

 Sarbanes - Oxley Section 404:
How BMC Software Solutions Address
General IT Control Requirements

TABLE OF CONTENTS

Executive Summary	2
Sarbanes-Oxley Section 404 Internal Controls	3
IT Involvement in Section 404 Compliance	4
The Scope of IT Control Requirements	5
Gap Analysis and IT Audit Preparations	8
Closing the Gap with Systems-Based Controls	9
BMC Software Solutions Meet General IT Control Requirements	11
Strong Controls Bring Benefits Beyond Compliance	18
Conclusion	18
Appendix: Product Overviews	19

EXECUTIVE SUMMARY

The Sarbanes-Oxley Act of 2002 will have a significant impact on IT organizations. In accordance with Sarbanes-Oxley (Sarbox), executives must attest to the adequacy and effectiveness of their internal controls, including IT controls. Internal financial process controls and related IT controls will be externally audited, and a statement of control, including material weaknesses found during the audit, must now appear in annual reports filed with the Securities and Exchange Commission (SEC).

In preparation for a Sarbox audit, companies must identify their significant financial accounts, the business processes that support those financial accounts, and the applications and IT systems that support those business processes. Then they must document and test controls at the financial process level, the application level, and the IT infrastructure level.

The process of identifying and documenting controls may reveal the need to remediate gaps – and a company may need to change some of its IT operations to demonstrate effective internal IT controls relating to financial reporting processes. People may need to change roles, new IT processes may need to be established, or new technology-based solutions may need to be implemented to demonstrate consistent controls.

Although Sarbox does not mandate technology or software-based controls, such controls may ease the compliance process by delivering a cost-benefit equation that is superior to manual or paper-based solutions. Auditors will be looking not only for process consistency, but also for the consistent application of controls over those processes. For this reason, auditors may well be wary of manual or paper-based processes in large or distributed organizations, since an audit trail would be difficult to establish. In many cases, software solutions are the best way to automate controls and enable the required consistency.

BMC Software solutions can help companies improve their general IT controls in areas such as security administration, change management, data management and disaster recovery, operations and problem management, and asset management. These solutions can also bring significant return on investment beyond compliance efforts, including improved operational efficiency, reduced costs and better alignment of IT resources with business requirements.

SARBANES-OXLEY SECTION 404 INTERNAL CONTROLS

The Sarbanes-Oxley Act was enacted in response to the corporate malfeasance cases that emerged in 2001 and 2002. The Act is best known for its requirement that the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) of a company personally certify the company's financial results.

Sarbox is a complex piece of legislation that has many sections, but Section 404 has the greatest relevance and impact for IT. According to Section 404, a company must attest to the adequacy and effectiveness of the company's internal controls for financial reporting. This statement, issued in the company's annual report to the Securities and Exchange Commission (SEC), must include the following:

- > The internal control framework used by management.
- > Management's assessment of the effectiveness of internal controls.
- > Disclosure of any material weaknesses found by the auditor.

The SEC has also ruled that the company's external auditor must independently evaluate management's assessment, and include a statement of any material weaknesses in the company's annual report.

IT INVOLVEMENT IN SECTION 404 COMPLIANCE

Section 404 is concerned with the general controls that maintain the integrity of processing and reporting of financial data. Any process or system that could influence the integrity of transaction processing or data must be examined, and controls must be in place to ensure overall process and system integrity.

A company's financial reporting processes rely on financial applications, which rely on computer systems. Many different systems, in different parts of the organization, can materially affect financial reporting. Human resources, payroll, inventory, accounts payable, accounts receivable, purchasing, order entry and custom applications are all common, and often independent, systems that can materially affect major financial accounts.

In today's highly computerized business environment, IT-related risks and controls must be considered in any overall evaluation of internal control over financial reporting. The Public Company Accounting Oversight Board (PCAOB), which was established by the Sarbanes-Oxley Act to oversee the audits of public companies, specifically mentions the importance of IT systems and IT general controls in its auditing guidelines dated March 9, 2004. Because external auditors will follow PCAOB guidelines during the audit process, companies need to document and evaluate the IT systems and controls that contribute to the financial reporting process. A company cannot pass an audit and demonstrate control of its financial reporting process without control of the underlying systems and IT management.

According to guidance provided by Protiviti, a leading Sarbanes-Oxley consulting firm, "The independent accountant will have IT-related risks and controls in mind when evaluating the basis for management's assertions in the internal control report. The general IT controls are pervasive controls that impact the integrity of most, if not all, transactions, as well as most, if not all, of the internal financial reports from which the financial statements are derived. A weakness in general IT controls potentially could have an effect over significant transactions and accounts. If there are gaps in the general IT controls, it is possible that the external auditor could insist that those gaps be addressed before an overall opinion is reached on the effectiveness of the internal controls."¹

Given the complexity of most IT environments, then, significant participation is required from the IT organization to ensure that internal controls are not only in place, but are effective, as well. The scope of what may be covered in an IT audit, as well as the process used by the auditor, are determined by the auditor. Any questions regarding scope or process should be addressed during preparations with the auditor selected.

¹ Frequently Asked Questions," Guide to the Sarbanes-Oxley Act: IT Risks and Controls, Protiviti, December 2003, p. 29.

THE SCOPE OF IT CONTROL REQUIREMENTS

The integrity of financial data relies on the integrity of the underlying IT systems. In most companies, IT provides the infrastructure for the processing, storage, and communication of financial data. Effective IT controls help ensure that the integrity of the financial data is maintained.

Auditors will review current process and control documentation to meet the requirements of specific control objectives at three levels. (See Figure 1.)

- > Organization level
- > Entity level
- > Process level

At the highest level, the external auditor will review control objectives related to the overall IT organization and structure. Starting at this level helps auditors determine a general control environment. Lack of controls at this level may not be considered a material weakness, but may give auditors insight into the general “tone at the top” of the IT organization. Discovering lack of controls at this level may cause an auditor to dig deeper at the other levels.

At the next level, the auditor will evaluate IT entity-level controls. Here, the auditor looks at the distributed organization, and scopes the control requirements based on division of process and responsibilities within the business unit, division of process and responsibilities by geography, and assessment of third party service provider process and responsibilities.

At the lowest level, the auditor will review IT process-level controls.

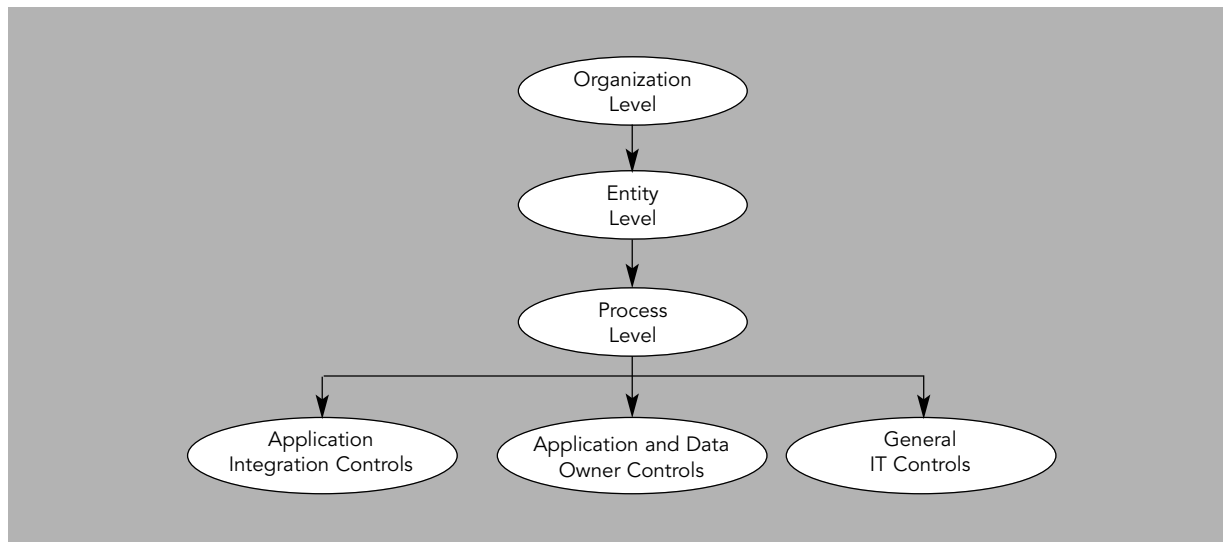


Figure 1: Three levels of IT control²

2 Based on diagram in “Frequently Asked Questions,” Guide to the Sarbanes-Oxley Act: IT Risks and Controls, Protiviti, December 2003, p.9.

At the process level, auditors will verify documentation and control that relate to control objectives in three primary areas:

- > Application integration controls
- > Application and data owner controls
- > General integration controls

Application integration controls provide a holistic way to evaluate IT controls that apply to multiple applications working together to process financial data. Application and data owner controls, which are the responsibility of the overall process owner, such as the owner of the accounts receivable or payroll process, include those controls specific to the applications and data related to those functions.

General IT controls address critical IT processes within each business entity or geographical organization, and include the operations of third party service providers that have access to applications or infrastructure within scope. General IT controls are designed to prevent, or detect and correct, undesired events that could compromise the integrity or transactions, data processing, and resulting data. General IT controls help ensure the proper management and function of the IT infrastructure that supports the financial reporting process, applications, and application integration. Effective general controls also provide a foundation for application and data-owner process controls that are integrated into software programs, such as an enterprise resource planning (ERP) system.

At the Process level, within the realm of General IT controls, the evaluation of controls should include five critical general IT process areas:

- > Security administration
- > Application change management
- > Data management and disaster recovery
- > Operations and problem management
- > Asset management

Controls in these five areas are critical to the integrity of the processes, systems and applications that contribute to a company's ability to produce accurate, reliable financial statements.

Strong general IT controls may reduce the need for a company to prepare additional documentation and compensating controls for Section 404 compliance. If general controls are weak, then the entire financial reporting process may be compromised. For example, a security or general process breach may open the possibility for unauthorized actions. Weak controls in the five areas of general IT controls may be considered material weaknesses, and will most likely require some type of remediation to pass an audit.

An auditor will systematically check controls by working through various control objectives detailed in a control framework. Companies must specify and use a recognized control framework to evaluate their controls. The IT Governance Institute (ITGI) has constructed an IT-focused control framework called Control Objectives for Information and related Technology (COBIT) that provides very specific IT governance guidelines. The ITGI also has published a subset of COBIT for Sarbox audit

preparation called IT Control Objectives For Sarbanes-Oxley, which includes detailed control objectives in twenty-seven different process areas. Many companies are using this subset of COBIT to evaluate their IT controls for Sarbox compliance. The relationship between these controls and the five general IT process areas are discussed later in this paper.

Other frameworks, such as the IT Infrastructure Library (ITIL[®])³ define best practices for IT service management and can help companies working toward Sarbox compliance.

ITIL, COBIT AND SARBANES-OXLEY

The Information Technology Infrastructure Library (ITIL) is an industry-leading set of IT Service Management best practices. These best practices for the support and delivery of IT services can help a company document IT processes as required for Sarbanes-Oxley.

Troy DuMoulin, managing consultant at Pink Elephant – an organization providing ITIL based consulting, education, conferences and outsourcing services, notes a shift in how organizations approach best practices for IT services: “In the past, companies used best practices out of a desire for self improvement and to create a positive impact on the bottom line. Now, with Sarbanes-Oxley, they have to do it because it’s a formal, legal requirement.”

ITIL is part of the foundation of the COBIT model, which defines control objectives for IT in support of business processes. COBIT was

explicitly chosen as the tool of choice for external auditors to use in IT audits for Sarbanes-Oxley. “Since auditors are using COBIT, it makes sense for organizations to learn about the model. The model identifies key performance indicators and critical success factors that organizations can take into consideration when documenting or re-engineering a process,” DuMoulin says.

“Although there are many different control frameworks out there, many of them have ITIL at their core. With COBIT for example, 45-50% of the control objectives are covered within ITIL. In particular, ITIL’s Service Support and Service Delivery processes address almost a dozen specific control objectives,” DuMoulin says.

The ITIL process documentation and COBIT control objectives are a powerful combination that can accelerate Sarbox compliance.

3 ITIL is a registered trade mark of OGC – the Office of Government Commerce

GAP ANALYSIS AND IT AUDIT PREPARATIONS

In preparation for a Section 404 external audit, companies are identifying Sarbanes-Oxley task forces comprised of IT audit and IT operations team members. The teams are mapping their companies' financial processes to major accounts, documenting processes, doing risk assessment and testing controls.

A company's IT compliance team would examine both the applications that generate financial data and the underlying systems on which the applications run. In addition to examining the application and data owner controls, the team would also look at the general IT controls for related infrastructure.

Many IT compliance teams are using a gap analysis approach to audit preparation. The gap analysis approach shown in figure 2 includes:

- > Assess current state IT process
- > Identify and document related IT risks
- > Identify and document related IT controls
- > Test controls to make sure they meet the required objectives
- > Identify the gaps or the new capabilities needed to meet the objective
- > Improve current state with new people, process or technology

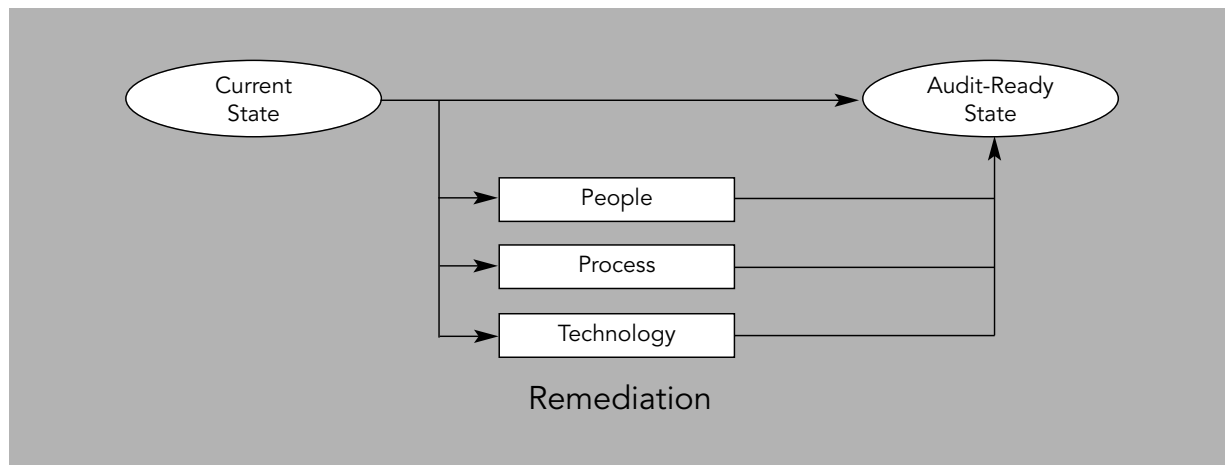


Figure 2: Audit preparation gap analysis

Gaps often can be categorized as people, process or technology gaps. For example, logging tools might capture voluminous data about the operations of IT systems, but the appropriate filtering tools and people might not be in place to enable a timely response to critical incidents. Or, a company might use a change management tool for infrastructure changes but not use the tool's capabilities for managing application changes. In that case, a gap exists in the process. Finally, the appropriate people and process may be in place, but the particular technology needed to ensure the efficiency and repeatability required by Section 404 may not.

After compliance teams identify and remediate the gaps, management must test and certify that proper internal controls are in place. To complete the annual compliance effort, an external auditor will review process and control documentation, re-test controls, and attest whether a company has effective IT controls in place – ensuring that those controls are not only designed, but are also effective and consistently being used.

CLOSING THE GAP WITH SYSTEMS-BASED CONTROLS

As companies identify the gaps in their general IT controls, they may choose different solutions to remediate those gaps. If a problem demands either a people- or process-oriented solution, then adjustments to current systems or new manual processes might resolve the deficiency. In some companies, documenting the current way of doing things may be adequate to pass an audit. However, for many companies, automated software systems are needed to ensure systems-based control over critical IT processes.

There are two key reasons why new systems-based controls may be the best way to achieve the consistency necessary to pass audit requirements.

First, for large or distributed organizations, manual or paper-based solutions may not meet auditors' requirements. According to Fred Roth of the MIS Training Institute, "The larger the organization, the more software-based control there should be." Roth, who has worked for 25 years in system development and IT audit and security, now provides consulting and training about Sarbanes-Oxley requirements to IT auditors. "The more we see manual controls, the more questions we ask—and the more we get nervous about the internal controls being consistently followed. Just having software is not going to ensure compliance, but it gives us an extra level of comfort."

A critical factor in large distributed companies is consistency. "Auditors look for consistent application of the process and of the control," Roth says. "You can install software and not consistently use it. On the other hand, if you install software and use it the way it's supposed to be used, and the software is effective in providing consistency, then it can help show compliance."

Systems-based solutions help ensure consistency in both processes and controls. These tools enable organizations to prove control on the basis of rules-based workflow, forcing everyone to use the same process in the same automated form. These tools also capture data automatically, providing comprehensive audit trails and reports. Proving control can be much more difficult when using a manual process, because it is difficult to prove the process is always followed.

The second key reason for new systems-based control solutions is that modifying current manual or paper-based processes to meet audit requirements may reduce operational efficiency and significantly increase cost. For each difficult compliance area, companies should conduct a basic cost-benefit analysis. If the only benefit of modification is compliance, and if modification would increase operating costs, then implementing new automated solutions may be the best approach.

According to Paul Hamerman and Robert Markham of Forrester Research, public companies with revenues of more than \$500 million and those with multiple divisions and lines of business should adopt a technology-based approach to Sarbox compliance. Using software to automate compliance, particularly for the internal controls required by Section 404, is an opportunity to make the process more efficient, sustainable, and transparent.⁴

4 Paul Hamerman and Robert Markham, Sarbanes-Oxley Solutions — Invest Or Pay Later: Hybrid Applications Emerge For Internal Controls Compliance, Forrester Research, March 11, 2004.

BMC SOFTWARE SOLUTIONS MEET GENERAL IT CONTROL REQUIREMENTS

Preparing for Sarbox audits and ongoing compliance requires companies to examine the processes and systems that contribute to the integrity of their financial reporting. For years, BMC Software has helped companies manage their most critical IT services by facilitating a better understanding of the relationship between IT and the business. This approach is the basis of Business Service Management (BSM), BMC Software’s dynamic IT management strategy – supported by technology – that enables companies to align IT resources with business priorities.

Companies that have implemented BSM and established their IT service model, can quickly identify the applications and underlying IT infrastructure involved in financial processes that feed major accounts. They can then rely on BMC solutions as systems-based controls in twelve key COBIT process areas.

For companies that do not yet have a BSM approach, adopting best practices required for Sarbox compliance is a good first step toward achieving the benefits of aligning IT with the business. With BMC Software, you can develop a BSM strategy that aligns people, processes and technology with key business objectives. In the context of Sarbox, BMC Software’s solutions focus on one primary area: controls of general IT processes.

Many BMC Software solutions can help you close gaps and implement systems-based general controls in twelve of the twenty-seven COBIT process areas that are relevant to Sarbanes-Oxley, as shown in Table 1. It’s important to note that these solutions each have different features and capabilities. Each company should conduct a gap analysis and rely on guidance from external auditors to identify areas that need improvement, and identify gaps that are best closed with systems-based solutions.

FIVE KEY GENERAL IT CONTROL AREAS	TWELVE COBIT PROCESS AREAS
Security administration	<ul style="list-style-type: none"> • DS5 Ensure systems security
Application change control management	<ul style="list-style-type: none"> • AI2 Acquire and implement application software • AI3 Acquire and implement technology infrastructure • AI6 Manage changes
Data management and disaster recovery	<ul style="list-style-type: none"> • DS4 Ensure continuous service • DS11 Manage data
Operations and problem management	<ul style="list-style-type: none"> • DS1 Define and manage service levels • DS3 Manage performance and capacity • DS10 Manage problems and incidents • DS13 Manage operations • M1 Monitor the processes
Asset management	<ul style="list-style-type: none"> • DS9 Manage the configuration

Table 1: Mapping key IT general control areas to COBIT control objectives

The remainder of this paper will focus on how BMC Software solutions can help close the gap with systems-based control solutions in the five key areas of general IT controls.

SECURITY ADMINISTRATION

One of the key areas of general IT controls is security administration, or the ongoing processes necessary to ensure that only the appropriate people have access to a company’s data and IT assets, such as applications, databases, operating systems and networks. In some organizations, security administration of these assets may be distributed and performed by different groups in the IT department.

Security administration also should account for users and administrators who have full access to IT systems and data. Controls should be in place to limit access to those with a business “need to know,” and mechanisms should allow organizations to monitor the actions of such users.

If you can’t manage the access to applications, networks and databases that are tied to financial processes, you can’t maintain the integrity of financial reports. To protect the integrity of your financial data and processes, you need general IT controls to support the security of the underlying IT infrastructure. To pass the IT audit, you will have to demonstrate consistent and reliable provisioning, authentication, authorization and identity management processes. BMC Software solutions can help you address security-related COBIT control objectives, as shown in Table 2.

COBIT CONTROL OBJECTIVE	BMC SOFTWARE SOLUTIONS
<p>DS5 –Ensure systems security Manage systems security to prevent unauthorized access and ensure integrity of financial data.</p> <p>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.</p>	<ul style="list-style-type: none"> • CONTROL-SA® • CONTROL-M • SmartDBA™

Table 2: Solutions that map to security control objectives.

APPLICATION CHANGE MANAGEMENT

Changes to applications and the technology infrastructure can greatly affect a company’s ability to maintain internal control over financial reporting. For example, when a company makes changes to the applications that process the data that feeds major accounts and financial statements, a loss of data integrity could occur. Similarly, changes to underlying infrastructure components may cause failures that degrade data integrity.

A company needs effective change management procedures so that all application and infrastructure changes are consistently tested and approved before being deployed in a production environment. A change management process should also include the capability to monitor activity and identify unacceptable changes – even those made by people who have the authority to do so.

The application software and technology infrastructure that support the financial reporting process must be designed, built/acquired, deployed, maintained and modified consistently and according to established policies.

BMC Software solutions can help you address COBIT control objectives that focus on application change management, as shown in Table 3.

COBIT CONTROL OBJECTIVE	BMC SOFTWARE SOLUTIONS
<p>AI2 –Acquire and implement application software Acquire, deploy, and update applications that support financial processes in order to protect the integrity of transactions and data processed by those applications.</p> <p>Deficiencies in this area may have a significant impact on financial reporting and disclosure. For instance, without sufficient controls over application interfaces, financial information may not be complete or accurate.</p>	<ul style="list-style-type: none"> • Remedy® Change Management • Remedy® Asset Management • PATROL®
<p>AI3 – Acquire and implement technology infrastructure Acquire, deploy, and update the technology infrastructure that supports financial processes in order to protect the integrity of transactions and data.</p> <p>Deficiencies in this area may have a significant impact on financial reporting and disclosure. For instance, without sufficient controls over network communications, financial information could be obtained and publicized without authorization.</p>	<ul style="list-style-type: none"> • Remedy® Change Management • Remedy® Asset Management
<p>AI6 – Manage changes Manage and control system production environment changes to ensure control and integrity of financial accounts.</p> <p>Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, changes to the accounts to which financial data are allocated require appropriate controls to ensure classification and reporting integrity.</p>	<ul style="list-style-type: none"> • Remedy® Change Management

Table 3: Solutions that map to application change management control objectives.

DATA MANAGEMENT AND DISASTER RECOVERY

Effective data management is extremely important for organizations today. As defined in the COBIT control objectives, data management should support information integrity, including its completeness, accuracy, authorization and validity. For this reason, “data management” includes the backup, management, recovery and restoration of data. To maintain the completeness and accuracy of financial data and transactions, a company must be able demonstrate the ability to restore or restart the processing while sustaining operations. The data management process also should include an assessment of the importance of the applications to the business. That assessment should guide a company’s backup policies and schedule.

If a disaster occurs, established disaster recovery and business continuity plans can improve your company’s ability to recover data and produce timely financial statements. From a Sarbox compliance perspective, disaster recovery is a “gray” area about which audit authorities have differing opinions. Therefore, each company must consult with its auditor to determine the level of control that is required to pass an audit.

BMC Software solutions can help you address COBIT control objectives related to data management and disaster recovery, as shown in Table 4.

COBIT CONTROL OBJECTIVE	BMC SOFTWARE SOLUTIONS
<p>DS4 –Ensure continuous service</p> <p>Manage continuous service, including controls to manage various disaster scenarios, from backup and recovery to full business continuity, to ensure the ability to produce financial statements in a timely manner.</p> <p>Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, the inability to recover from a disaster after year-end could prevent the organization from producing financial reports that are supported with source documentation and details of transactions that make up financial reporting balances.</p>	<ul style="list-style-type: none"> • BMC® Service Impact Manager • PATROL® • SmartDBA™
<p>DS11 – Manage data</p> <p>Manage data to include controls and procedures to support information integrity, including its completeness, accuracy, authorization, and validity. Controls support initiating, recording, processing and reporting financial information to ensure reliability of financial data.</p> <p>Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, without appropriate authorization controls over the initiation of transactions, resulting financial information may not be reliable.</p>	<ul style="list-style-type: none"> • SmartDBA™

Table 4: Solutions that map to data management and disaster recovery control objectives

OPERATIONS AND PROBLEM MANAGEMENT

Operations and problem management are necessary to help ensure the integrity, completeness and accuracy of financial data and transactions. A company must demonstrate the ability to respond to system failures so that operations are sustained and the integrity and completeness of financial transactions or data are maintained.

A company's operations and problem management processes can help maintain effective operations and facilitate consistent responses to incidents that disrupt IT operations. IT service levels should be established to meet your business objectives, and system performance and capacity should be sufficient to support transactions and financial reporting processes. Furthermore, your IT organization should have the ability to prevent, minimize and respond to events that interrupt normal operations of IT systems.

BMC Software provides numerous solutions to assist you in meeting COBIT control objectives focused on operations and problem management, as shown in Table 5.

WHAT WAS ONCE CONSIDERED BEST PRACTICE – IS NOW THE LAW

COBIT CONTROL OBJECTIVE	BMC SOFTWARE SOLUTIONS
<p>DS1 – Define and manage service levels</p> <p>Define and manage operations service levels to meet requirements specific to financial processes.</p> <p>Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, if systems are poorly managed or system functionality is not delivered per agreed-upon service levels, financial information may not be processed as intended.</p>	<ul style="list-style-type: none"> • Service Level Management Solutions from BMC Software • Remedy® Service Level Agreements
<p>DS3 – Manage performance and capacity</p> <p>Maintain complete and accurate data. They also allow an organization to trace back transactions to source information to support their validity.</p> <p>The lack of performance and capacity could result in the financial reporting process not meeting its reporting deadlines.</p>	<ul style="list-style-type: none"> • PATROL® • MAINVIEW® • BMC® Service Impact Manager • SmartDBA™
<p>DS10 – Manage problems and incidents</p> <p>Respond to system failures consistently and effectively in order to sustain operations and preserve the integrity of financial data.</p> <p>Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, significant events such as breach of corporate security or unauthorized access to confidential information may result in a material weakness in disclosure controls.</p>	<ul style="list-style-type: none"> • Remedy® Help Desk • PATROL®
<p>DS13 – Manage operations</p> <p>Maintain reliable application systems in support of the business to initiate, record, process, and report financial information.</p> <p>Deficiencies in this area could significantly impact an entity’s financial reporting. For instance, lapses in the continuity of application systems may prevent an organization from recording financial transactions and, thereby, undermine its integrity.</p>	<ul style="list-style-type: none"> • PATROL® • SmartDBA™ • MAINVIEW®
<p>M1 – Monitor the processes</p> <p>Monitor to ensure that the collection of information aligns with the information and communication and monitoring components of COSO. If insufficient information is collected, it could impact the effectiveness of internal control assessment.</p>	<ul style="list-style-type: none"> • PATROL® • Remedy® Service Level Agreements • Remedy® Flashboards®

Table 5: Solutions that map to operations and problem management control objectives

ASSET MANAGEMENT

Asset management, from an audit perspective, involves accounting for IT assets — from requisition and receipt to installation and maintenance, and finally to retirement. Companies should periodically verify the list of IT assets and evaluate the recorded balances, as well as ensure the realization of assets over their useful life. Finally, companies must also carefully monitor proper use of software licenses to avoid the issue of unrecorded liability, as well as the possibility of violating software usage laws, which may be a disclosure requirement of the auditor.

These reporting issues are similar to those relating to all fixed assets. They appear in general IT controls because processing and accounting of these assets is often an IT area of responsibility, with separate processes and oversight distinct from other fixed assets. The management of IT asset general controls overlaps with control responsibility in the process level, and application and data owner areas.

An audit will require you to properly account for your IT assets – throughout the entire asset lifecycle. You will also need to configure hardware and software to minimize unauthorized access to systems and data. Therefore, security, availability and processing integrity controls should be established in the system and maintained through the asset lifecycle.

BMC Software offers solutions to help you demonstrate that process and systems are in place to control asset and configuration management, as outlined in Table 6.

COBIT CONTROL OBJECTIVE	BMC SOFTWARE SOLUTIONS
<p>DS9 –Manage the configuration</p> <p>Ensure that security, availability and processing integrity controls are set up in the system and maintained through an asset’s lifecycle.</p> <p>Deficiencies in this area could create security and availability exposures. Configuration errors could permit unauthorized access to systems and data that could jeopardize accuracy of financial information.</p>	<ul style="list-style-type: none"> • Remedy® Asset Management • CONTROL-SA® • SmartDBA™

Table 6: Solutions that map to asset management control objectives

STRONG CONTROLS BRING BENEFITS BEYOND COMPLIANCE

BMC Software solutions not only help IT organizations implement systems-based controls to improve the general IT controls necessary for Sarbox compliance, but they also deliver significant operational benefits and financial Return On Investment (ROI), helping you to manage IT resources from a business perspective.

Using BMC Software solutions, you can manage the IT-to-business impact of IT operations and deliver the quality of service those relationships demand by managing IT assets, monitoring their health, and tracking their effectiveness—all from a business perspective. BMC Software solutions help you preempt problems, diagnose causes, and prevent recurrence, increasing the responsiveness of the IT organization, the support it provides, and the business service it enables.

Managing IT risks and ensuring the integrity of business operations is crucial in an ever-changing environment. BMC Software products can help you automate processes, take advantage of best-practice methods, predict the impact of IT changes, manage identities, and maintain system performance. Finally, in business terms, these tools enable:

- > **Improved operational efficiency** – prioritize and optimize IT resource usage based on business impact.
- > **Reduced costs** – Integrate and automate key IT functions to reduce resource and asset costs.
- > **Better IT/Business alignment** – Align IT objectives with the needs of the business to ensure success of strategic business initiatives.

CONCLUSION

On the road to Sarbox compliance, auditors will require companies to demonstrate a documented process and control plan for specific control objectives. Some objectives may not be easily controlled by an adjustment to an existing process or control, or they may not be cost-effectively solved using a new simple manual process or control. In those cases, systems-based solutions, such as those from BMC Software, may offer a more compelling cost-benefit equation than manual processes and controls.

Companies can use BMC Software products to automate controls that support Sarbanes-Oxley compliance. These products can improve general IT controls and increase the efficiency of the ongoing compliance process. Furthermore, BMC Software can offer compelling solutions and real ROI with business and operational value beyond the compliance checklist. For more information, please contact your sales representative or visit www.bmc.com and www.remedy.com.

APPENDIX: PRODUCT OVERVIEWS

PRODUCT	OVERVIEW
BMC Service Impact Manager	<ul style="list-style-type: none"> • A real-time service impact management solution that helps identify related financial applications, underlying systems and databases of any software or infrastructure change as well as any infrastructure implementation or maintenance activity • Ties systems level monitoring back to related financial applications and helps automatically respond to monitored levels that exceed specifications
CONTROL-M	<ul style="list-style-type: none"> • A business integrated scheduling product that focuses on the production environment's business applications and platforms. • Provides advanced production-scheduling capabilities across the enterprise from a single point of control. Control-M for FTP monitors and schedules FTP and secured FTP.
CONTROL-SA	<ul style="list-style-type: none"> • An all-encompassing identity management solution that enables automated and simplified management of all enterprise security systems from a central point of control • Centralizes management of all aspects of provisioning user accounts for financial applications
MAINVIEW	<ul style="list-style-type: none"> • A comprehensive suite of management, monitoring, automation and optimization solutions for the operating system, subsystems, network, middleware, web, storage • Monitors performance of entire mainframe environment
PATROL	<ul style="list-style-type: none"> • A comprehensive suite of managing and monitoring solutions for infrastructure components, including servers, networks and databases • Provides network communications controls to prevent unauthorized access to financial information • Manages application response time service levels and report deviations, and monitors performance of hardware, database, or network systems • Provides "find and fix" support, accelerating time to close problems
Remedy Asset Management	<ul style="list-style-type: none"> • A complete solution that tracks and manages enterprise assets, their configurations and standard configurations in configuration/asset database • Ensures that software meets configuration and software-licensing requirements
Remedy Change Management	<ul style="list-style-type: none"> • A single consolidated change management system that automates planning and managing all application and system change requests • Ensures that all application and infrastructure change requests follow standard documented procedures and approval workflow, and creates an auditable record of each change
Remedy Dashboards	<ul style="list-style-type: none"> • A monitoring solution that presents key metrics from Remedy applications graphically, dynamically and in real time • Provides visual alerts that conditions are outside of acceptable ranges <p>A comprehensive IT service management solution that supports integrated ITIL incident and</p>
Remedy Help Desk	<ul style="list-style-type: none"> • problem management processes <p>Provides automatic escalations through built-in workflow, while incident and problem ticket creates complete audit trail of steps taken, approvals and resolution</p>
Remedy Service Level Agreements	<ul style="list-style-type: none"> • A complete IT service level agreement solution <p>Defines and manages service level agreements between business users and internal or outsourced IT service providers</p>

WHAT WAS ONCE CONSIDERED BEST PRACTICE – IS NOW THE LAW

PRODUCT	OVERVIEW
Service Level Management Solutions	<ul style="list-style-type: none">• Solutions that allows users to define service level agreements (SLAs) and then measure, manage, monitor and report on SLA status to ensure proactive service level management• Includes SLAs relating to system response time, system availability and other service and support functions
SmartDBA	<ul style="list-style-type: none">• Complete database administration and monitoring solution that optimizes performance and availability• Provides sophisticated backup and recovery management with “find and fix” support, greatly improving application availability• Extensive identification and correction of database security exposures

REFERENCES

COBIT Management Guidelines, Third Edition. Information Systems Audit and Control Foundation and IT Governance Institute. July 2000.

“Frequently Asked Questions.” Guide to the Sarbanes-Oxley Act: IT Risks and Controls. Protiviti. December 2003.

IT Control Objectives for Sarbanes-Oxley. IT Governance Institute. 2003.

Sarbanes-Oxley Solutions—Invest or Pay Later: Hybrid Applications Emerge for Internal Controls Compliance. Forrester Research, March 11, 2004.



About BMC Software

BMC Software, Inc. [NYSE:BMC], is a leading provider of enterprise management solutions that empower companies to manage IT 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 2003 revenues of more than \$1.3 billion. To learn more about Business Service Management solutions from BMC Software, visit us on the Web at www.bmc.com/bsm or call 1-800-278-4262.

About Remedy, a BMC Software company

Remedy, a BMC Software company, delivers Service Management software solutions that enable organizations to align internal and external service and support processes to business goals. More than 10,000 customers worldwide, from small and medium businesses to global enterprises, have chosen Remedy software to automate their support processes, improve service levels, manage assets, and lower costs. Remedy's highly flexible, best-practice applications enable enterprise-wide Business Service Management, and allow customers to easily adapt to unique and changing requirements.

BMC Software, Remedy a BMC Software company, the BMC Software logos, and Remedy logo, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc. All other registered trademarks or trademarks belong to their respective companies. ©2004 BMC Software, Inc. All rights reserved.