Using Microsoft Active Directory to Address Sarbanes-Oxley (SOX) Compliance in Heterogeneous Environments

RFG believes the seemingly benign verbiage in section 404 of the Sarbanes-Oxley Act (SOX) has created anxiety, tumult, and a multi-billion-dollar-per-year industry. That industry is largely dedicated to helping companies prove that they are not misstating their financial results, and much of that money is coming from IT budgets. It has fallen to IT to assure that authorized people conduct all financial transactions and data entry, and that all transactions get logged and tracked in ways that support comprehensive auditing. To meet these and other business requirements, IT executives must ensure that the identity and access management (IAM) solutions at their enterprises deliver adequate levels of demonstrable, transparent compliance. These solutions, in turn, must be built on a foundation of secure access management, across all systems.

Business Imperatives:

- SOX compliance that is demonstrable "on demand" is a critical challenge for IT executives, their non-IT executive colleagues, and their enterprises. Some IT industry-watchers estimate that enterprises will spend more than $2 billion on compliance technologies in 2005 alone. The ultimate goal of compliance is to protect the integrity of the enterprise's financial transactions and the tracking and reporting of those transactions. Given the prodigious fines and potentially crushing blows to a company's reputation associated with non-compliance, the above expenditure could quickly become an established part of "the cost of doing business." Specialized SOX compliance solutions exist, but for many enterprises, the primary focus will be on driving compliance with incumbent technologies. IT executives should ensure that all current and future solutions and initiatives are fully integrated into effective strategies for transparent and demonstrable compliance. Independently developed guidelines, such as the Control Objectives for Information and other Technologies (COBIT) can significantly aid such efforts.

- SOX Section 404 and other regulatory requirements stipulate that enterprises create and maintain detailed information about information flow and user access across (and sometimes beyond) entire enterprise networks. Centrally managed repositories of such information are also essential elements of effective identity and access management (IAM) and IT security architectures. IT executives should ensure that IT infrastructures at their enterprises can easily support creation and maintenance of such repositories in ways that minimize risk by maximizing both compliance and security.

- At a growing number of enterprises, Microsoft Corp.'s Active Directory is rapidly establishing itself as a de facto standard for enterprise directory services and IAM initiatives according to RFG research. Active Directory is powerful and flexible, and enables and supports effective, policy-based management of "compliance-ready" IAM initiatives. However, Active Directory by itself offers only limited benefit to client systems not running Microsoft Windows. IT executives considering or pursuing compliance and/or IAM initiatives should look closely at Centrify Corp.'s DirectControl, which "embraces and extends" Active Directory in ways that enable centralized policy enforcement and audit control across heterogeneous environments.

SOX already affects almost every publicly traded company. Other federal regulations focus on specific industries, and are being joined by analogously rigorous regulations from states and other localities. Figure 1 below offers summary descriptions of key regulations, including SOX, and demonstrates how other regulations are increasingly intersecting with SOX.
Compliance is also critical because of the risk created by non-compliance. SOX and other regulations include significant corporate and personal financial liabilities – sometimes up to $20 million for each incident of non-compliance. This financial risk is accompanied by what some refer to as the threat of the "CNN moment," which usually involves visions of a CEO and his or her colleagues doing a "perp walk" before television cameras.

Moreover, SOX and other regulations require that IT executives affirm that their bosses are justified in claiming that their enterprises are compliant. Specifically, according to the U.S. Securities and Exchange Commission (SEC), the internal control report mandated by Section 404 must include "management's assessment of the effectiveness of the company's internal control over financial reporting." Since that "internal control" is almost always IT-based, this makes IT executives more involved, visible, and potentially vulnerable if such claims cannot be fully supported by demonstrable facts. On the other hand, IT executives who develop effective strategies for SOX compliance will advance development and deployment of best practices and technologies that enable compliance with other regulations.

**SOX in Detail: What it Means and What Really Matters**

As mentioned in Figure 1 above, SOX includes multiple sections, each of which includes different specific requirements. For many IT executives, SOX Sections 404 and 409 are the most immediately compelling.

SOX Section 404 requires corporate management to implement effective controls and procedures for financial reporting, and for an auditor to attest to the effectiveness of these controls and procedures. SOX Section 409, meanwhile, requires enterprises to disclose publicly "material changes" in "financial conditions or operations," in plain language, and upon demand from a court or regulator.
RFG believes SOX Section 404 is the most significant specific regulatory challenge facing most enterprises and IT executives now. According to the SEC, Section 404 requires security controls that demonstrably enable the enterprise to ensure that only authorized users have access to enterprise IT resources and financial information. Section 404 also requires that security controls be demonstrably effective. This implies that those controls be based on well-defined, well-documented, and consistently implemented best practices. In addition, Section 404 requires that an external audit validate that the mandated security controls are both implemented and effective.

Any enterprise that cannot guarantee that its network and financial information are protected from unauthorized access, and cannot back up that guarantee in the face of an audit, faces significant financial, legal, and reputational risk. This risk is compounded as SOX and other regulations evolve to address enterprise intellectual property beyond financial information.

For example HIPAA, which focuses on the personal and private information of health care consumers, mandates specific electronic transactions standards. The U.S.A. PATRIOT act, meanwhile, requires subject companies to prove that they are not doing business with specific countries and criminals. Thus, IT executives at companies anywhere along a relevant communication or transaction chain must now or soon be prepared to document and guarantee effective oversight of all regulated information passing through those companies.

Faster reporting alone cannot guarantee compliance, and non-compliance is not an option. Thus, some enterprises are spending $1 million or more per year for every $1 billion of enterprise revenues to address SOX compliance, and are still largely uncertain of the success of their efforts. These expenditures are significantly increasing enterprise general and administrative (G&A) budgets, and affecting net incomes. IT executives should identify and assess carefully the improvements in access control, audit-readiness, documentation, and process management demanded by SOX compliance requirements.

**SOX: the Opportunities**

While the challenges presented by SOX are significant, effective compliance efforts also present great opportunities to IT and the enterprise. Among the most important of these is the opportunity to leverage SOX requirements to increase available funding for IT initiatives.

In addition, achieving and sustaining SOX compliance will deliver far greater organizational benefits than a good report card from auditors. Compliance efforts can significantly accelerate and expand the development and deployment of best practices for effective, business-centric policies, for IT and information security management. These practices and policies, in turn, will result in closer IT-business alignment, greater competitive elasticity and agility, and higher ROI from IT.

These benefits can help to transform the perception of IT as a cost center or simple source of cost savings to an enabler of immediate and sustained business benefits. At a time when IT budgets are flat, growing at only 1 to 2 percent annually, or shrinking, this improved perception can be critical to IT’s ability to garner political and financial support for future initiatives. IT executives should ensure that compliance initiatives at their enterprises address both the challenges and the opportunities compliance requirements create.
How to Become and Remain Demonstrably Compliant?

To deliver effective, consistent compliance, IT must first develop and maintain current knowledge about the specific regulations that directly affect the enterprise. With this knowledge, IT executives and their teams can equip the enterprise IT infrastructure with best practices, policies, and tools that deliver effective compliance and comprehensive, auditable management of all key elements and users.

Where SOX compliance is concerned, one of the most popular best practices frameworks is the COBIT guidelines. These are issued by the IT Governance Institute (ITGI), a research organization affiliated with the Information Systems Audit and Control Association (ISACA). The COBIT guidelines articulate specific control objectives that meet most if not all requirements for full and fully demonstrable compliance.

The American Institute of Certified Public Accountants (AICPA) is another source of useful information and guidelines for compliance best practices, offered from a largely financial perspective. IT executives should explore these and other resources to help develop and justify best practices at their enterprises.

Regardless of the guidelines used to support them, best practices begin with efforts to identify and pursue initial opportunities to deploy such tools and policies that deliver rapid, specific business benefits. IT should then "replicate and scale" these successful initial efforts, then integrate them over time into fully, reliably compliant IT infrastructures. At most enterprises, IAM and security management offer some of the strongest initial opportunities for success with regulatory compliance.

Compliance, IAM, and Security

IAM and security are essential elements of compliance. Comprehensive IAM and security are both required to protect the enterprise IT network, its financial information, and its intellectual property. Without the ability to guarantee and demonstrate that these resources are secure, all other efforts at compliance, governance, and security, are suspect. If IT cannot guarantee that access to data is restricted only to those with a legitimate right to it, IT cannot guarantee that the data has not been compromised. Such conditions guarantee that the enterprise is out of compliance.

The best IAM and security efforts rely upon and support directories that maintain and use repositories of information about users and their activities. These repositories are much more than generic databases or stores of user names and passwords. Instead, these repositories quickly become the places where enterprises store and manage information about the responsibilities, restrictions, rights, roles, and rules that govern access to enterprise resources.

With such repositories, IT executives are more able to guarantee and demonstrate that all access attempts and users are accounted for. Such repositories, in turn, help to enable effective compliance, as well as strong audit tracking and reporting features, and consistent enforcement of relevant business policies.

Obstacles to Success

Unfortunately, at many enterprises, IAM efforts are not yet sufficiently robust enough to address or support compliance requirements. Challenges include expensive, unwieldy, and incomplete solutions, inadequate or missing best practices, financial constraints, and the heterogeneity of IT environments. Increasing urgency from "C-level" executives outside of IT is exacerbating these challenges.
Also, many enterprises have multiple IAM "silos," each with its own repository of critical access control information. This means no enterprise-wide visibility of that information, which severely limits its business value. It also means no consistent, central control of user and administrator rights and restrictions.

These challenges, in turn, lead to difficulty in maintaining consistent policies across platforms with different capabilities. Because policies cannot be enforced consistently and automatically across all platforms, multiple administrators often arrive at multiple policy interpretations. Policies often cannot be implemented or changed in timely response to shifting business or technological conditions. Multiple repositories make consistent deployment and enforcement of management policies all but impossible – which all but assures that the enterprise will be out of compliance.

Overcoming the Obstacles: Directory Consolidation

All of the benefits of IAM and security are maximized when multiple, separate repositories are replaced by an architecture that supports central management and policy enforcement for all users and computers in the enterprise IT infrastructure. Central management also overcomes the security limitations that result from maintaining multiple directories.

A consolidated, centrally managed architecture can also help to integrate controls, enabling administrators while imposing practical, effective constraints upon them across the entire enterprise. These benefits are closely aligned with the goals and requirements outlined in the COBIT guidelines. IT executives should strive to ensure that all compliance, IAM, and security efforts at their enterprises both support and are supported by common, comprehensive, consolidated repositories.

Several vendors offer tools designed to address this problem. Some use metadirectories constructed from abstractions of the individual repositories. Some rely on synchronization of those repositories. Some employ provisioning technologies to achieve consistency. Such tools can help to reduce overall complexity of multiple IAM repositories in some cases. However, even though they can define and propagate policies, these tools are unable to ensure that the application enforces the policies. And none of these tool architectures can reduce all multiple repositories to the ideal number in terms of control, management, and policy enforcement – one.

Active Directory: The Leading Repository Management Solution

Microsoft’s Active Directory solution is by many measures the most pervasive and fastest-growing directory service solution today. Active Directory enables comprehensive, flexible, and secure management of users and computers via business-defined policies applicable to business-defined groups. Effectively, Active Directory enables powerful, risk-reducing IAM, by establishing enterprise-wide security policies. Active Directory also includes extensive auditing, authentication, and security features.

In addition, Active Directory is designed to be highly fault-tolerant and robust, even in large, distributed environments. The very ubiquity of its Windows environments all but forced Microsoft to deliver a directory services solution that could support wide ranges of applications, systems, and users, even while being scaled broadly.

Active Directory also enables enforcement of enterprise-defined, business-driven Group Policies for consistent security configurations, across multiple groups of users and computers. Further, Active Directory delivers these features at little to no additional costs beyond those of Windows Server 2003. In addition, support of third-party auditing, logging, and reporting tools expand Active Directory’s ability to support compliance efforts.
With the introduction of Windows Server 2003, Active Directory gained significant improvements in security and usability over previous versions. Among these is the Group Policy Management Console (GPMC) for consolidated management of Group Policy objects (GPOs).

These and other strengths are rapidly increasing the percentage of Windows sites deploying Active Directory, according to Microsoft and published reports. Some 65 percent of enterprises reliant upon Windows currently use Active Directory, a number soon expected to exceed 85 percent, according to Microsoft and some market-watchers. Active Directory is therefore consolidating repositories for directory services, IAM, security, and other critical functions at a growing number of enterprises.

**Active Directory, Compliance, and Effective Governance**

As delineated above, where SOX is specifically concerned, IT executives and the enterprises they support must be able demonstrate the integrity of financial transactions, from start to finish. In addition, all relevant processes and steps in every transaction must be transparent to auditors, and ultimately to regulators.

Beyond specific transactions, compliance best practices dictate that IT executives, their teams, and their enterprises must ensure the authenticity and authority of those responsible for administering relevant processes. In fact, regulatory compliance requirements are evolving to demand that enterprises be able to prove at any time that no processes have been corrupted or circumvented.

IT executives should therefore strive to view compliance requirements more broadly. IT executives should use compliance requirements to drive development and enforcement of policies and roles that ensure that all involved in business transactions are authenticated, authorized, legitimate, and validated.

Further, IT executives must ensure that all such policies and roles are consistently, comprehensively documented. In addition, IT executives and their teams must ensure that the systems supporting financial transactions and business operations are consistently, demonstrably resistant to inadvertent or malicious access attempts.

In its latest iterations, Active Directory offers enterprises significant assistance in achieving regulatory compliance, and in delivering optimum IT and business governance. Active Directory is well suited to help enterprises determine who should be authorized to do what based on its Kerberos infrastructure and Group Policy. Active Directory enables administrators to consistently and centrally authenticate each user, then to delegate and provide access to the resources each user needs to do his or her job. Active Directory also maintains a central repository of audit logs for all access attempts. This can significantly aid efforts to demonstrate adequate controls over enterprise network identities and access rights.

**Active Directory, COBIT, and SOX: Tying it All Together**

The COBIT guidelines mentioned above identify and address a number of "domains" that comprise effective governance and compliance frameworks. Figure 2 below outlines some key SOX requirements, their related COBIT domains, and the features of Active Directory that help to address them.
### Figure 2: SOX Compliance and Active Directory: Specific "Match Points"

<table>
<thead>
<tr>
<th>SOX Requirements (and related COBIT Domains)</th>
<th>Relevant Active Directory Features</th>
</tr>
</thead>
</table>
| Assess, Organize, and Plan (COBIT Domain: Planning & Organization – PO)  
  - Align IT & business efforts  
  - Develop & implement policies, procedures, processes, rights, roles, rules, and responsibilities  
  - Manage IT projects, quality, resources, and risks |  
  - Enables and supports secure, flexible planning  
  - Supports deployment, enforcement, and monitoring of role-based policies, procedures, and processes |
| Implement Security Controls (COBIT Domain: Acquisition & Implementation – AI)  
  - Identify, then acquire and maintain appropriate technologies  
  - Develop and maintain procedures  
  - Manage changes |  
  - Enables deployment and enforcement of proper system configurations via Group Policy features  
  - Enables managed delegation of system administration tasks  
  - Ensures secure deployments of acquired software  
  - Maintains an accurate, managed, searchable, and up-to-date repository of administrator and user roles and activities  
  - Supports logs of privileged and exceptional operations related to the directory |
| Demonstrate Effectiveness (COBIT Domain: Delivery & Support – DS)  
  - Ensure continuous service and security  
  - Manage configurations and their capacities and performance |  
  - Audit and discovery support features enable "on-demand" demonstrations of compliance with relevant policies and processes  
  - Enables centralized, policy-based, secure control and management of access, authentication, and authorization for IT users and resources  
  - Group Policy features enable "fine tuning" of delivery and support policies and processes based on user roles and business goals |
| Enable External Auditing and Validation (COBIT Domain: Monitoring – M)  
  - Assess and assure adequacy of internal controls and operational security  
  - Monitor processes |  
  - Maintains an "audit-ready" repository of accurate, complete information about business and security policies governing access, authentication, and authorization  
  - Provides a repository interoperable with third-party tools for more comprehensive monitoring and enforcement of relevant policies, and/or more extensive reporting  
  - Supports consistent, policy-based, secure delegated administration |

Source: Centrify Corp., the ISACA Web site (www.isaca.org) Microsoft Corp. Web site (www.microsoft.com), and Robert Frances Group (RFG)
Active Directory is a powerful tool. As delivered from Microsoft, it only supports systems running Microsoft Windows. However, most enterprises support heterogeneous computing environments, often including multiple versions of UNIX, Linux, and even Windows. To maximize the business value of Active Directory deployments and investments, IT executives should seek to extend the benefits of Active Directory to non-Windows systems.

The DirectControl Suite from Centrify Corp. integrates closely with Active Directory, to extend Active Directory management and policy capabilities to non-Microsoft environments. This provides the multi-platform support that Active Directory requires for maximum effectiveness in heterogeneous environments. DirectControl also enables Active Directory auditing to include security authentication events across the heterogeneous enterprise.

Further, Centrify's unique Zone technology enables group-based user access controls for non-Windows systems, and provides access control reports for users and computers. DirectControl also extends Active Directory's Group Policy security configuration and policy enforcement features, with more than 50 pre-defined templates for UNIX and Linux systems.

At many enterprises, while there may be more aggregate Windows systems, the most business-critical applications and data are running on UNIX and/or Linux systems. The DirectControl solution offers patent-pending Zone technology, which allows IT executives to isolate these more critical systems and assign access rights to them and their administrators, depending upon specific business conditions and requirements. DirectControl therefore enables levels of granularity and flexibility for user and administrator access not easily matched by competing alternatives. IT executives should recognize the need to provide adequately fine-grained user and administrator access control within a consolidated management framework, and focus on solutions that meet this critical need.

**Active Directory + DirectControl = Enterprise-Wide Compliance**

The combination of Active Directory and DirectControl enables enforcement of best practices for IAM and security controls across an enterprise's entire IT architecture. The combination securely connects non-Windows systems with Active Directory, leveraging current business practices and security policies. This ensures comprehensive coverage where compliance, IAM, and security initiatives are concerned. Active Directory and DirectControl also establish a firm foundation for future enterprise-wide IT initiatives in compliance and other areas.

With Centrify's DirectControl Suite, IT executives can build upon their enterprises' Active Directory deployments to deliver effective immediate and sustained responses to the challenges of regulatory compliance, today and tomorrow.

**RFG believes** regulatory compliance is a significant challenge to most enterprises, and that non-compliance represents significant risk to those organizations. IT executives should build and deploy comprehensive, consistent, and policy-driven responses to the challenges and opportunities presented by regulatory compliance requirements, leveraging incumbent technologies wherever possible. For enterprises using or considering Active Directory deployments, Centrify's DirectControl Suite can enable compliance and deliver high levels of business benefit and ROI. IT executives at such enterprises should evaluate the potential of DirectControl to deliver such advantages to their specific enterprise situations.
RFG analyst Michael Dortch wrote this Custom Research Note for Centrify. Interested readers should contact RFG Client Services to arrange further discussion or an interview with Mr. Dortch.