

# Enterprise Provisioning

## Reducing the Costs of Sarbanes-Oxley Compliance

In the wake of a number of high-profile accounting scandals, the U.S. Congress passed the Sarbanes-Oxley Act of 2002 (SOX) to reform the accounting practices, financial disclosures and corporate governance of public companies. It not only mandated that companies strengthen and document controls to prevent the commission of fraud, but it holds CEOs and CFOs legally and financially liable for complying with the act.

For many companies, the greatest challenge is not only how to comply with SOX, but specifically to be able to implement and enforce proper control and then validate the effectiveness of those controls in a cost-effective manner. One of the first and most critical controls needed to promote compliance is the ability to track who in the organization has access to what information and why. The more these user access privilege control and monitoring processes can be automated, the less money and time it will take to achieve compliance in a sustainable manner. To support compliance initiatives, organizations must be able to effectively:

- Ensure that only authorized users gain access to data,
- Protect data confidentiality, integrity and accuracy, and
- Control and monitor user activity.

Enterprise provisioning systems automate many of the key internal controls needed to help ensure compliance with Sarbanes-Oxley, as well as other regulatory requirements. These systems automatically apply policies and rules governing who can access what systems and what privileges users have within these systems to detect users who are not properly authorized, automatically manage and update user rights and privileges across the enterprise, and track changes for auditing purposes.

TABLE OF CONTENTS

RSA SECURITY IS YOUR COMPLIANCE PARTNER	1
I. AUDIT AND COMPLIANCE DRIVERS	1
The Sarbanes-Oxley Act	1
The Cost of Compliance	2
II. UNDERSTANDING SOX REQUIREMENTS	2
Internal Controls	3
Attestations	4
Compliance Strategies	4
Methodology	4
III. HOW XELLERATE IDENTITY MANAGER AUTOMATES COMPLIANCE	5
Accessing Affected Systems	5
Automating Access Policies	6
Policy-based Revocation	6
Fine-grained Entitlement Management	6
Policy History	6
Segregation of Duties	6
Workflow	7
Approval and Notification Process	7
Dynamic Task Assignment	7
Rogue and Orphan Account Detection	8
Reconciliation	8
Policy Violation / Exception Detection	8
Auditing	8
Evidence	8
Reporting	9
Policy Exception Reporting	9
Periodic Review of Access Levels	10
ID Consistency	10
IV. CONCLUSION	10
APPENDIX: LEGISLATIVE DRIVERS	11

## RSA SECURITY IS YOUR COMPLIANCE PARTNER

RSA Security offers a range of solutions for helping to comply with the many regulations related to the protection of information. With more than 17,000 customers worldwide, RSA Security is an industry leader in information security. RSA Security solutions—which include solutions for identity & access management, secure mobile & remote access, secure enterprise access, secure transactions and consumer identity protection—help organizations address the requirements of SOX. This white paper explains how the Xellerate® Identity Manager provisioning and user life cycle management solution by Thor Technologies, an RSA Security strategic partner, is ideally suited to help enterprises cost-effectively support their Sarbanes-Oxley compliance initiatives.

Xellerate Identity Manager software is engineered to strictly enforce user information access policies, detect unauthorized system access privileges and ensure that such rights are immediately and accurately revoked for terminated employees, contractors or customers. Xellerate Identity Manager software can implement and track compliance with the most complex security policy requirements, as well as work with the access control mechanisms resident within leading mission-critical enterprise ERP, HR and CRM applications. Through its robust reporting and auditing capabilities, Xellerate Identity Manager is built to enable companies to demonstrate to regulators that access rights to key corporate systems are properly managed, without the need for labor-intensive testing.

The Xellerate Identity Manager solution provides a comprehensive enterprise provisioning solution optimized for identity management and is an important tool in helping companies cost-effectively enforce SOX compliance. Xellerate Identity Manager is designed to quickly and easily help firms implement, test and deploy even the most complex forms of internal controls. Its powerful reporting capabilities give management and auditors confidence in these controls. All proof of activity and control history is properly evidenced, helping to ensure that auditors have the information that they need in order to attest to the firm's assessment of its internal controls. Finally, due to its powerful process automation capabilities, Xellerate Identity Manager software is designed to enable firms to significantly reduce the initial and ongoing cost of audit and SOX compliance.

## I. AUDIT AND COMPLIANCE DRIVERS

Several sets of business drivers are forcing companies down the road to compliance. Although this paper focuses on Sarbanes-Oxley, several other legislative requirements exist for companies of varying size and in specific vertical markets (see Appendix for additional detail). In addition to these legislative requirements, most corporations' board of directors and executive management mandate additional internal corporate governance guidelines.

### The Sarbanes-Oxley Act

The U.S. Public Company Accounting Reform and Investor Protection Act of 2002 was passed to address major corporate accounting scandals that severely damaged investor confidence in the securities markets in 2001 - 2002. In addition to mandating major changes in accounting, auditing and financial reporting practices, Section 404 of the Act requires companies to strengthen and document their internal controls in order to prevent individuals from committing fraudulent acts that may compromise a firm's financial position or the accuracy of the company's financial statements.

Because SOX focuses on accounting practices, corporate governance and accountability, it has significant impact on the underlying IT systems that support corporate accounting and financial reporting. Specifically, the Act has defined a deadline for establishing, documenting and auditing adequate internal controls to prevent fraud. Internal controls are a set of formally defined business processes, corporate guidelines and other mechanisms that can materially influence a firm's financial statements. Because much of the information and processing that generate these financial statements take the form of digital assets, corporate IT systems play a key role in enforcing such internal controls. Unauthorized access to financial systems and the data they contain may allow dishonest individuals to alter that information or commit fraud that may damage the company financially and cause it to violate regulatory standards.

Of all the legislative drivers, Sarbanes-Oxley is the most far-reaching in terms of its compliance requirements and the number of firms that it affects. This is due to several factors, including:

- Company executives can personally be held legally and financially liable for acts of wrongdoing;
- It applies to any domestic and foreign companies that publicly list securities in United States markets. These companies span almost the entirety of the Global 2000, including firms that are headquartered outside of the United States;
- Such firms are increasingly concerned about potentially losing ground to competitors that are not required to comply with the Act; and
- The cost of ensuring compliance with all provisions of the act is incredibly high in terms of hard cash and the sheer amount of effort and manpower required.

The fact that key corporate executives carry personal financial and legal liability in the event of noncompliance ensures that SOX compliance is a key initiative in most large organizations today. In addition, many companies that are not yet public, and therefore are not obligated to comply with the Act, are voluntarily embarking on compliance efforts to demonstrate their readiness to comply with public market requirements. Finally, most corporations agree that compliance with the Act ensures that they are following generally accepted best practices for corporate governance and management.

### The Cost of Compliance

A key concern of most firms affected by SOX is not compliance itself, but rather the ability to prove compliance in a reasonably cost-effective manner. The act's requirements are reasonably straightforward, but meeting them without the help of IT to automate and audit relevant transactions is incredibly costly. Unless a well-thought-out, IT-based audit and compliance strategy is defined and executed, firms will incur these costs on a recurring basis in their efforts to validate ongoing compliance efforts—a costly proposition.

If not managed effectively, SOX compliance can be very expensive because it requires a company to document, test, audit and prove that its internal controls are being adhered to and are adequate to ensure that its financial statements contain no material irregularities. These requirements can be met by internal or external auditors through a process known as substantive testing, which requires selecting a sufficiently large sample of the transactions that can materially influence a firm's financial statement and reviewing each transaction from start to finish. This can be extremely labor-intensive, time-consuming and costly.

How can a firm meet SOX compliance requirements without requiring scores of internal auditors to document, test and remediate the necessary processes and then pay an external independent auditor to largely repeat the exercise?

Understanding these specific requirements is the first step towards complying with them in the most efficient and cost-effective manner.

## II, UNDERSTANDING SOX REQUIREMENTS

Among the primary requirements of the Sarbanes Oxley Act is Section 404, which requires a company's annual report to specify who within the organization is responsible for establishing and maintaining internal controls and procedures for financial reporting. It also requires that the company and its external auditor conduct their own assessments of the effectiveness of those controls. Both these requirements imply that the management of the company:

- 1) understand all the processes that may affect their financial statements;
- 2) have necessary controls in place that ensure that these processes are conducted appropriately; and
- 3) has tested these controls to ensure that they are working as intended.

The requirement that an external auditor attest to the statements made by management implies that the accounting firm has enough insight into corporate processes and controls to determine if management's assessment of those controls is sound. A closer look at the various types of controls required by SOX, as well as the various strategies for complying with it, illustrate how an automated provisioning solution can help companies achieve compliance in the most cost-effective manner.

**Internal Controls**

Internal controls are the processes that ensure that financial transactions within a firm are being conducted in line with generally accepted ethical and business best practices. They include a wide set of policies and procedures (both documented and implicit), the people that conduct financial transactions, the inclination of the board and the management team to conduct business ethically, and the very culture of the firm.

In the context of SOX, controls range from the specific (a corporate policy mandating how revenue is recognized) to the general (a management-instilled culture that encourages employees to behave ethically). Four types of controls can be implemented, each with different objectives.

*Preventive* controls attempt to avoid undesirable behavior and, if properly designed and implemented, may discourage such behavior. For example, a preventive control may ensure that only the CFO and the controller have the ability to invoice customers and recognize revenue above a

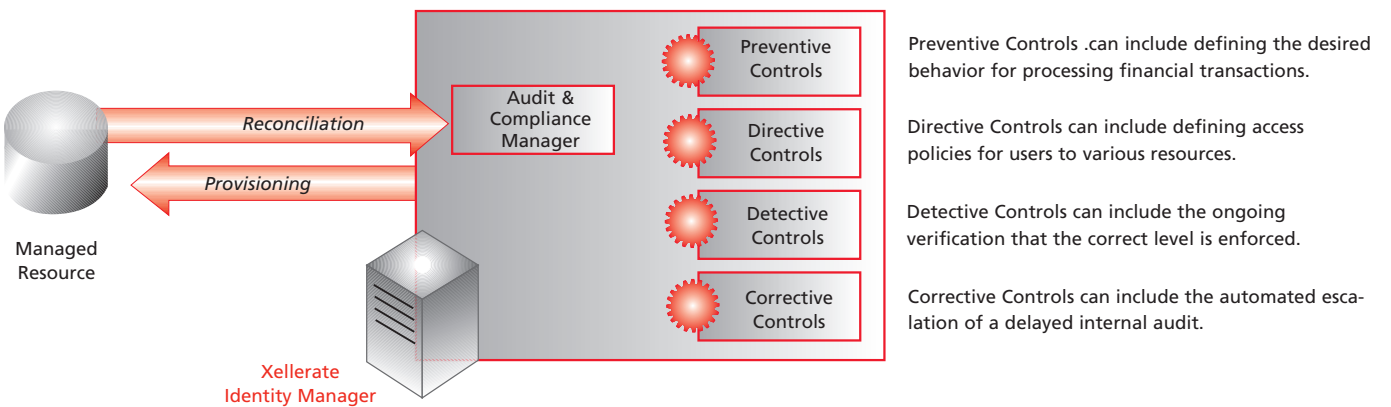
predefined limit. If properly deployed, this ensures that only those with sufficient visibility into the firm’s business operations are able to close transactions large enough to have a material impact on the firm’s financial statements.

*Directive* controls pro-actively foster the intended behavior and are the mainstay of an organization’s efforts to encourage proper behavior. Examples include policies that define which individuals within the firm should have specific levels of access to the various systems that support financial transactions or hold financial transaction data.

*Detective* controls identify improper activity when its proactive system of directive and preventive controls has failed. Examples include ongoing verification that the correct access level is being enforced for all users in the enterprise.

*Corrective* controls, most commonly used in conjunction with detective controls, ensure that improper actions are corrected. For example, an internal audit that is delayed past a certain point may be automatically escalated to a different person within the firm.

**FIGURE 1 INTERNAL CONTROLS**



### Attestations

Sarbanes-Oxley also requires that a firm’s independent auditor attest to the correctness (or incorrectness) of the management team’s assessment of the internal controls structure as stated in the annual report. The most crucial element the auditor needs in order to make a positive attestation is evidence—verifiable proof that management has identified a sound system of internal controls and has implemented them properly. Without proper evidence, a firm can find itself in a situation where it fails to get a positive attestation from the auditor, despite investing in internal control structures. In such a case, the firm faces significant additional expenses because it must pay the auditor to test its controls before issuing a judgment about their effectiveness.

### Compliance Strategies

Based on an understanding of the key requirements of SOX, the different types of controls a company might put in place and the importance of attestations to ensure compliance, how should a company go about ensuring its compliance with SOX? Most will choose a combination of corrective and preventive strategies.

A corrective strategy focuses a company’s spending on corrective or reactive controls, which allow it to react to policy violations in a timely manner. A firm that embraces a corrective strategy is willing to accept the marginal but real risk that it will be non-compliant from time to time. It is extremely important to be aware that purely corrective

strategies represent only a starting point to compliance. They can meet tactical SOX requirements, but over time, usually prove costly and expose the firm to business risk. A purely corrective strategy is typically used only when a preventive strategy, or a mix of corrective and preventive action, would require too much time or expense.

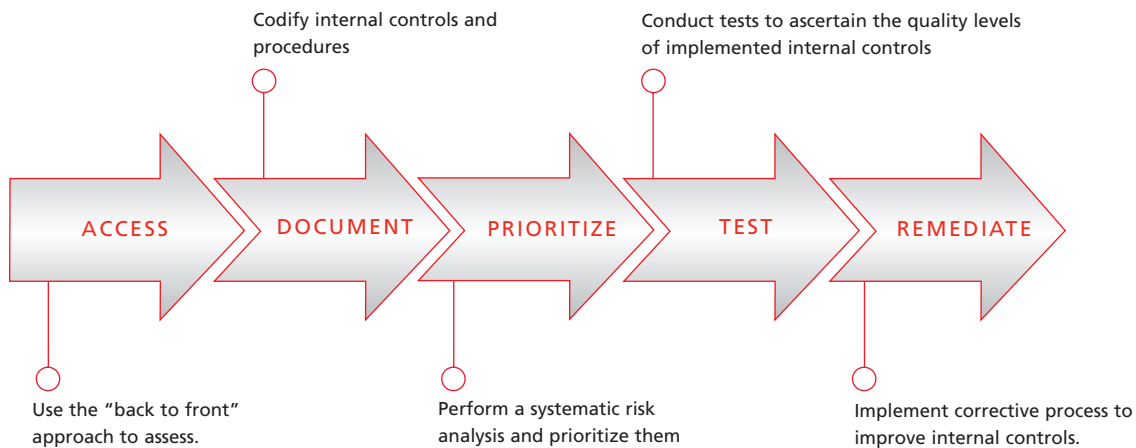
Preventive or proactive compliance strategies are typically implemented when a firm can make the needed investment to be reasonably sure that undesirable behavior never takes place. A purely preventive strategy is rarely deployed. When a firm has the time and resources to deploy preventive mechanisms, they are typically implemented with complementary corrective mechanisms to provide a more complete and thorough approach to ensuring compliance.

An effective compliance methodology includes a mix of corrective and preventive controls, and provides the evidence that auditors need to attest to the effectiveness of those controls in a cost-effective manner.

### Methodology

A good methodology, vetted against industry best practices, provides a stable foundation on which to build an effective compliance framework. The high-level methodology below has been prescribed by auditors for many public firms as part of their SOX compliance efforts. Indeed, it helped many of these same audit firms deliver risk management projects for their clients in the Global 2000 long before the passage of the Sarbanes-Oxley Act.

FIGURE 2 METHODOLOGY



**Assess:** Most auditors agree on the need to begin with a “back to front” assessment, beginning with the balance sheet and financial reporting statements to understand the systems and transactions that feed into those reports. The firm can then track those transactions through the back-office and toward the front-office functions from which those transactions originate.

**Document:** Identify and codify all the internal controls discovered in the assessment that could have a material impact on financial statements. Define a standard to measure the type and degree of documentation needed to accurately capture the procedures that are followed or need to be followed. Being able to document and articulate the processes that are already in place (no matter how ineffective they may be) is critical to remediation and compliance.

**Prioritize:** Of the relevant controls identified and documented from the previous phases, perform a systematic risk analysis and prioritize those transactions that have the most impact on the firm’s ability to accurately reflect its financial condition. It is important to conduct this phase with a fair amount of diligence because it will direct where the firm makes its remediation investment.

**Test:** Test the controls to ensure that they are working as intended. Conduct combinations of manual and IT-automated tests to ascertain the quality levels of the different types of controls that have been implemented. Identify which ones are working and where improvements need to be made. Cross-reference the test results with the prioritization activity from the previous phase. Any control areas identified as high-risk/low-quality should become the top candidates for remediation.

**Remediate:** Begin the corrective process to improve the controls that aren’t working as intended or as designed. Where needed, implement appropriate controls. Once the appropriate corrective measures have been implemented, wait for a sufficiently large sample size of transaction data to accumulate and then iterate through the Test and Remediate phases as needed until the firm is comfortable with its level of compliance.

Next, we’ll examine how an enterprise provisioning system such as the Xellerate Identity Manager solution can enable cost-effective automation of such a compliance process.

### III. HOW XELLERATE IDENTITY MANAGER HELPS AUTOMATE COMPLIANCE

A key contributor to cost-effective SOX compliance on an ongoing basis is automating the capture, control and documentation of critical financial transactions and automating the process of demonstrating that these controls are enforced. This section explains how the Xellerate Identity Manager solution can help companies become SOX-compliant in a highly efficient and cost-effective manner.

#### Explicit Permit

The most basic type of access policy is the explicit permit policy, which allows the implementation of directive controls that define which users should be granted access to specific systems and data. Examples include:

- Everyone in finance has access to SAP® Business Warehouse, and
- The CFO and CEO have access to Siebel® Reports.

Such policies are prevalent throughout any large public or private enterprise. Automating them enables a firm to implement basic internal controls without the delay and expense of making manual changes to access policies.

#### Explicit Deny

An explicit deny policy specifically mandates which level of access specific users or groups should not have. This is more critical than an explicit permit policy because it supports the implementation of preventive controls that help avoid undesirable activity. Examples include:

- The research staff never has access to any trading systems.

#### Accessing Affected Systems

As prescribed by the back-to-front methodology advocated by many auditors, it is vital to identify systems that play a significant role in the generation of financial statements. Typically, they span several key software categories, such as ERP (Enterprise Resource Planning), HRMS (Human Resources Management Systems), CRM (Customer Relationship Management) and other related systems.

**The Xellerate Advantage:** The Xellerate Identity Manager Adapter Factory Integration Engine is designed to provide out-of-the-box adapters for many of the key systems that are affected by SOX compliance requirements ensuring that firms can rapidly deploy the solution and understand their level of compliance. This avoids the delay, and the often substantial cost, of building custom adapters for each application.

### Automating Access Policies

The Xellerate Identity Manager software's Access Policy feature set enables firms to define and automate the mechanisms by which people are granted access to various applications. This advanced set of capabilities represents the foundation upon which a rigorous internal controls structure can be built. Access policies are used to implement directive and preventive controls, as described below. They are based on tying privileges and restraints to defined user groups. Because access policies automate manual controls, they enable the firm to realize significant cost-efficiency benefits.

*The Xellerate Advantage:* Explicit deny policies are crucial to a firm's ability to implement some fundamental preventive controls. Xellerate Identity Manager enables organizations to automatically restrict access rights based on organizational policy.

### Policy-based Revocation

Just as important as policies for granting a user access to information or systems are policies dictating when to revoke such access. Because such policies can be complex, it is important to choose a flexible provisioning tool that allows the company to create and change policies as required. Examples of policies requiring revocation of access rights include:

- The CFO has access to Oracle® Financials (but if a person is no longer the CFO, this access should be immediately revoked).
- Anyone on the internal audit committee has access to Siebel and PeopleSoft systems (and if someone is no longer on the internal audit committee, the access should be revoked).

There are also many cases in which a user should continue to have certain types of access even if the policy that granted them access no longer applies. The most common scenario involves employees accessing benefits and other HR data. Typically, employees receive access to their benefits data as soon as they are hired. However, even after they leave the company they should be allowed access to the company's HR portal to view their 401(k) and other benefits information.

*The Xellerate Advantage:* Xellerate Identity Manager software supports optional policy-based revocation. With the click of a mouse, administrators can specify when users should be granted exceptions to access policies. This provides the flexibility to implement internal controls with great precision, but without the time and expense of custom coding.

### Fine-grained Entitlement Management

True risk mitigation and regulatory compliance require fine-grained entitlements management. It is not enough to dictate who should (or should not) have access to a specific application, but rather to define the specific level(s) of access granted or denied to a user. Most of the systems that generate financial transactions, such as SAP, PeopleSoft and Siebel software have their own unique models for managing access control and permissions management. In order to support compliance initiatives cost-effectively, a provisioning solution must be able to perform fine-grained calibration of these controls. It is absolutely vital that the provisioning solution include mechanisms that implement the controls within these CRM, ERP or other enterprise applications in an automated and auditable manner.

*The Xellerate Advantage:* Xellerate Identity Manager software allows administrators to define and implement extremely granular access policies within enterprise applications. This reduces the time and cost required to implement appropriate controls (and prove the effectiveness of such controls) within the systems that most affect corporate financial performance.

### Policy History

The Sarbanes-Oxley Act requires that auditors attest every year to the adequacy of a company's process for producing its financial results. Unless auditors have access to a history of how access control policies have changed, they must perform substantive testing on the same controls year after year. This results in one of the most significant costs of SOX compliance.

*The Xellerate Advantage:* Xellerate Identity Manager software allows companies to track how various access policies (each embodying internal controls) have been updated or modified. By giving auditors quick and verifiable insight into how a given control has been modified since it was last tested, auditors need to test only those controls that are new or have significantly changed since they were last tested. The ability to track and display policy history is a key element in reducing audit and compliance costs over time.

### Segregation of Duties

Segregation of Duties (SoD) is a key vehicle for preventing fraud and detecting errors in the processing of financial transactions. SoD ensures that the same person does not participate in more than one key function of a transaction, to ensure their actions are properly monitored or overseen by others. Effective implementation of a strong SoD model makes use of the various access policy controls previously described above (explicit permit/deny, fine-grained entitlements, etc.). However, in some cases, a user's

responsibilities are not predefined and thus cannot be captured as Xellerate Identity Manager access policies. In these cases, the user's access rights are defined by the rights they are granted within a specific target application. For instance, a firm may specify that anyone in the office of the controller can be granted access to SAP General Ledger, but only if that person doesn't already have access to SAP Business Warehouse. If that person already has SAP Business Warehouse privileges, access to SAP reconciliation is not permitted. Successful implementation of SoD requires a provisioning system that can dynamically recognize the privileges a user already has and make intelligent decisions that comply with the firm's stated control objectives.

### Workflow

Business processes and workflow automation are most commonly used to implement preventive and detective controls. Workflows are implemented within an organization to ensure that the appropriate people are kept apprised of key decisions and that, if necessary, transactions that may have significance to a company's financials are first put through appropriately rigorous authorization (approval) processes.

*The Xellerate Advantage:* Xellerate Identity Manager software has powerful pre-provisioning extensions that support dynamic, real-time entitlements calculation to prevent users from being granted an entitlements "basket" that would violate SoD policies. Using a sophisticated framework that enables real-time analysis of a user's entitlements, Xellerate Identity Manager software can model and support very intricate controls to properly enforce SoD. Many competitors claim some degree of ability to handle SoD requirements, but most can handle only the narrowest of compliance-driven use cases. Xellerate Identity Manager is specifically designed to support very sophisticated SoD requirements.

### Approval and Notification Process

The most common types of workflows implemented involve approval (authorization) and notification. Approval workflows ensure that the appropriate personnel have approved a particular transaction request. Approval processes are examples of preventive controls that force access requests through a policing process that allows an approver (authorizer) to reject inappropriate requests. Notification refers to workflow that informs interested parties, such as auditors, when certain predefined conditions occur that indicate sensitive activity. This provides the firm some assurance that if the activity is potentially harmful, the appropriate individuals have been informed and can take the necessary corrective actions. Customers need provisioning solutions that can handle the new, nonstandard workflows required to achieve SOX compliance.

*The Xellerate Advantage:* Although most identity management and provisioning vendors claim their solutions can handle workflow requirements, they can actually handle only the most simplistic approval or notification schemes. Xellerate Identity Manager software has been widely recognized as a robust, flexible and powerful process engine. It supports single and multi-step approvals, branching and joining scenarios, approval voting, dynamic assignment and others that represent common business processes and internal control mechanics.

### Dynamic Task Assignment

Ensuring that the appropriate people are tasked with the appropriate types of approvals (authorizations) is at the very heart of what makes approval an effective preventive control. Therefore, it is imperative that any tool used to implement such controls has the flexibility to handle very complex, real-world scenarios for determining which business users have the ability to grant approval for various transactions. As with workflow, although most products claim to handle sophisticated task assignment scenarios, they can actually assign tasks in a workflow only to a named individual or group. There is very little scope in such tools for handling any kind of dynamic behavior that takes relevant inputs and making a decision based on specified rules regarding the assignment of an approval task.

*The Xellerate Advantage:* SOX compliance controls need intelligence in the implementation of the preventive control requirements to take into consideration relevant contextual data, such as the beneficiary for the transaction, the specific system being requested, the level of access requested and the like. The Xellerate Identity Manager solution supports the use of multiple approval processes for each type of request and then allows administrators, via a rule-definition GUI, to define specific process selection rules that will decide at run time which one of the specified processes to execute. In addition, within each process, Xellerate software is designed to use plug-ins built from the Adapter Factory integration engine to route transactions to the appropriate approver(s). Without this level of sophistication, firms cannot model controls with the degree of rigor needed to meet compliance requirements.

### Rogue and Orphan Account Detection

A common type of security vulnerability that can threaten SOX compliance is the presence of rogue or orphan accounts. Rogue accounts have typically been explicitly created as exceptions to documented policy and serve as “back doors” to allow fraudulent use. They represent a crucial area of vulnerability, because a firm may not notice inappropriate activity from such accounts until it is too late to stop the offender(s). Orphan accounts were originally provisioned correctly but were never removed when the business reason for the account disappeared. Orphan accounts occur most commonly when the individuals for whom they were created have left the firm, but appropriate processes were not in place to ensure that all the accounts for that individual were rescinded. Although more benign than rogue accounts, they still expose a firm to noncompliance because they represent avenues for unknown or unmonitored access to systems that drive financial statements. Reconciliation allows a firm to deploy a control that can detect these types of accounts and bring them to the attention of appropriate security administrators for corrective action.

*The Xellerate Advantage:* The Xellerate Identity Manager Reconciliation Engine and standard reconciliation adapters to common systems enable users’ accounts and entitlements within critical SOX-relevant resources to be monitored at client-specified periodicity. Xellerate software can then proactively correct any identified exceptions to corporate policy.

### Reconciliation

As the name suggests, reconciliation is an ongoing process that ensures that the provisioning transactions that have occurred comply with the internal control structure laid out by management. Reconciliation is a classic example of a detective control. It identifies past events that do not comply with defined policies. It is a firm’s most basic defense when directive and preventive controls have been circumvented or have broken down.

### Policy Violation/Exception Detection

Even more important than eliminating unnecessary accounts on sensitive systems is quickly detecting when valid accounts have been provisioned with inappropriate privilege levels, because this lead to violation of SoD policies and other undesirable scenarios.

*The Xellerate Advantage:* The Xellerate Reconciliation Engine is engineered to detect all such policy violations and exceptions on the high-sensitivity systems that manage company financial data. The Reconciliation Engine takes what is typically a detective control and

turns it into a corrective control. It can be configured to not only detect such exceptions but also to automatically take corrective action such as the revocation of prohibited privileges or even the temporary suspension of all suspect accounts.

### Auditing

Although all of the remediation steps outlined so far can add significant value to the proper operation of a business, their value for SOX compliance is marginal at best without a strong audit component. This is because of the importance of the auditor’s attestation that management has implemented adequate internal controls. This attestation can be made in a cost-effective manner only if internal controls and their resulting transactions have been properly evidenced.

### Evidence

Evidence is verifiable proof that proper internal controls have been implemented and are being followed. SOX defines evidence as all data pertaining to policies (controls) and policy history, requests and approvals, and requires that data be properly captured and stored in a reasonably secure manner. In addition, it must be maintained in a format that easily lends itself to robust reporting. Although competing products capture some evidence of requests and approvals, they are often only written into a log file which makes building meaningful reports very difficult. Furthermore, these other products capture virtually no evidence of the types of controls that have been implemented and absolutely no evidence regarding the evolution of those controls (policy history data). As with other requirements discussed in this paper, although the capabilities offered by such tools can handle some simplistic scenarios and use cases, they stand almost no chance in effectively helping a firm managing SOX requirements.

*The Xellerate Advantage:* Evidence of all transactions handled by Xellerate software is stored in the Xellerate repository, a relational database. This not only ensures that the evidence data is properly captured and stored but also puts it into a format that is accessible by standard reporting tools such as Crystal Reports, Business Objects and Actuate. This model lends itself very effectively to helping an auditor understand and believe that appropriate controls have been implemented and are being followed properly. As discussed earlier, proper maintenance of evidence, in particular relating to how internal controls have evolved since the last audit, can be an extremely powerful tool for managing costs for future audits.

**Reporting**

The final element of an effective SOX strategy is the use of reporting to maintain an ongoing understanding of the state of compliance within the enterprise. Reporting plays a crucial role as a key detective control (in conjunction with reconciliation) that can be used to catch exception conditions where proactive controls (directive and preventive) have not functioned as designed. When looking at reporting requirements in the Sarbanes-Oxley context, it is important that a provisioning solution supply a robust and extensible framework that provides access to meaningful, high-quality data in a responsive manner.

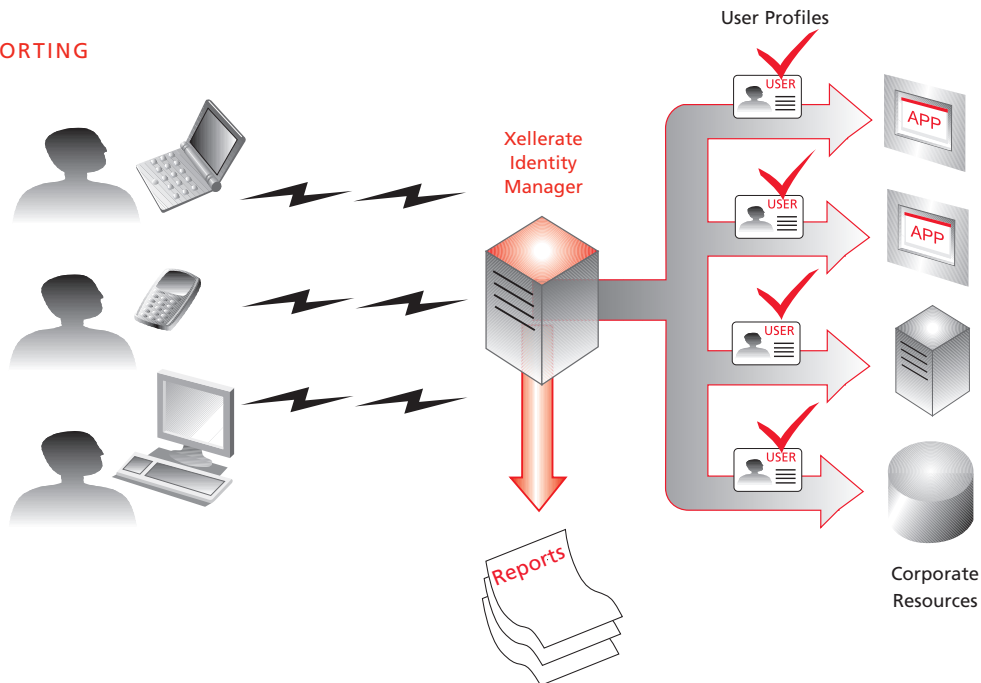
*The Xellerate Advantage:* Building on the capabilities outlined in the “Auditing” section above, Xellerate’s reporting infrastructure allows a firm to mine relevant data as needed to meet specific reporting criteria and requirements. The reporting engine is based on stored procedures, delivering high-performance reporting as needed. Furthermore, the Xellerate Identity Manager solution includes several reports and templates that allow a firm to get immediate value from its SOX compliance strategy. The most basic type of report is “Who Has What,” which can be used to generate a comprehensive fine-grained listing of the access privileges and levels of the users in the enterprise. This report can also be generated in a resource-centric manner, which gives an auditor immediate insight into which users have access to the firm’s most sensitive applications from a financial reporting perspective.

In addition, Xellerate Identity Manager software maintains data that shows detailed traces for individual requests, approvals and provisioning/deprovisioning date/time stamps. It can also capture audit trails for situations in which an approver has been authorized to act as a proxy for another approver. This capability is mandatory when a business approver is away from their regular duties. Due to business travel, vacations and the like, approvers must delegate approval responsibilities. Not only must a provisioning solution support this functionality, but it must flag it in an audit trail. An auditor needs to be able to differentiate between self-approval of workflow tasks and approval of workflow tasks by one entity on behalf of another business authority.

**Policy Exception Reporting**

The use of exception reporting (which highlights instances where a user’s access levels are not aligned with the documented internal controls) is a powerful tool for reducing the time and cost of the audits required by SOX. With this report, auditors can assess how to handle the policy exception. If an auditor identifies a justified exception (for instance, the individual in question was part of an ad hoc working group that required a certain level of access), that person can approve the exception through a normal Xellerate approval process. If an exception is approved, it will be flagged as such and will no longer appear on future policy exception reports. Alternatively, if the exception is determined to be unacceptable, the auditor can notify the appropriate security administrators to request immediate corrective action.

**FIGURE 3 REPORTING**



*The Xellerate Advantage:* Once a company's controls (access policies) are appropriately configured within the Xellerate Identity Manager software, the firm can run an exception report showing instances in which a user's access levels are not aligned with documented internal controls.

#### Periodic Review of Access Levels

Detective and corrective controls such as the ability to generate policy exception reports are an important component of a solid SOX strategy. However, due to their reactive nature, they are by definition weaker than proactive controls. Xellerate Identity Manager technology delivers a mechanism that extends the reactive policy-exception-reporting mechanism and allows a firm to implement it in a proactive manner. Xellerate Identity Manager software can also be configured to periodically remind various individuals to generate various reports (Who Has What, Exceptions, and so on), acknowledge that they have examined the results and are satisfied that they properly reflect the firm's policies. This gives a firm greater confidence that its proactive controls are working properly and that the appropriate personnel are validating that they are working.

*The Xellerate Advantage:* This ability to pro-actively drive validation of reactive controls leverages and extends capabilities that already serve as significant differentiators for the Xellerate Identity Manager solution. Competing solutions simply don't have the level of sophistication required to support such advanced scenarios.

#### ID Consistency

One common problem in large enterprises is the proliferation of various application-specific identities (sometimes called handles) for the same user. In a typical scenario, each of these identities follows a different, application-specific naming convention, and some are machine generated, giving the "handles" no deterministic attributes to link them back to the user. This leads to the challenge of linking the disparate identities and linking them to the main user identity in the system of record.

*The Xellerate Advantage:* The Xellerate Identity Manager solution can help mitigate this problem. Where target systems allow it to do so, Xellerate Identity Manager software is engineered to automatically generate a deterministic user ID for new users. This makes it easier for auditors who are examining extensive reports to visually link users across disparate systems.

## IV. CONCLUSION

Compliance with the Sarbanes-Oxley Act hinges on three key requirements:

1. Successful implementation of adequate internal controls that ensure the veracity of the firm's financial statements;
2. Management's ability, on an ongoing basis, to prove the effectiveness of these controls to the external auditor; and
3. The ability of the external auditor to attest to the effectiveness of these controls each year, based on reliable evidence.

These requirements can be met by the labor-intensive, and therefore extremely expensive, process of substantive testing—effectively a brute force audit that can definitively prove that internal controls are working properly. However, the business challenge is to prove compliance in a cost-effective manner.

Xellerate Identity Manager software meets this challenge with a strong set of capabilities that are designed to:

- Automate the directive internal controls that dictate the specific levels of access that individuals and groups of users should have to systems and data;
- Automate the preventive internal controls that handle authorization and segregation of duties;
- Maintain and present evidence that proper controls have been implemented and are working as intended;
- Perform change management to track modifications made to controls, driving down the cost of audit over time;
- Deliver timely, relevant reports that enable internal auditors to quickly identify areas of noncompliance; and
- Ensure ongoing compliance through robust automated reconciliation and other workflow capabilities.

By providing an automated platform to dynamically manage "who has access to what," the Xellerate Identity Manager is a compliance-driven IT investment that promotes clear, quantifiable return on investment by significantly reducing the initial and ongoing cost of audit and SOX compliance.

**APPENDIX: LEGISLATIVE DRIVERS**

Numerous legislative requirements affect many firms in the Global 2000. In some cases, these have an impact on firms in a specific vertical segment, such as healthcare or financial services, whereas others are more broadly applicable to almost every company that has a publicly-traded security in the United States.

The accompanying table describes some of the key legal regulations, the companies affected by them and the impact of the requirements. Although proper audit and compliance can help meet the requirements mandated by these regulations, further discussion of how they can be addressed is not within the scope of this paper.

Regulation	Mandating Organization	Security Tools	Affected Companies
Gramm-Leach-Bliley	U.S. Office of the Comptroller of the Currency (OCC)	Authentication, access controls, encryption, data integrity controls and audit controls	All financial institutions regulated by the OCC
HIPAA	U.S. Department of Health and Human Services (DHHS)	Authentication, access controls, transmission security, audit controls and data integrity	Healthcare organizations in the U.S.
21 CFR Part 11	U.S. Food and Drug Administration (FDA)	Authentication, access controls, data integrity controls, audit controls, encryption and digital signatures	Companies regulated by the FDA, such as pharmaceutical firms
Basel II	Basel Committee on Banking Supervision	FFIEC framework-access rights administration, authentication, network access, operating system access, application access, remote access, logging and data collection	Global financial service organizations
California Privacy (SB 1386)	State of California	Encryption, access control	Companies that own or lease data containing personal information of California residents

## ABOUT RSA SECURITY

RSA Security helps organizations confidently protect identities and information access. The company secures more than 15 million user identities, safeguards trillions of business transactions annually, and manages the confidentiality of data in tens of thousands of applications worldwide. RSA Security's portfolio of award-winning solutions—including identity & access management, secure mobile & remote access, secure enterprise access, secure transactions and consumer identity protection—set the standard in the industry. Our strong reputation is built on a 20-year history of ingenuity, leadership and proven technologies, and our more than 17,000 customers around the globe. Together with more than 1,000 technology and integration partners, RSA Security inspires confidence in everyone to experience the power and promise of the Internet. For more information, please visit [www.rsasecurity.com](http://www.rsasecurity.com).

