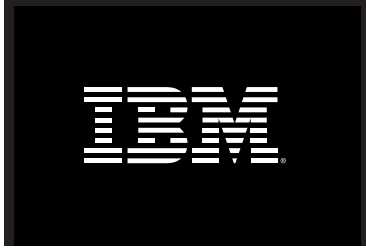
IBM compliance solutions
White paper

Tivoli® software



Addressing the key implications of Sarbanes-Oxley.

September 2004

Contents

Introduction

The Sarbanes-Oxley Act of 2002 (SOX) introduced significant changes to financial practice and corporate management regulation. Passed in the wake of numerous corporate scandals, SOX is a complex piece of legislation that requires companies to make major changes to bring their organizations into compliance. The act holds top executives personally responsible for the accuracy and timeliness of their company's financial data – under threat of criminal prosecution. Thus, SOX compliance has become a top priority for publicly traded companies.

The act also sets deadlines for compliance, all of which will take effect during the next two years. Of the sections already in effect, the most publicized has been Section 302, implemented in August 2002, which requires CEOs and CFOs to personally certify quarterly and annual financial statements. The first indictment of a CEO for failure to comply with the act occurred in 2003. This is just the tip of the iceberg – violating SOX can bring fines up to $5 million or 20 years in prison.

Smart companies recognize that Sarbanes-Oxley presents an opportunity to improve information management and increase efficiency. According to the technology research firm The META Group Inc., "Many firms will utilize the Sarbanes-Oxley Act as a means of improving business efficiency, going beyond what is merely required to comply … Forty-nine percent of firms polled believe SOX is a necessary cost of doing business and 39 percent say it will eventually make them more competitive."* For business leaders who recognize that change is both a challenge and an opportunity, SOX represents a gateway to bigger and better things. The trick is to comply and use compliance as a lever for positioning your company for maximum business effectiveness and continued success during the long term. Even private companies not bound by the law often are adopting SOX as a template for their internal data retention, control and management practices. By looking beyond details of compliance, your company can leverage SOX initiatives to build an on demand environment that has the flexibility to respond quickly to changes in your business environment. This paper highlights some key requirements of

SOX, their effects on IT departments and how IBM solutions can help you optimize your business practices.

IT challenges

A recommended control framework: COSO, COBIT and ITIL

In its final rule for SOX, the United States Securities and Exchange Commission (SEC) mandated that a company's internal control of financial reporting must be based on a recognized internal control framework. On May 23, 2003, the SEC defined in final ruling 2003-66 the requirements for reporting on internal controls (www.sec.gov/news/press/2003-66.htm).

"Under the final rules, management's annual internal control report will have to contain:

- *a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;*
- *a statement identifying the framework used by management to evaluate the effectiveness of this internal control;*
- *management's assessment of the effectiveness of this internal control as of the end of the company's most recent fiscal year; and*
- *a statement that its auditor has issued an attestation report on management's assessment.*"

The rule referred specifically to the framework created by the Committee of the Sponsoring Organizations of the Treadway Committee (COSO) and suggests its use as a model framework (the COSO official Web site is at www.coso.org). By requiring a company to adopt an internal control *framework* for its control environment, the SEC merely requires a *systematic process methodology* for evaluating internal control over financial reporting. Evidence of this systemization comes in the form of policy and procedure guidelines, reports and process documentation including audit logs and reports detailing conformance to the policies and procedures. A COSO evaluation is principally about *documenting* what a company does to

Highlights

support the five steps of the COSO internal controls methodology and providing supporting materials broken down by each step. The COSO Framework contemplates satisfying the intent of each of the five steps: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. According to the "SEC Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports" (August 14, 2003), the scope of internal control includes "policies, plans, procedures, processes, systems, activities, functions, projects, initiatives, and endeavors of all types at all levels of a company."

IT managers need detailed guidelines to establish, document and evaluate their company's controls

The importance of IT controls is implicit in the COSO internal control framework, but IT managers need detailed guidelines to establish, document and evaluate their company's controls. Of the IT control frameworks available, the model of choice among many external auditors is Control Objectives for Information and Related Technology (COBIT) – a general computer control framework developed by the IT Governance Institute (the COBIT official Web site is at www.itgi.org).

The detailed COBIT control objectives align with COSO and define its controls from an IT perspective. The framework incorporates Information Technology Infrastructure Library (ITIL) best practices for service delivery and support (the ITIL official Web site is at www.itil.co.uk). COBIT can help IT managers address specific control objectives for SOX compliance.

SOX IT challenges

A critical SOX IT challenge is to manage vast and ever-increasing amounts of business data and information in ways that verify accuracy. IT managers want technology solutions that satisfy control requirements without sacrificing performance.

Your systems and infrastructure should incorporate several specific capabilities. Your technology should facilitate establishment, monitoring and documentation of internal controls and data management – in a way that provides proof of effective controls. Information management processes

Highlights

should contain scrupulous access controls and protect data, business records and financial information from unauthorized or inadvertent alteration, destruction or corruption. All interactions with systems that house critical records and information should have audit trails to accurately track every transaction. Archival and storage systems and the media used to retain required records must support reliable, long-term access. In addition, records information and management software and hardware should be flexible and support new policies and procedures as your company grows and changes.

Although a number of vendors claim to have software solutions to support compliance, most focus on a single component or requirement. IBM takes a different approach. Beyond just SOX, IBM analysts and consultants have found commonalities among more than 50 new laws and regulations that have been introduced during the last several years, and we have worked with customers to develop integrated solutions that can help address multiple challenges. This unified approach enables businesses to meet the challenges associated with deadlines and be proactive in meeting future requirements driven by changes in the legal and regulatory operating environments for many public organizations. Many of the regulatory compliance issues facing publicly traded organizations today involve controls applied through technology to help reduce the risk of noncompliance, and IBM has developed a prescriptive approach to the most common findings identified through the internal audits of IBM customers. These findings and mitigation strategies can be found in the appendix of this white paper.

Lotus Workplace for Business Controls and Reporting, Tivoli software and IBM Global Services Business Consulting Services work together to help address SOX requirements and optimize business controls and data management

IBM integrated compliance solutions

IBM Lotus® Workplace for Business Controls and Reporting, IBM Tivoli® management solutions and IBM Global Services Business Consulting Services (**ibm.com**/services/us/index.wss/so/bcs/a1002618) supply integrated software and services offerings that can help your company through the compliance process. These solutions work together to help address SOX requirements and help improve business controls and data management at each level.

Identify control deficiencies with the Lotus Workplace for Business Controls and Reporting solution

The first step in your company's compliance efforts should be to assess the effectiveness of your current internal controls and information management processes. Lotus Workplace for Business Controls and Reporting provides an organized approach to identify potential issues. By automating workflow, the offering helps document and evaluate internal business controls. This documentation helps support the identification of risks and controls and evaluate the effectiveness of these controls. It also links to multiple data sources, even from different vendors, to tell you where content is located and how it is managed. Lotus Workplace for Business Controls and Reporting is a cost-effective way to assess controls, with minimal impact on day-to-day operations.

For more information on Lotus Workplace for Business Controls and Reporting, visit www.lotus.com/sox

Use Tivoli solutions to address SOX compliance challenges

While Lotus Workplace for Business Controls and Reporting focuses on automating the evaluation and assessment of business controls, the Tivoli software portfolio helps customers mitigate weaknesses in their organizations' internal controls. Tivoli software provides a suite of solutions to strengthen internal controls with automated solutions and procedures for financial data and systems, strengthen data retention and help mitigate security risks. Three real-world examples from different industries illustrate how Tivoli integrated offerings have helped enable companies to correct gaps identified by auditors and implement robust, company-wide internal controls that help support their compliance program.

Case one — retail chain

Internal auditors focus on ineffective controls on updates to financial data

The scenario

A large retailer hired a Big 4 accounting firm to assess the chain's internal controls in terms of IT processes around the creation, update, manipulation and use of the financial data for sales, purchasing and accounting. Each of

Highlights

these systems – accounting, sales and purchasing – had its own database. The organization's financial systems used an Enterprise Resource Planning (ERP) software application to manage operational details and create the main financial data and reports for all SEC filings. Internal auditors found excellent controls concerning the organization's use of financial data through this system. However, after closer analysis of the organization's behavior and process for updating financial data, the internal audit team identified a significant practice that could impact the integrity of the financial data.

Auditors found that the organization used a variety of desktop tools throughout the organization to access, update, create and delete financial data directly in the underlying databases of the ERP system. These actions only required the system user to have an internal user ID and password to authenticate to the database. The organization had no controls over the activity of the user once they were "logged in." The primary risk focused on activities and access through desktop Microsoft® Open Database Connectivity (ODBC) applications like Microsoft Access, Microsoft Excel and the like. The access and update privileges in these systems were not maintained in the database or at the network level; no controls were in place beyond the requirement for basic authentication. Internal auditors determined that this represented a significant threat to the integrity of the financial data and accountability of the organization's processes and procedures for reporting financial activity and would require notation on the financial reports left unmitigated.

No controls were in place beyond basic authentication, causing a significant threat to financial data integrity and financial reporting accountability

Audit findings

Auditors reported that these unmitigated updates, inserts and deletions through ODBC presented a significant risk, especially because the organization had no way to track these transactions. Although the retailer had security policies in place, inadequate logging neutralized the ability of these policies to manage risk and preserve the integrity of financial data. Auditors also reported inadequate internal controls of user ID privileges. The lack of company-wide, role-based access definitions resulted in multiple directories for the retailer's various systems and inconsistent transaction privileges.

Customer's strategy for mitigation
Working with the internal audit team, the customer identified three key IT processes and requirements that would need to be changed to mitigate these findings.

- *Create controls on data access and update the underlying financial databases that can manage the ERP system access and any other access, including users accessing the data through an ODBC connection.*
- *Create an automated provisioning process that allows for the segregation of duties to approve the creation of system user IDs and access privileges, as well as modification and removal.*
- *Create an audit logging and reporting infrastructure for reporting system activity to help demonstrate conformance to the organization's internal policies and standards.*

To meet the first challenge – control of financial data updates and changes – the retailer chose IBM Tivoli Access Manager and IBM Tivoli Privacy Manager. Tivoli Access Manager applies a consistent access policy that spans crucial financial systems, including controls that help prevent overrides from local administrators. In addition, the organization selected Tivoli Privacy Manager to help apply the organization's "Information Classification and Control" standard to financial data. Tivoli Privacy Manager would be used to intercept all system calls to the financial systems data, offering a layer of protection around the financial systems databases. This "database proxy" approach would allow the organization to control who could update, delete or create financial data at a transaction and data level. Integrating Tivoli Access Manager and Tivoli Privacy Manager would control access and updates to the financial systems data by evaluating the user's access and update privileges and the system call initiated against the financial data – to control activity of the ERP system and ODBC access to the financial databases. It also creates an audit trail of who accessed what system and when, allowing access and updates to be monitored efficiently. Tivoli Privacy Manager authorizes access based on specific use, data and purpose criteria of each transaction and

Highlights

Tivoli Identity Manager creates an identity management life-cycle framework of controls and segregation of duties for user IDs and access privileges

creates a granular audit trail down to individual data items. Automated access control and tracking helps minimize the time and cost of manual review and creates a clear link between the organization's policy, procedures and standards for IT activity and updates to financial systems.

The second objective was to help strengthen the organization's controls over the creation of user IDs and their privileges for IT system activity. The customer selected IBM Tivoli Identity Manager to create an identity management life-cycle framework of controls and segregation of duties for user IDs and access privileges. Tivoli Identity Manager automates the creation of user IDs and the association of system privileges and can include a workflow process that allows a segregation of duties for access to sensitive systems such as financial reporting systems. The organization created a role-based access policy and used Tivoli Identity Manager to implement this policy consistently across all IT systems in the organization. In addition, they were able to help prove conformance to the organization's policies and maintain compliance with these policies and standards through the use of the Tivoli Identity Manager automated user ID account reconciliation process. This helped the organization verify that there were no user IDs with excessive system privileges and no user IDs that were not tied to real users of the organization, enabling the organization to ensure that all access to financial systems would be based on corporate policy, as well as provide an audit trail of creation of user IDs and who approved the association of privileges for access to financial systems. This helped the organization provide consistent association of system privileges enterprise wide. As with most organizations today, different authoritative sources existed for existing users and user accounts. IBM Tivoli Directory Integrator helped identify these different authoritative sources for user account attributes, including the organization's HR systems and ERP system, and consolidate access into a single virtual repository. By creating a single, reliable source of information on individual users and their access rights, Tivoli Directory Integrator enforces role-based privileges to help protect data from unauthorized access throughout the organization.

The third objective was to increase the quality of the logging and reporting infrastructure of the key IT systems that could impact the quality of the financial reporting. The focus was on creating a strong link between the organization's policy and standards around access and updates to the financial systems and the user accounts allowed to implement transactions within those systems. The customer's strategy was to use Tivoli Identity Manager logs to collect the secondary approvals to associate access privileges with the financial systems and log the conformance determination of all access and updates to the financial data. By consolidating the evaluation of conformance, logging and reporting, the organization could reduce its ongoing audit costs for evaluating the effectiveness of its internal controls and clearly link its policy and standards to the IT systems activity.

Case two — insurance company

Internal audit focuses on risk management and accountability

The scenario

A regional insurance company's internal auditors examined the organization's risk management and IT security controls as a part of its SOX compliance program efforts. As with many other financial service firms, the company has an office of risk management and a separate office for security management. As the company started its SOX internal audit, these two offices started to examine their existing controls and monitoring systems that support their IT operational processes as part of an overall IT risk and regulatory compliance assessment.

The first task undertaken by the internal audit team was the development of an inventory of IT audit logs and IT security event audit logs. While internal auditors developed this inventory, they also collected the status of the subject system for conformance to the organization's standards for audit logs, security and operating system and application configuration baseline. In addition to the application systems, they identified all of the dedicated security controls including the firewall, intrusion detection systems and remote access points. Each of these systems creates logs, identifies security risk events and records them in the system audit log and reports. This inventory became quite large

because the team identified all of the agent offices directly connected to the company's internal systems over high-speed Internet connections. The inventory revealed that most of the security controls had implemented various standards inconsistently, and many of the systems did not use the company's baseline configuration standards or the retention standard for audit logging data. It became clear to the internal audit team that the IT processes for examining threats and risks to the enterprise systems were ineffective and inconsistent.

Many of the systems and security control alerts were never noticed or examined by the security team. In addition, these logs and reports from the security systems often were not examined as a part of its annual IT assessment. The company used these findings to drive the development of a new IT risk analysis process. As a part of this new process it also created the requirement that all audit logs be centrally integrated and retained for a consistent period of time online and then archived for several years.

The organization had stringent security standards with clear configuration definitions for its servers, firewalls and other security devices – based on risks associated with the threats to the confidentiality and integrity of sensitive data, including financial data and customer records. However, the company had no central data collection or report processes to track security risk events centrally, and the existing controls did not adequately pinpoint sources of data access or changes. The company had no way of knowing which servers complied with configuration standards and had no process for updating systems. For example, if Microsoft issued a patch for Microsoft Windows® 2000 or Microsoft Windows NT®, the insurance company could not track which servers had installed the patch or when it had been applied.

Audit findings

The organization's internal auditors found that the lack of an enterprise-wide risk management process and lack of IT technology to help manage conformance to the organization's standards and policies made the existing standards program ineffective. In many ways, the illusion of security created

more risk. Data could be compromised – or lost – without detection, because the company did not consistently monitor security alerts or system access.

Auditors made four primary findings around these issues and made several recommendations including:

Finding	Recommendation
Ineffective security event evaluation and resolution process	Collect all system logs and security device logs centrally, identify critical events and alert appropriate staff security handling the incident.
Ineffective process for tracking regulatory compliance for sensitive data handling	Automate the analysis of system configuration. Require authentication and logging of all access to systems that contain sensitive information. Analyze system access and use for conformance to the organization's policy and standards.
Lack of a system change management process	Develop and implement an organizational IT standard for application and system change control. Develop and implement a change control process for all computing platforms with segregation of duties to request and then approve changes to systems and applications across the organization.
Ineffective and inconsistent data retention of system and security logs	Develop and implement an enterprise data retention standard for all data classifications. The standard will specify standards for retaining data online, archiving and specifying data destruction timeframe and procedures.

Highlights

Customer's strategy for mitigation

The security and risk management team evaluated the findings and recommendations from the internal audit team and developed a strategy designed to accomplish four key objectives:

- *Establish a common user credential system that allows the identification and authentication of users. This information would be used to help establish accountability for changes and change requests.*
- *Establish an integrated, centralized audit logging and reporting infrastructure.*
- *Establish an automated system to apply and track changes to systems and applications.*
- *Establish an automated data retention system and backup services that can manage data by type and catalog and archive specific data types and systems.*

Tivoli Access Manager for e-business and Tivoli Access Manager for Operating Systems enabled the company to implement a common authentication standard and integrate information into diverse systems

The first step was to replace the diverse identification and authentication system with IBM Tivoli Access Manager for e-business and IBM Tivoli Access Manager for Operating Systems on the company's UNIX® boxes. The security and risk management team implemented a common LDAP directory containing user credentials for all registered and authorized users of any enterprise system. This included credentials for all independent agents of the company. With this software the company could implement a common authentication standard and easily integrate the credential information into their diverse systems. In addition, this credential information would be used to identify users who create, approve and manage system change requests. It would also be used by various systems to record activity in system audit logs. The second phase of the remediation program included using two key Tivoli software tools to help track and manage access and disclosure of sensitive data types to work towards the goal of developing the centralized logging infrastructure. The customer selected the Tivoli Access Manager family of software and Tivoli Privacy Manager to create audit logs of all system access to privileged operations on the large UNIX systems and to sensitive data types stored on those systems. Tivoli Privacy Manager audit logs and all other

security device logs and system logs would be collected and analyzed for potential risks and threats by IBM Tivoli Risk Manager. Tivoli Risk Manager collected security alerts across the company and reported the events to a central location for analysis.

Once the activity could be recorded and analyzed through the audit logging and risk management system, the third phase of the project was started: develop and implement an enterprise technology change control system and procedures. The development team targeted two primary technology domains. The first was the configuration of each operating platform. The objective was to reduce risks associated with excessive privileges, misconfigured systems for security standards and rapid deployment of security patches and configuration changes that may be identified through the risk management system. The customer selected Tivoli Configuration Manager and IBM Tivoli Compliance Manager to address these needs and implement the change management system. To address the need for servers being updated in a timely manner, the insurance company chose Tivoli Configuration Manager. This solution allows IT to control the implementation of patches and updates. By managing the rollout process, Tivoli Configuration Manager provides the ability to test, approve and implement changes to servers from one location, verifying that every server has the same configuration.

As an additional anticipated benefit, the technology support organization expected to substantially reduce the number of help-desk calls from agent offices requesting help in resolving misconfigured systems. The enterprise operational team would have a clear view into the status of all systems and be able to track and manage the rollout of patches and system upgrades across the enterprise and across all of the remotely connected agent offices.

Logs from these three primary systems – audit logging and reporting, the risk management system and change management system – would be archived by the new storage management system based on Tivoli Storage Manager. The policy-based implementation of backup and archival processes allowed the organization to implement a new data retention policy across all systems and leverage the investment in a centralized, consistent system.

Highlights

The company decided to implement all three projects at the same time, staggering them by several weeks. Each project would first be implemented in their system testing lab and policies refined as needed. Once the policy and system configuration was stabilized and reviewed by the internal audit team, the organization would begin to roll out the new enterprise infrastructure. This inclusion of internal audit helped bridge IT management, security management and risk management offices. The company's expectations for this new capability went beyond SOX program support to include better risk management and support for other legal and regulatory compliance programs.

Case three — regional bank

Data retention without data management

The scenario

An assessment for a regional bank revealed that storage management practices were operating independently of the bank's data retention practices. One of the storage management practices had storage administrators freeing up space by deleting data that had not been accessed in a year. The storage administrators needed alternative cost-effective storage systems for the retention of managed data.

Audit findings

The bank's internal auditors recommended a storage system that could prevent the deletion of the data needed for data retention requirements.

Customer's strategy for mitigation

The use of IBM TotalStorage® Data Retention 450, which leverages the intelligent capabilities of IBM Tivoli Storage Manager for Data Retention, helps prevent the storage administrators from inadvertently deleting retained data prematurely. Additionally, TotalStorage Data Retention 450 provides a storage platform to address the requirement for cost-effective storage.

TotalStorage Data Retention 450 helps prevent retained data from being prematurely deleted

Tivoli Risk Manager allows management of security incidents from a single Web-based security console. It integrates data from applications, operating systems and network devices to provide real-time visualization and management of security events. By automatically generating incident reports, Tivoli Risk Manager lets the bank quickly identify exposure and take action to fix it. The solution also stores records of security alerts and incidents that prove the effectiveness of security management.

The bank enhanced the security of its data by implementing Tivoli Privacy Manager. This solution authorizes access to sensitive data according to specific criteria for data use, data type and transaction purpose. The granular audit trail of Tivoli Privacy Manager logs user access all the way down to individual line items. To extend the data storage capabilities of Tivoli software, the bank added IBM DB2® Records Manager. The DB2 Records Manager solution stores electronic documents in their original formats, so important e-mail and sales activity data are retained as required.

Other Tivoli solutions

These scenarios represent selected findings related to Tivoli software, but they are by no means comprehensive in describing Tivoli solutions or the complete capabilities of the Tivoli security software portfolio. Tivoli software has been used to help many organizations meet their objectives as a result of various laws and regulations and serves as a business enabler to help reduce the level of effort for integrating systems within an organization and across organizational boundaries. Tivoli products enable management of data, users, transactions and systems based on your company's business policies. Tivoli security software can help organizations integrate their security controls and automate their security processes. Tivoli software enables organizations to "externalize" controls over their IT systems by implementing a system that contains and manages IT resources by policy. This "externalization" and policy-based control will help organizations establish a direct link between their IT governance policies and standards and the systems they manage. For a detailed description of the Tivoli suite of products, visit **ibm.com**/tivoli

Addressing your complexity through integrated solutions

SOX section	IT requirements implication	Solution
Section 404 — Annual report by management on internal controls over financial reporting, attested by external audit firms	• Process mapping and documentation of existing controls on financial reporting • Test for efficacy, and report on gaps and deficiencies • Ability to monitor control compliance • Accelerated reporting requirements	• Lotus Workplace for Business Controls and Reporting • IBM WebSphere® Business Integration Modeler • Tivoli Identity Manager • Tivoli Access Manager • Tivoli Privacy Manager
Section 409 — SEC to consider rules providing for real-time disclosure of material events	• Accelerated reporting requirements place a premium on disclosure controls and quick quarterly close • Expanded list of events deemed to be "material changes" and requiring disclosure	• IBM DB2 Document Manager, IBM DB2 Content Manager and IBM WebSphere MQ • IBM DB2 Data Warehouse Edition • Tivoli Privacy Manager
Section 802 — Criminal penalties for failure to comply with record retention policies	• Strengthened document management and retention practices • Supports the establishment of ethical behavior	• DB2 Content Manager and DB2 Records Manager • Tivoli Storage Manager for Data Retention • TotalStorage Data Retention 450
All sections	• Stringent security • Cohesive management of the infrastructure	• IBM WebSphere Portal • IBM Tivoli integrated identity management suite • IBM Tivoli Business Systems Manager

On demand solutions

IBM solutions include powerful products that integrate seamlessly with one another and with your current applications. IBM solutions provide companies with confidence in their internal controls today and the resilience to respond to future requirements. IBM will work with your company to construct customized solutions quickly and cost-effectively.

For more information

To learn more about IBM solutions and other tools to help your company create an on demand environment, contact your IBM sales representative or visit **ibm.com**/solutions

Appendix: Common IT assessment findings

This matrix is based on interviews with IBM Business Partners that perform audits and the experience with IBM customers who have asked for assistance to mitigate their findings from their internal audits.

Finding	Customer strategy	IBM product capability	IBM product
Inadequate controls of user IDs and association of privileges for access to financial data	Implement identity management processes to manage user identity life cycle and maintenance of access privileges.	• Tivoli Identity Manager delivers user identity life-cycle management services including provisioning, ongoing monitoring and maintenance of access privileges, and deprovisioning services. • Implement a common authentication system with access controls for financial applications.	Tivoli Identity Manager Tivoli Access Manager for e-business
Inadequate segregation of duties for granting access to financial information, records and data	Implement a standard that all requests for access to financial systems have to be approved and documented by a separate individual.	• Tivoli Identity Manager enables a company to define a workflow with multiple approval authorities and methods. Approvals are then documented within the product logs and reports.	Tivoli Identity Manager
Lack of controls over financial data access and updates through ODBC connections or other methods outside of a company's ERP or accounting application	Implement database-level controls to monitor and manage all access, updates, inserts and deletions made to the financial data from the accounting applications as well as other desktop tools such as Microsoft Excel.	• Tivoli Privacy Manager can provide a "database" proxy capability to help monitor and manage all access to the financial data.	Tivoli Privacy Manager
Inadequate IT system change management controls for operating systems and applications	Implement an automated system change management process.	• Tivoli Compliance Manager can monitor and assist with the application and management of settings and system attributes of most IT devices and systems. • Tivoli Configuration Manager can automate the rollout of updates and system changes.	Tivoli Compliance Manager Tivoli Configuration Manager
Inadequate documentation of system configurations, policies and standards	Implement an automated tool to collect and compare all system configurations to the organization's defined baseline for computer systems in specific security "zones" of control.	• Tivoli Compliance Manager can collect operating system configurations and compare them to baseline configuration for each operating system in each security "zone" of control.	Tivoli Compliance Manager
Inadequate audit logs for data access, update, delete and insert operations	Implement an enterprise audit logging solution that captures all activity from users accessing and updating the financial data system. These audit logs are collected and correlated with other system logs to monitor systems and assess risks of confidentiality and integrity of financial data.	• Tivoli Privacy Manager can be used to create access and update audit logs that detail the conformance to the organization's data use policies. • Tivoli Risk Manager can collect the Tivoli Privacy Manager logs and other system logs and correlate the events described in these logs to identify threats to the confidentiality and integrity of the information.	Tivoli Privacy Manager Tivoli Risk Manager
Lack of audit logs for privilege changes to user IDs	Implement a role-based access control system and processes for assigning data access and use privileges. Any changes to a user's role or privileges will be captured by the privilege change management processes or by regular automated audits of role and privilege assignments.	• By implementing Tivoli Identity Manager, the organization has the benefit of the automated user privilege and account reconciliation processes. This process helps ensure that users only have privileges that their roles are authorized to have. Any changes to privileges with an account on a specific system can be identified and automatically corrected by the system.	Tivoli Identity Manager
Inadequate data retention controls for access logs and financial data, and inconsistent application of data retention standard	Implement an automated system to back up and achieve on permeate write once media the audit logs and financial data.	• Implementing Tivoli Storage Manager with the TotalStorage Data Retention 450 solution can help the organization meet its data retention and long-term availability needs.	Tivoli Storage Manager .
Inadequate monitoring of financial systems for availability and support of timely reporting of financial activity	Implement an automated system monitoring for uptime and availability of key financial systems including the ERP system and supporting database systems. Manage system activity so that critical financial reporting processes have IT resources when needed to complete timely financial reporting.	• By implementing IBM Tivoli Monitoring for Applications and IBM Tivoli Monitoring for Databases, key financial systems availability can be tracked and maintained. Tivoli Performance Products and Job Scheduling Software helps to ensure high priority of financial reporting processes and transactions.	Tivoli Monitoring for Applications Tivoli Monitoring for Databases Tivoli Performance Products and Job Scheduling Software
Inadequate controls and processes for risk management and security threat monitoring under the COSO and ITIL frameworks	Implement an automated system for collecting and correlating all security events from systems across the enterprise including firewalls, IDS systems, operating system logs and other security logs.	• Tivoli Risk Manager can collect security event logs from all systems and security safeguard controls. These events are then automatically examined with the Tivoli Risk Manager imbedded intelligent correlation engine to associate and evaluate the threats to financial systems and data.	Tivoli Risk Manager

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Printed in the United States of America
09-04

*The META Group Inc., "Organizational Trends in Sarbanes-Oxley and Regulatory Compliance Issues," July 23, 2004.

♻ Printed in the United States on recycled paper containing 10% recovered post-consumer fiber.

G507-1087-00