the IT investment				
Communicate management aims and direction				
Manage human resources				
Ensure compliance with external requirements				
Assess risks	●		●	
Manage projects				
Manage quality				
ACQUIRE AND IMPLEMENT				
Identify automated solutions				
Acquire and maintain application software	●			
Acquire and maintain technology infrastructure				
Develop and maintain procedures				
Install and accredit systems				
Manage changes	●		●	
DELIVER AND SUPPORT				
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				
Monitor the process			●	●
Assess internal control adequacy	●	●	●	●
Obtain independent assurance	●		●	●
Provide for an independent audit	●		●	●

IPLocks Vulnerability Assessment Solution is available stand-alone, or as part of the IPLocks Database Security and Compliance Solution.

ABOUT IPLOCKS

IPLocks, Inc. is the leading provider of database security and information risk management solutions. The company works with enterprises worldwide to protect critical information assets from negligent and malicious user threats, manage database security policy vulnerabilities, ease the pain of compliance and to protect privacy. San Jose, California-based IPLocks is a privately held global corporation with customers throughout North America, Asia Pacific, South America, and Europe. For additional information, visit www.iplocks.com

IPLocks and the IPLocks logo are trademarks of IPLocks, Inc. All rights reserved. Any unauthorized use or reproduction of the IPLocks logo is prohibited. ©2006 IPLocks, Inc.

Rev 2 2/06