How to use identity management to reduce the cost and complexity of Sarbanes-Oxley compliance*
In the rush to meet Sarbanes-Oxley compliance deadlines, many companies have implemented manual processes to quickly demonstrate compliance. Short-term, manually intensive solutions implemented during the first year of compliance expose a company to additional risk and are not sustainable from a cost and efficiency standpoint. Companies that implemented manual controls to meet initial deadlines must now readdress their “quick fix” approach to build a long-term, sustainable solution that includes automated, streamlined and secure operations.

Information technology plays a key role in supporting a company's internal control framework and compliance with Sarbanes-Oxley requirements. Identity management is one component of a strong security program and is necessary if companies are to satisfy and sustain long-term compliance requirements while achieving their business objectives. When combined with improved business processes and procedures, identity management technology can help companies maintain strong internal controls by providing the infrastructure to automate user management processes, improve auditing and reporting, provide access control and authentication, support IT controls—and ultimately, reduce risk.

The key components of identity management used to support compliance objectives include access control, user management, authentication and the application of a user data repository. In this paper we outline how taking an integrated approach to managing these components can help reduce the spiraling costs of compliance to your organization.
Situation
It’s been a long, hard first year
Over the past twelve to eighteen months, U.S. public companies and foreign enterprises with U.S. operations have been rushing to meet the first round of compliance deadlines imposed by the Sarbanes-Oxley Act of 2002.

It has not been easy. In order to comply with the Act’s strict requirements for internal controls and financial reporting—particularly with Section 302 and 404 requirements—companies have worked diligently, often touching nearly every operating and administrative function across the enterprise. For many companies, the exercise proved to be far more rigorous, costly and time-consuming than first anticipated. But was the mission accomplished? Not necessarily. Although it may appear that most of the heavy lifting is done, in many respects the real work lies ahead.

With reporting deadlines occurring quarterly, management now has to address the fact that, as a result of the first year’s rush to compliance, a large percentage of newly implemented internal control processes are based on manual procedures or tactical “work-arounds.” These processes may have helped the company “get by” the first time, but since they drive up costs and complexity, they’re inefficient for long-term compliance.

Manual processes are inherently more risky because they’re prone to human error and may be more susceptible to fraud. In addition, many organizations concerned about the elevated risks associated with manually dependent procedures designed their internal control systems with deliberately high levels of redundancy and duplication—a short-sighted tactic that will continue to drain compliance budgets until remediation action is taken. Today’s CFOs are increasingly looking to their CIOs and IT departments to counter-balance these trends and help create a strategic, long-term framework that increases efficiency while reducing costs.

Lessons learned from recent PwC 404 readiness projects:

- Controls implemented are typically reactive—not preventive
- Communication is frequently poor between operating departments and administrative functions
- Monitoring of controls is often lax
- Compliance programs are highly inefficient
- Data quality is frequently suspect
As the largest corporate reform of business process since the Securities and Exchange Act of 1934, the Sarbanes-Oxley Act has established new or enhanced standards for corporate accountability and penalties for corporate wrongdoing.

The legislation includes 11 titles ranging in focus from additional responsibilities for audit committees to tougher penalties for white-collar crimes such as securities fraud. In particular, two sections of this law represent major challenges for senior executives: Title III, Section 302 and Title IV, Section 404.

**The 302 Requirement:** The Act requires that, as part of each annual or quarterly financial report filed by a publicly traded company, the CEO and CFO must provide certifications regarding the completeness and accuracy of such reports as well as the nature and effectiveness of the internal controls supporting the quality of information contained in these reports.

**The 404 Requirement:** The Act also requires that each annual report filed by the company include management’s assertion as to the effectiveness of internal controls, and an attestation on the part of the company’s auditors as to the accuracy of the report. In the U.S., the most broadly accepted framework for internal control is provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The COSO framework and U.S. auditing standards define “internal control” as a process—effected by an organization’s board of directors, management, and other personnel—that provides reasonable assurance regarding the achievement of objectives in the following categories: 1) Effectiveness and efficiency of operations; 2) Reliability of financial reporting; and 3) Compliance with applicable laws and regulations.

Realize value from your Sarbanes-Oxley investment

As executives look beyond first-year Sarbanes-Oxley compliance, the strategic agenda begins to shift to building cost effectiveness and realizing value from the significant investment of the last two years. We see four successive compliance steps moving forward that represent not only important steps in achieving risk reduction but also, if done correctly, in gaining measurable business value.

**Remediation:** Many companies applied manual fixes to meet 2004 deadlines, leaving them highly susceptible to a repeat of control breakdowns. Further remediation is required to address these weaknesses.

**Sustainability:** Once compliance is assured, companies need to ensure they can cost-effectively sustain it in the constantly changing business and regulatory environment. Implementing a sustainable Sarbanes-Oxley compliance program requires a holistic view of day-to-day activities involving people, processes and technology, as well as a solid understanding of risks facing the enterprise.

**Optimization:** As a result of their 404 investment, companies have gained considerable insight into the complexity and redundancy of their business processes. Leveraging this knowledge can enable them to optimize financial, operational and compliance processes. Standardizing and simplifying processes, combined with effectively using technology helps streamline the control environment, increases efficiency, and leads to more accurate and timely reporting and improved risk management.

**Integration:** Research has demonstrated that addressing compliance requirements in isolation is far less efficient and effective than integrating governance, risk management and compliance on an enterprise-wide basis. Building on Sarbanes-Oxley readiness, sustainability and optimization work requires only incremental steps to integrate compliance processes into business processes and establish a capability to routinely identify, assess and challenge the processes for managing risk. The benefits of these actions are significant, leading to reduced operational surprises, increased efficiency, improved reputation and brand value, and better decisions to improve the balance of growth, risk and return.
Security is critical to the controls environment

One of the strongest trends driving sustainable Sarbanes-Oxley compliance programs is the realization that IT and information security are a crucial part of the internal control environment. This delayed acknowledgment may seem surprising, especially given IT’s ubiquitous role in enabling virtually every critical business process. But apart from the fact that Sarbanes-Oxley legislation does not reference security, there are good reasons behind this trend. Attention to security has come only after other key compliance readiness steps have been addressed—such as identifying critical business processes, defining key control objectives and testing their effectiveness across the enterprise. These steps have consumed the lion’s share of attention from top executives during the rush to first-year compliance.

In addition, in many organizations these first-year efforts were often led by the CFO and the finance organization, with the CIO, CISO (Chief Information Security Officer) and the IT department playing a more tactical role in documenting the design of the controls.

These trends are now shifting as business leaders realize that IT is crucial to compliance.

It’s also becoming overwhelmingly apparent to compliance teams in every industry that the CIO and senior IT executives must provide the strategic direction to help organizations identify where automation and technology can provide a more sustainable compliance and risk management solution.
How does IT security support Sarbanes-Oxley compliance? Not only does IT drive efficiency and lower costs, while reducing compliance risks, but it also frequently generates the data on which many internal controls depend. In fact, the increasing dependence upon digital information requires continually evolving information security capabilities to protect the value of information—its confidentiality, integrity and availability—and also the integrity of the internal control system required to meet compliance and reporting obligations. IT security is the means to support internal controls by helping enterprises meet the following control objectives:

**Enabling appropriate access controls:** It’s essential that companies establish and maintain tight control over user permissions, privileges and profile data in order to restrict access to data, applications, operating systems and infrastructure to only authorized users and programs.

**Enforcing segregation-of-duty requirements:** Strong internal control procedures separate the activities and responsibilities of a company’s employees, particularly with respect to sensitive transactions. In general, the main functions that must be separated include custody of assets, and the recording and authorizing of transactions.

**Protecting information assets:** Control procedures will not be effective unless the appropriate processes, technologies and people are in place to protect enterprise assets from threats and vulnerabilities.
Safeguarding data integrity: Each of the control objectives is necessary to ensure that the data underlying financial reports is complete, accurate, and valid. (See sidebar “An auditor's yardstick: How internal controls are assessed”)

Often, the best groundwork for achieving these control objectives is provided by addressing IT general controls. As pointed out by the Public Company Accounting Oversight Board, “…information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively.”

Internal controls are assessed against a standard that includes the following elements:

**Completeness:** Completeness is satisfied when: 1) All recorded transactions are accepted by the system once and only once; 2) Duplicate postings are rejected by the system; and 3) Any transactions that are rejected are addressed and fixed.

**Accuracy:** Accuracy is satisfied when key elements for transactions recorded and digitally entered into the computer are reasonable and correct.

**Validity:** Validity is satisfied when transactions, including changes to data are relevant, authorized, and not fictitious.

**Restricted Access:** Restricted access is satisfied when companies take comprehensive steps to protect against unauthorized amendments of data, ensure data confidentiality, and protect physical access.

How does security map to these characteristics of internal controls? As one of several strategies engaged by companies to meet these objectives, security focuses primarily on ensuring restricted access and, to some extent, on ensuring the accuracy and validity of data and transactions.
Our Perspective
Compliance requires tight access controls
While security performs a crucial role in supporting Sarbanes-Oxley compliance along each of the four control objectives already outlined, it’s almost impossible to rely on the effectiveness and efficiency of any Section 302 or Section 404 compliance program without a clear commitment to ensuring that only authorized users have appropriate access to the critical systems that contribute data inputs to material financial statement accounts.

What makes user and access controls such a timely issue is that, even after the high costs associated with the first-year rush to compliance with respect to Sarbanes-Oxley, many companies continue to suffer material security and control weaknesses in access-related capabilities crucial for sustaining compliance. The following pages provide a brief summary of the deficiencies encountered most frequently.
Controls over user access and privileges are often weak

One of the most common problems uncovered during Sarbanes-Oxley readiness work involves critical delays in terminating access privileges for users who either no longer work for the organization or have transferred to other working departments within the same company. When access is not removed in a timely manner, the company confronts higher levels of risk associated with unauthorized use and access.

In many organizations, a terminated employee’s system access is removed only when the weekly or monthly termination report is distributed by the human resources department. And far too frequently, access is only partially removed or not removed at all. Addressing these challenges requires a way to be able to remove terminated users from all systems (and certainly from all higher-risk systems) if not in real time then at least in a timely manner.

With respect to users who are transferred from one job to another, it is critical that all access not required for their new job function is removed so that the user is granted access only to systems necessary to support their new responsibilities. If access is not carefully controlled, users can accumulate access to various applications as they move around the organization, introducing the enterprise to elevated levels of risk.
Internal controls over business processes require that user access to transactions is restricted and that certain combinations of transactions not be assigned to a single user. For example, a single user who has access to both purchasing and accounts payable functions should be restricted so that the user cannot create a new vendor, issue a purchase order and then write a check to pay that vendor. In some cases, conflicts emerging from inadequate segregation of duties are not addressed until a problem or fraudulent event occurs. Unfortunately, monitoring of access conflicts with respect to segregation-of-duties requirements is often a time-consuming manual process.

Companies frequently neglect to impose appropriate access control restrictions for IT professionals. In fact, in most IT organizations, IT personnel are routinely granted high levels of access to systems, networks, and applications as well as the ability to administer the settings that prescribe their own access control privileges. Corporations need to more rigorously ensure that IT administrators are subject to controls that grant them access only to the systems they are individually responsible for supporting.

Think through who has access to what, and why. IT personnel are routinely granted high levels of access yet this can introduce increased risk.
Many companies have difficulties in managing access authorizations. Manual processes tend to generate a lot of paperwork. When administrators are inundated with forms, reports, and hardcopy logs that are not always carefully filed or organized, it becomes extremely difficult to produce the control reports required for auditing purposes.

As an alternative to paper-based systems, many companies have chosen to use email as a method for documenting approvals. While storing access approvals electronically is more efficient, similar control deficiencies exist. For example, if an individual who stores the approvals in an email box is terminated, locating the electronic folder where the authorization logs are stored can be much more difficult.

Companies need a way to manage, store and retrieve approvals in a streamlined, automated fashion. Also important is having the ability to monitor approvals as well as track actual changes made to access permissions. While some applications and systems provide automated logging reports, access to these reports is typically restricted to a system administrator. This is frequently an inefficient restriction, because greater management access to this information would significantly reduce the time needed to monitor the effectiveness of the control environment and help the external auditors complete a timely audit with minimal disruption to the business. It is critical that organizations develop the capability to produce timely reports on who requested access, what access was requested, who approved the request, and what level of access was approved.
From the start of the Sarbanes-Oxley readiness campaign, executives realized that there were some critical control issues on the table.

To begin with, the company’s user management process was manual, fragmented, and inconsistent. It was split by application, and there was no notification process in place to communicate with each administrator when an employee account needed to be added, modified or removed. In fact, the company relied on “word of mouth” notification—even for sensitive matters such as employee termination. There was no automated and secure process to initiate account removal—a deficiency that contributed to significantly elevated risks of non-compliance.

Without a clear process, it was difficult to ensure that the multiple and diverse users accessing the company’s systems were authorized and legitimate users in the organization.

The company recognized that a centralized approach to user management would not only resolve compliance issues but also would provide increased security for financially significant applications.

The deployment of an identity management solution across the corporation’s key applications resolved the user access and audit-related issues. This was a major step toward Sarbanes-Oxley compliance.

In addition to addressing compliance issues, there were other benefits for the corporation, including increased security for financially significant applications covering both salaried employees and contractors, and improved customer service. And, what was once a three-day manual process for adding new accounts is now streamlined and automated.
Password policy enforcement is frequently insufficient

As companies document controls over their financial reporting and related applications, some are beginning to uncover password-related compliance deficiencies. Introducing new applications and systems to an increasingly layered and poorly integrated enterprise environment creates more password management inconsistencies. Organizations are also finding that password policies are not enforced across all systems.

As a result, some applications require passwords of different lengths and complexities. This inconsistency, combined with a rapidly expanding number of user IDs and passwords that each user must remember, often increases the risk that users write their passwords down and store them in unsecured locations—such as under their keyboards or on notes stuck on their monitor.

Having a method to synchronize passwords and maintain minimum standards for the majority of passwords would significantly reduce risk.
User information may be subject to mismanagement, exposure and compromise

Information related to users is often stored throughout the enterprise in multiple applications and systems. It is almost impossible to manage and update this information in a timely manner without the proper policies, procedures and technical infrastructure. And with the added complexity of increased regulatory requirements, it is becoming more difficult to manage user information with even the minimal levels of discipline and control necessary to give senior executives confidence in certifying corporate reports. Organizations require a secure, effective and cost-efficient means of managing user information stores.
Access control is critical to compliance. Companies must ensure that only authorized users have access to the systems that contribute data to financial statements and reports.
Implications
A first step toward sustainable compliance should include identity management
It is almost impossible to address many of the control deficiencies and risk drivers identified in the preceding sections without leveraging technology. As a critical technology component within an organization’s security management program, identity management performs a strategic role in improving the processes that control access to programs and data.

Information security is no longer merely a means to “keep people out” of an organization and its critical business systems. Today information security, particularly identity management, is recognized as the primary way to enable appropriate access to an organization’s systems, assets and data for a full range of user constituencies.

A comprehensive identity management solution provides organizations with a structured approach to align the people, process and technology elements of an effective IT solution with critical business and compliance requirements. This enables secure interaction with employees, customers, partners and suppliers.

Once processes and controls have been documented and critical control gaps identified, identity management can help executives create a sustainable set of internal controls. Identity management provides the infrastructure to automate user management processes, improve auditing and reporting, provide access control and authentication, support IT controls—and ultimately, reduce risk.

The key technology components of identity management that support compliance objectives include:

**Access Control:** What information are you allowed to add, change, remove or view? Are your access permissions consistent with your job responsibilities and role in the organization?

**User Management:** How do you manage access across the user management lifecycle in the organization, including user management, provisioning and self-service functions, such as password reset?

**Authentication:** Who are you? How do you identify yourself? Are you who you say you are?

**User Data Repository:** Does user information reside centrally or virtually? What is the “authoritative” source of user information? Here integration is key, as each of the controls and capabilities identified above are closely interrelated. When implemented as a set of common or shared services or interfaces, they form a single logical view of users and the systems and information to which they have access.
By strengthening their access control capabilities, organizations can ensure that their users are given access to only the applications or resources they’re entitled to see or use. These strategies are typically either “user-”, “rule-” or “role-” based—or represent a combination of these approaches.

For example, Role-Based Access Control (RBAC) enhances an identity management solution by providing an easier way to grant access to a user based on a predefined role. RBAC provides organizations with a consistent and standardized means of assigning access and privileges to a user based on a job function or role that is consistent with segregation-of-duties (SOD) restrictions. This integrated and systematic approach discourages the creation of “one-off” roles, or the granting of privileges on an individual basis, while simultaneously improving the controls around reporting and accountability.

How does access control support Sarbanes-Oxley control objectives?

- Helps to enforce segregation of duties by standardizing user access, based on predefined roles
- Addresses restricted access as defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- Provides an automated approach to managing access that builds a more sustainable controls environment
By implementing an integrated approach to user management, organizations can use automated tools that provide uniform, consistent and auditable business processes to manage user profile information across various platforms. User management is a set of processes and supporting infrastructure encompassing automated workflow, delegated administration, user self-service and provisioning (the automation of the user management process).

A comprehensive user management solution provides the automated logging, monitoring and reporting of user access and approvals that senior management can view in real time. User management also plays a key role in reducing the overall cost of compliance by enabling organizations to provide self-service for time-consuming administrative functions related to password administration. In addition, it improves security by enhancing the enforcement of policies and reducing the frequency of unauthorized access.

The workflow component of an identity management solution automates the business processes around the creation, modification and termination of user access. For example, let’s say that a business manager requesting access permissions for a new hire keys the request into the online request system. The request is then electronically transmitted to the designated person for approval. The system automatically creates a new account for this user and sends a confirmation notice back to the business manager. This automated approach to workflow provides the checks and balances to ensure that the access granted is consistent with the organization’s compliance and control objectives.

How does user management support Sarbanes-Oxley control objectives?

- Defines the procedures that ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts
- Provides a standardized approach to password administration across disparate systems
- Delivers the platform component necessary to enforce segregation-of-duties restrictions with respect to requesting and granting access to critical systems and data
- Enhances controls by automating the logging, monitoring and reporting of user management issues

Implications
How authentication supports internal controls

Authentication is a process that verifies a user’s identity before granting access to an application or resource. In essence, it verifies that they are who they say they are. Authentication mechanisms such as passwords, PIN numbers, digital certificates, tokens or Smart Cards provide increasingly stronger levels of certainty with respect to the validity of a particular identity. Consistent and careful application of authentication mechanisms ensures resources are protected from unauthorized access in a way that is commensurate with the criticality of the system being safeguarded.

How does authentication support Sarbanes-Oxley control objectives?

• Safeguards corporate information by preventing unauthorized access
• Supports COSO control criteria with respect to restricting access
• Increases security and controls by establishing and enforcing a set of authorized security and permission policies
• Establishes procedures to authenticate users and support the validity of transactions
How a user data repository supports internal controls

The user data repository is the cornerstone of any identity management solution. It includes the infrastructure necessary to store user information that supports access and user management decisions. This data includes information used to validate identities, personal information, and information on roles and reporting relationships, as well as passwords and other user credentials. In many organizations, user profile information is stored in multiple and diverse systems and applications, making it almost impossible to keep it synchronized and continually updated. Consolidation or—at a minimum—synchronization of this information is critical for maximizing its value. User data repositories also provide a consolidated and controlled approach to storing user information, which increases its integrity and security.

Organizations need to consider how authentication, authorization and administration data should be stored, retrieved and reported. In other words, it may not be realistic to centrally store all authentication and authorization credentials. The alternative to a centralized model for storing data is to develop a meta-data model for access and accountability. In the event that a single authoritative directory services infrastructure is not viable, organizations should consider a meta-directory or virtual solution to create a consolidated view of users from various sources.

Developing such a model places structure around the data and its use, movement and storage, helping ensure the overall accuracy and availability of the information. This, in turn, can significantly reduce the time required to respond to auditors and/or regulators, while building confidence in the results of user-related inquiries.

How does a user data repository support Sarbanes-Oxley control objectives?

- Closes control gaps with respect to user information mismanagement
- Enables organizations to maintain essential control over user information
- Helps keep user information consistent across multiple systems and applications
- Provides an “authoritative source” for creating and maintaining user profile information, which clearly defines responsibility and accountability for that information
How to get started

1. Begin by understanding your Sarbanes-Oxley security-related challenges. Determine if you have issues with security and user access.
   - Did you uncover security and user access control issues as a result of your Sarbanes-Oxley readiness review?
   - Do you know who has access to your financially significant applications and what access they have?
   - How many manual fixes are currently in place related to user access?
   - What is the cost associated with maintaining your current user access control environment?
   - Can automation and a more streamlined process help you improve the effectiveness and efficiencies of compliance?

2. Based on the answers above and the information provided in this white paper, evaluate if and how identity management can help you create a more cost-effective, secure, and streamlined approach to managing compliance.
3. Move forward by creating your identity management strategy and action plan.

- What are your priorities? Think about the short-term compliance issues that need to be addressed, balanced with your strategic business objectives.

- Determine the extent to which role-based access control might be utilized within the organization.

- Develop a strategy for designing and implementing an identity management solution that incorporates its impact on business processes and organizational structure. Your strategy should also include company-specific technical considerations, as well as enterprise-wide control requirements.

- Develop an action plan that breaks down the implementation into logical steps or phases that accomplish short-term needs, and demonstrates repeated and measurable success.

4. After addressing the “people” and “process” impacts, evaluate the technology options available and select a vendor.

- Which identity management vendor has the “right” product to meet your unique requirements?

- Will one vendor’s technology answer all of your challenges, or will you need to integrate a combination of solutions?

5. Finally, design, build and deploy the solution based on your strategy and action plan.
The ideas presented within this paper are examples of how CFOs and their finance departments are increasingly looking to CIOs, CISOs and senior IT managers to help provide long-term, sustainable solutions to Sarbanes-Oxley compliance. Robust identity management processes play an important part in this evolution. By eliminating redundant infrastructures and reducing the costs inherent in manually-driven security and access control configurations, identity management helps to bring down the spiraling costs of compliance.
For further information, please visit
www.pwc.com/security

or call:
1.800.639.7576