

Complying with Sarbanes-Oxley
The Identity Management Connection

BMC Software Identity Management solutions for Sarbanes-Oxley

EXECUTIVE SUMMARY

Sarbanes-Oxley has become a fact of life for most large companies doing business in the United States. Although the legislation is sweeping in scope, there are process frameworks which help identify specific capabilities IT organizations must develop in order for their companies to be compliant. Among these capabilities, Identity Management is a key group. CONTROL-SA[®], one of the most complete Identity Management solutions on the market, can help companies achieve compliance with respect to these capabilities. Furthermore, the operational benefits of CONTROL-SA can make complying with the identity management aspects of Sarbanes-Oxley pay for itself.

SARBANES-OXLEY: OVERVIEW AND INTENT

The Sarbanes-Oxley Act of 2002¹ was enacted in response to the outbreak of corporate malfeasance cases that emerged in the 2001-2002 timeframe, Enron being a prime example. This outbreak illustrated two weaknesses in financial reporting.

First, that it was easier than previously thought to manipulate financial statements. Even though each of these companies had internal financial reporting standards and auditing groups, and their financial statements were approved by external auditors, large-scale fraud still occurred.

Second, that it was very difficult to establish responsibility for fraudulent financial statements. That is, so many people are involved in the overall process of preparing financial statements that identifying specific individuals who could actually be held responsible for the fraud was tremendously difficult. Sarbanes-Oxley addresses these weaknesses.

At a high level, the Act is best known for its requirements that the CEO and CFO of a company personally certify the company's financial results and the adequacy and effectiveness of the company's internal controls. These requirements address the weakness of responsibility, as now the CEO and CFO² accept personal responsibility for the accuracy of financial statements. To add "teeth" to these certification requirements, SOA also requires companies, on an annual basis, to provide a management report which strenuously evaluates the company's internal controls, including identification of any known deficiencies. Companies' external auditors must also attest to management's report.

Although Sarbanes-Oxley is a complex piece of legislation with many sections, Section 404 is the part that has the greatest relevance and impact for IT.

However, it is still worthwhile to briefly examine other major sections of the legislation:

Section 302 requires the CEO and CFO to make a variety of attestations regarding the accuracy and reliability of quarterly and annual reports. These attestations include assurances that:

- The report does not contain any untrue statements or untrue material items, nor does it omit any material facts that would impact the financial report.
- The report fairly represents the financial condition and performance of the company for the stated period
- The company has in place an adequate set of internal controls to provide assurance that the financial report is a fair representation of the company's position
- Any material deficiencies in the company's internal controls have been disclosed.
- Any fraud conducted by the employees of the company has been disclosed.

Section 906 also requires the CEO and CFO to certify that periodic financial filings fairly represent the company's position and performance. The certification requirements of section 906, however, are somewhat less rigorous than Section 302 because 906 only requires that the executives certify that the financial requirements are in compliance with existing statutes; compliance with section 302 should largely be sufficient for 906 as well. The major change provided by section 906 is the establishment of new, specific criminal penalties for violations.

¹ The Sarbanes-Oxley Act is often referred to as Sarbanes-Oxley, SOA, SOX and SarbOx. In this paper, "Sarbanes-Oxley" and "SOA" will be used as the abbreviated forms.

² In practice, it is the CEO and CFO that will most often be required to provide attestations, but the SOA does allow for other officers to attest as well. For simplicity, we will refer to the base case, which is CEO and CFO.

Together, sections 302 and 906 comprise the bulk of what the average person associates with Sarbanes-Oxley: much more rigorous certifications of financial statements and underlying controls feeding those statements, and specific criminal penalties for violations of the Act.

Section 409 requires that any material changes to the firm's financial condition be disclosed on a rapid and current basis.

SECTION 404: ANNUAL ASSESSMENT OF INTERNAL CONTROLS

Section 404 is the part of Sarbanes-Oxley that has the most significant impact on IT organizations. It requires firms, on an *annual* basis, to issue a report that describes the following:

- Management's responsibilities to establish and maintain an adequate system of internal controls related to financial reporting
- The *framework* used by management for evaluating the effectiveness of the system of internal controls. The framework requirement is a critical one, and is examined in more detail below.
- Management's assessment of the effectiveness of the company's system of internal controls. This assessment *must* also disclose any material weaknesses in the system of internal controls. The SEC has also ruled that the company's external auditor must independently evaluate Management's assessment.

"Internal Controls" has a specific meaning with respect to auditing in general and to regulatory compliance in specific. The SEC has defined the term "internal control over financial reporting" to have the following meaning:

A process designed by, or under the supervision of, the issuer's principle executive and principal financial officers, or persons performing similar functions, and effected by the issuer's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- *Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of assets of the issuer;*
- *Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the issuer; and*
- *Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.*

The definition does not specify whether the process needs to be manual or automated, computer- or paper-based, only that the process exists and is effective.

In principle, the definition does not sound terribly complex. In practice, however, the complexity of modern organizations makes the certification of internal controls extremely challenging. After all, there are many different systems in different parts of the organization that can materially impact financial reporting. HR, payroll, inventory, accounts payable, accounts receivable, purchasing, and order-entry are all

common (and often independent) systems that can materially impact the financial results reported by a firm. This list does not include the myriad custom applications most firms employ in support of their businesses, which also may materially impact the firms' financial reporting.

Given the complexity of most IT environments, significant participation is required from the IT organization in order to ensure that internal controls are not only in place, but are effective as well.

It is important to note that Section 404 really requires 3 things: (1) the organization has *implemented* appropriate controls, (2) that those controls are *effective* and, (3) that the external auditor has *validated* the existence and effectiveness of these controls.

As noted above, the complexity of modern companies means that it may be very difficult to establish the effectiveness of controls if those controls are not automated. In fact, at one point the SEC was considering mandating automation as part of 404 compliance. Even without the *requirement* of automation, however, external auditors will consider whether a non-automated process is both effective and sustainable. For many large organizations, managing access rights over time is neither effective nor sustainable without some degree of automation.

The requirement of *validation* is also important because it means organizations must have an *effective audit trail* for use by their auditors. Without an audit trail, it is very difficult for auditors to determine whether a process, such as access management, is effective or not; the organization simply lacks the information required for an auditor to make such a determination.

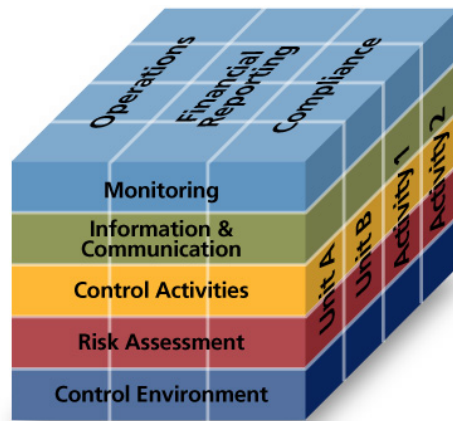
Thus in addition to evaluating technologies that automate effective controls, organizations must also consider the technologies' ability to demonstrate compliance after the fact.

SECTION 404: REQUIREMENT FOR A FRAMEWORK

One of the requirements of Section 404 is that the evaluation of the effectiveness of internal controls must be based on a *recognized framework*. In other words, it is not sufficient for management to say that they have rigorously evaluated their internal controls and found them to be effective. Rather, management must use an evaluation framework that is well recognized and has been subject to extensive public review.

Specifically, the SEC mentions the COSO³ Internal Control – Integrated Framework as being an appropriate framework. Other frameworks, such as Turnbull or King, may also be acceptable, but since the SEC *specifically* mentions the COSO Integrated Framework, many companies view COSO as the safest approach.

The Integrated Framework evaluates internal controls across three dimensions, as described in the following diagram:



The first dimension, on the top of the cube, covers objectives. The purpose of internal controls is to ensure that the organization runs effectively, that financial reporting is accurately performed, and that the organization is in compliance with required statutes.

³ COSO stands for Committee of Sponsoring Organizations of the Treadway Commission, a private sector, non-profit organization dedicated to improving financial reporting. More information can be found at www.coso.org.

The second dimension, along the right side of the cube, covers organizations and activities within the company. Internal controls, when made concrete, apply specifically to units and activities of the company, not to the company as a whole.

The third dimension, on the face of the cube, covers the specific activities required for effective internal controls:

- The Control Environment is generally at a corporate or large business unit level, and refers to the “culture of control” across large organizational units. For example, does the organization promote aggressive or conservative booking of revenue? Are groups that “make their numbers” subject to much lower levels of scrutiny than groups that don’t?
- Risk assessment is the process of identifying and understanding the risks internal controls are designed to mitigate.
- Control Activities are the specific activities (such as ensuring separation of duties) that control and mitigate risk.
- Information and communications means ensuring that the *right* information is communicated to the *right* parties to enable all four of the other activities.
- Monitoring is the process of ensuring, on an ongoing basis, that the controls are operating as expected.

Although the COSO framework provides a strong basis for creating internal controls, it does not provide much guidance specific to IT. Fortunately, the IT Governance Institute (ITGI) has constructed a framework called COBIT that provides very specific governance guidelines for IT organizations.

In the document entitled “IT Control Objectives For Sarbanes-Oxley”, the ITGI describes how to map COBIT to COSO. While each company striving for Sarbanes-Oxley compliance ultimately needs to work with its own legal and audit teams to ensure they’re on the right track, this document provides an excellent starting point for understanding the types of activities required.

Specifically, the document is organized around a set of Control Objectives. An example of a Control-Objective is the following:

“Ensure Systems Security: Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Actions performed in this area align with the control activities, information and communication, and monitoring components of COSO. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in unreliable financial reporting and disclosure controls.”⁴

Within each Control Objective, ITGI provides a number of concrete, actionable items that are generally required to satisfy the objective. We will shortly examine some of these specific items that are relevant for Identity Management.

OVERVIEW OF CONTROL-SA

We now have high-level description of Sarbanes-Oxley and have seen the reliance of Section 404 on an established framework and how the COSO framework provides specific and detailed guidance to ensure internal controls are effective. If we next look at BMC Software’s Provisioning solution - CONTROL-SA, we will be able to see how this system can help address key components of Sarbanes-Oxley compliance.

CONTROL-SA is a modular solution that centralizes and streamlines the identity management process. In most organizations, identity management is a vexing problem. Every platform – operating system, database, application, etc. – has a set of user accounts. Each platform also has a different mechanism for administering its accounts. Simply determining *who* has access to what resources becomes a daunting task, the processes of actually managing those accounts on an ongoing basis is an even more complex challenge. CONTROL-SA employs a proven successful architecture that addresses many of these challenges.

⁴ “IT Control Objectives for Sarbanes-Oxley”, p. 44. The document may be found at www.itgi.org.

The core of CONTROL-SA is an identity repository; in this repository rest all the organization's valid *identities*. CONTROL-SA maps these valid identities to the actual accounts on the different platforms in the enterprise. Built around this core is a set of modular capabilities that enables organizations to deploy as much or as little of the identity management solution as appropriate for their needs.

First and foremost is CONTROL-SA's *provisioning* module. This module enables companies, from a *single* console and a consistent interface, to provision accounts on *all* of the managed platforms in the enterprise.

Instead of requiring multiple administrators to create accounts for a new employee, a Service Desk staff member can simply enter the new employee's information once, select the platforms and associated access levels, and with a click of the mouse complete all provisioning activities.

In view of the expanding auditing requirements promoted by the SOA, the CONTROL-SA architecture provides an equally significant capability in *de-provisioning* activities - when an individual's responsibilities changes or a person leaves the organization: a single mouse-click revokes (or modifies) access across all managed platforms. And because all account information resides in the identity repository, there is no risk that some platforms will be overlooked during the provisioning process.

Another benefit of centralized provisioning is that all provisioning actions are logged. Every time an account is created, modified or deleted, a record of that specific provisioning action is stored in the audit log. Even if an administrator bypasses the CONTROL-SA system, and creates or modifies an account *directly* on the managed platform, CONTROL-SA will identify the change and log it.

The second module manages access request and approval workflows. All provisioning actions are the result of a *request*. That is, someone requests that a person be given access to a system. Managing such requests as they flow through a manual process is typically very inefficient and often error-prone.

The access approval module enables an organization to formalize the way in which requests are handled, to easily track the status of requests, and to provide escalation actions if a request is not processed in a timely fashion.

Additionally, this module helps to enforce *policy* – how requests *should* be processed rather than how they actually wind up being processed in a manual or ad hoc system. As with provisioning activities, all requests and steps in the approval process are recorded in the audit log.

The third module supports password management. This module enables the organization's end-users to manage their own passwords across systems, rather than having to call the Service Desk for assistance. This module enables users to reset their own passwords (either when the passwords expires or when they are forgotten), and synchronize passwords across platforms. Synchronization makes life easier for end-users, since they only have one password to remember. Requiring that users remember only one password allows organizations to enforce stronger password policies.

The unique architecture of CONTROL-SA allows you to deploy these capabilities as modules, rather than as a single monolithic application. It also enables you to extend the identity management solution in new ways. Examples of such extensions are the forthcoming Audit Module, which will assist with regulatory compliance issues raised by statutes like Sarbanes-Oxley, and a new Web Access Module.

The modularity of CONTROL-SA, however, extends beyond "plug-in" modules. On the back-end of the system, where identity data resides and is processed, there are additional modular capabilities. CONTROL-SA can work with a variety of data sources for its identity data, and manage, propagate, or synchronize identity data across those sources. Additionally, CONTROL-SA is built on a highly extensible architecture that is in the process of becoming even more extensible.

BMC Software is a founding member of the OASIS committee responsible for the Service Provisioning Markup Language (SPML) standard. This standard has been finalized and is supported in the new releases of the product.

SPML means very simple integration with any other application or platform that also supports SPML. BMC Software is also enhancing the CONTROL-SA architecture around a J2EE core that enables easy, industry-standard integration to J2EE-compliant applications.

In short, the architecture of CONTROL-SA addresses the three key general requirements of Section 404 as applied to Identity Management: it enables a company to *implement an effective* mechanism of controlling access to SOA-related systems and data, and it creates an audit trail through the process that facilitates *verification* of the systems effectiveness. Additionally, the modular and standards-based architecture provides the highest degree of flexibility in Identity Management generally, both today and moving forward into an unknown future.

MAPPING CONTROL-SA TO THE INTEGRATED FRAMEWORK

Most of the Integrated Framework is concerned with specific elements that ensure accurate and meaningful financial reporting, such as ensuring that orders are accurate, that separation of duties exist, that assets are treated appropriately, and so forth. Underlying many of these elements, however, is an assumption that the *identities* of individuals who are making transactions are themselves accurate and meaningful.

For instance, when someone moves out of the procurement organization, in most instances, that person should no longer have the ability to authorize purchase orders. If the person were able to continue to authorize purchase orders, new opportunities for fraud might exist. Consequently, a number of Control Objectives within the Integrated Framework address issues that are specifically related to Identity Management.

The following table lists some of these Control Objectives and illustrates how an Identity Management solution like CONTROL-SA can help achieve Sarbanes-Oxley compliance⁵.

⁵ The Control Objectives listed here are from the document "IT Control Objectives for Sarbanes-Oxley".

Integrated Framework Control Objective Task	How CONTROL-SA helps Address the POF
Controls are in place to support appropriate and timely responses to job changes and job terminations so that internal controls and security are not impaired by such occurrences.	CONTROL-SA addresses this objective in several ways. First, by managing the business process of requesting changes through an access approval module, the organization processes these changes more quickly and efficiently. The access approval module also enables the organization to set thresholds, so if a request is <i>not</i> processed on a timely basis the request is escalated. Once approved, CONTROL-SA makes the requested changes immediately and automatically
Procedures exist and are followed to ensure that all users are authenticated to the system to support the validity of transactions.	In order for users to properly authenticate to the system, they must first be effectively provisioned to the system. Otherwise controls get circumvented and users “borrow” other users’ credentials to access to the resources they need. By streamlining the provisioning process, CONTROL-SA improves the ability of the company to ensure proper authentication is actually occurring.
Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts	The core functionality of CONTROL-SA is designed to improve the management of ALL aspects of provisioning user accounts, from of the initial request for an access change until the requested change is executed and completed.
Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms	Authentication and access mechanisms are effective only to the extent that they are timely. Password synchronization helps companies enforce stronger password policies, which clearly improves the effectiveness of authentication mechanisms.
A formal approval process exists for granting access privileges to systems and data.	CONTROL-SA’s access approval solution enables organizations to formally define and enforce the way in which requests and approvals are handled. It further enables the organization to better manage and track the inevitable “one-off” requests that come through the system.
A control process exists and is followed to periodically review and confirm access rights.	By mapping all accounts to “identities”, viewing all the access rights associated with a particular person or group of people becomes a simple matter. Additionally, by using role definitions, a company can further simplify the process; now the company only has to verify that: a) the roles are correct, and b) there are no instances where a person’s access is at variance with respect to his or her role.
The IT security administrator monitors and logs security activity, and identified security violations are reported to senior management	CONTROL-SA can help track a variety of security access violations, such as when accounts are modified out-of-process (i.e., an administrator creates or modifies an account directly on a system), when suspicious login attempts are made (i.e., too many attempts to access an account), etc.

Although these issues represent a fairly small part of Sarbanes-Oxley, they are extremely important. Without effective controls around *identity*, it is hard to envision how a firm can provide effective controls for transactions conducted by those identities.

From the regulatory perspective, the process of *managing* identities is no more important than ensuring that the underlying activities are amenable to the audit process.

Returning to the summary of 404: the company must have *implemented* internal controls, those controls must be *effective*, and once a year the external auditor must *validate* the controls. Ultimately validation requires an audit trail: take a random sample of transactions and verify that the controls worked. In other words, validation requires data.

One of the key benefits of CONTROL-SA from a Sarbanes-Oxley perspective is that all transactions are logged. The initial request for access, including who requested what access for whom and when, and every step of the approval process, is logged and available for validation.

Whenever access is changed, both the “before” and “after” states are recorded. Even if changes are made outside of the CONTROL-SA system, CONTROL-SA still notices the change, logs them, and can take corrective action if the change violates policy. Moreover, the use of roles improves audit capabilities by explicitly mapping access rights to the business process.

ADDITIONAL BENEFITS OF CONTROL-SA

As illustrated above, BMC Software's Identity Management solutions address a small but critical aspect of Sarbanes-Oxley. However, the benefits of the solution extend far beyond compliance.

CONTROL-SA provides tremendous benefits both in improving operational efficiency and reducing an organization's security risk profile. These benefits include:

- **Streamlined provisioning time**

It often takes days, if not weeks, to manage the approval process for access changes. During this time the end-user is not productive, because he or she does not have access to the resources needed to do the job.

By managing and automating the request activities, the time to process requests is greatly reduced, resulting in higher productivity for end-users and a more effective work force for the organization.

- **Minimal de-provisioning time**

Not surprisingly, de-provisioning is often more time consuming than provisioning. Without a central provisioning system, it is difficult for an IT organization to know which accounts are 'owned' by a given individual.

De-provisioning with this lack of basic information results in a tedious, manual process that requires a review of all systems and application do determine if any active accounts belong to a departing individual. With a central provisioning system, once the decision is made (e.g., the person resigns), de-provisioning is effectively instantaneous and comprehensive.

- **Reduced Service Desk costs**

On average, 30% of calls to the service desk are for forgotten passwords. By implementing the password management solution, end-users can reset their own passwords and reduce the volume of service desk calls by 70-80%.

This represents *hard dollar savings* to the service desk. There can also be additional savings in organizations in which password resets are handled by 2nd-level support rather than the service desk.

- **Centralized administration**

In most organizations, different IT administration groups perform provisioning activities for each platform and/or application.

Because of this 'silo' approach to user provisioning, redundant (and sometimes contradictory) policies often exist and, fairly expensive resources such as systems administrators often perform the provisioning activities.

A central provisioning system reduces expenses in several ways. First, it moves the provisioning burden from highly paid platform administrators to less expensive service desk personnel. Second, it reduces the actual workload, as only a single provisioning step is required. (Request one change through CONTROL-SA, the system handles the necessary multiple back-end provisioning actions.) Third, because all provisioning is done from a single console, training and skill level requirements are lower.

- **Password security**

By enabling users to synchronize their passwords across multiple platforms, organizations can implement stronger password policies.

Typically the intended effects of strong password policies are diluted by the fact that multiple strong passwords are difficult to remember, so end-users wind up either writing down passwords (making them susceptible to theft) or using easy to guess passwords.

By keeping passwords synchronized, users must remember only one password. This means organizations can achieve the security benefits of strong passwords without the operational weaknesses that often accompany such policies.

- **Elimination of ghost accounts**

When a person leaves a company but not all of his or her accounts are revoked, the "left-behind" accounts are called ghost accounts.

Ghost accounts are favorite targets for hackers because account activities will not be noticed by the now absent valid owner.

Over time, as individuals' roles change or they leave an organization, many ghost accounts are 'created'. In fact, on average 30% of accounts in most organizations are ghost accounts.

One of the first steps in an Identity Management implementation is to match all accounts on all managed platforms to actual *people* (or system identities) in the organization. Any remaining unmatched accounts are by definition ghost accounts, and can be managed appropriately.

In short, the operational and security benefits of BMC Software's Identity Management Solution - CONTROL-SA - extend well beyond simply achieving compliance with the relevant parts of Sarbanes-Oxley.

Implementation of CONTROL-SA provides a solid foundation upon which an organization can build and enhance its security posture while achieving compliance with legislative mandates and, most importantly, all of this can be accomplished while enhancing business operations.



About BMC Software

BMC Software, Inc. [NYSE:BMC], is a leading provider of enterprise management solutions that empower companies to manage their IT infrastructure from a business perspective. Delivering Business Service Management, BMC Software solutions span enterprise systems, applications, databases and service management. Founded in 1980, BMC Software has offices worldwide and fiscal 2004 revenues of more than \$1.4 billion. For more information about BMC Software, visit www.bmc.com

CONTROL-SA
trusted security solutions