

MAGIC  
WHITE PAPER

Sarbanes-Oxley Section 404: How  
Magic IT Service Support Addresses  
General IT Control Requirements

---

*What was once considered a best practice is now the law*

**Table of Contents**

Introduction . . . . . 2

Executive Summary . . . . . 2

Sarbox Section 404 Internal Controls . . . . . 2

IT Involvement in Section 404 Compliance . . . . . 3

The Scope of IT Control Requirements. . . . . 3

Gap Analysis and IT Audit Preparations. . . . . 5

Closing the Gap with Systems-Based Controls . . . . . 5

Magic IT Service Support Applications Meet  
General IT Control Requirements . . . . . 6

Strong Controls Bring Benefits Beyond Compliance . . . . . 9

Conclusion . . . . . 9

Appendix: Product Overviews . . . . . 10

## Introduction

With more than 10 years in Service Management, and more than 10,000 customers worldwide, Remedy, a product line of BMC Software, has a history of innovation in the area of IT Governance and Best Practices. To support our leadership in this arena, a white paper was written to provide enterprise organizations with information to help them pass the IT audit required for Sarbox compliance.

As the leading provider of IT Service Management solutions for businesses of all sizes, we understand that large enterprises are not the only organizations impacted by the Sarbanes-Oxley Act. Rather, any publicly traded company in the United States—regardless of size—is impacted by this law.

Magic IT Service Support for the Mid-sized Business was developed specifically for mid-sized organizations looking to optimize efficiency, increase customer satisfaction, and lower costs. Now, with the deadline for Sarbox approaching, these same solutions can also help you to prepare for the IT audit portion of your company's Sarbox audit.

To help you understand how the Magic IT Service Support product line can help, we have repurposed this original white paper to focus on those aspects of the law most relevant to your mid-sized business. The paper explores the issues and challenges facing organizations as they prepare for their IT audit, and includes information on how Magic IT Service Support can facilitate that process.

## Executive Summary

The Sarbanes-Oxley Act of 2002 will have a significant impact on the IT organizations of mid-sized businesses. 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. They must also 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 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.

Magic IT Service Support solutions can help companies improve their general IT controls in areas such as security administration, change management, data management, 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.

## Sarbox 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:

1. Management responsibility for establishing and maintaining adequate internal control over financial reporting.
2. The internal control framework used by management.
3. Management's assessment of the effectiveness of internal controls.

#### 4. 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. In addition, the SEC has also mandated that companies perform quarterly evaluations of changes that have materially or are reasonably likely to affect the companies' internal controls over financial reporting.

U.S. companies that have an equity market capitalization of more than \$75 million must comply with these reports by June 15, 2004, and all public companies below the \$75 million mark have until April 15, 2005. No matter what the date, the need to have a strong internal control framework that can be validated is a must. Manual internal control processes will drive up costs; however, using IT to ensure an effective framework can reduce the costs of a manual process and provide a more reliable process.

#### 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 Sarbox 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."<sup>1</sup>

Given the complexity of most IT environments, 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.

#### 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, page 4)

1. Organization level
2. Entity level
3. 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

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

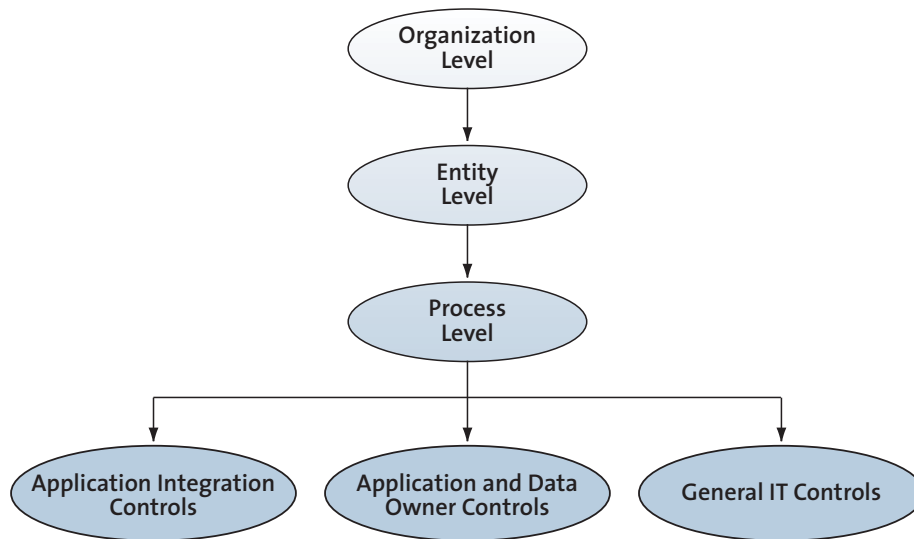


Figure 1: Three levels of IT control

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

1. Application integration controls
2. Application and data owner controls
3. 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.

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

**ITIL, COBIT and Sarbox**

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 Sarbox.

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 Sarbox, 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.

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 27 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<sup>2</sup>), define best practices for IT service management and can help companies working toward Sarbox compliance (see sidebar)<sup>2</sup>.

**Gap Analysis and IT Audit Preparations**

In preparation for a Section 404 external audit, companies are identifying Sarbox 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:

1. Assess current state IT process
2. Identify and document related IT risks
3. Identify and document related IT controls
4. Test controls to make sure they meet the required objectives
5. Identify the gaps or the new capabilities needed to meet the objective
6. Improve current state with new people, process or technology

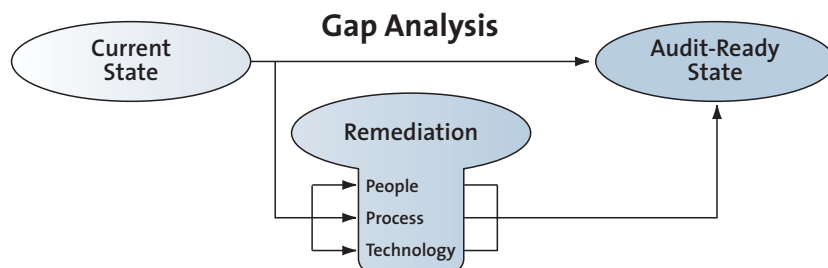


Figure 2: Audit preparation gap analysis

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

2 ITIL<sup>®</sup> is a registered trade mark of OGC - the Office of Government Commerce.

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, 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 Sarbox 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 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.

### Magic IT Service Support Applications 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. Many Magic IT Service Support solutions can help you close gaps and implement systems-based general controls in eight of the 27 COBIT process areas that are relevant to Sarbox, 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.

Table 1

Key General IT Control areas	COBIT process areas
Security administration	<ul style="list-style-type: none"> <li>▪ DS5 Ensure systems security</li> </ul>
Application change control management	<ul style="list-style-type: none"> <li>▪ AI2 Acquire and implement application software</li> <li>▪ AI3 Acquire and implement technology infrastructure</li> <li>▪ AI6 Manage changes</li> </ul>
Operations and problem management	<ul style="list-style-type: none"> <li>▪ DS1 Define and manage service levels</li> <li>▪ DS10 Manage problems and incidents</li> <li>▪ DS13 Manage operations</li> </ul>
Asset management	<ul style="list-style-type: none"> <li>▪ DS9 Manage the configuration</li> </ul>

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

The remainder of this paper will focus on how Magic IT Service Support applications 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. Magic IT Service Support for the Mid-sized Business solutions can help you address security-related COBIT control objectives, as shown in Table 2.

**Table 2**

COBIT Control Objective	Software Solutions
<p><b>DS5 –Ensure systems security</b> 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>	<p>P-Synch<sup>®</sup> Password Management from M-Tech Information Technology (partner product)</p>

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.

**Table 3**

COBIT Control Objective	Software Solutions
<p><b>AI2 –Acquire and implement application software</b> 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"> <li>▪ Magic Change Management</li> <li>▪ Magic Desktop Automation Suite</li> </ul>
<p><b>AI3 – Acquire and implement technology infrastructure</b> 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"> <li>▪ Magic Change Management</li> <li>▪ Magic Desktop Automation Suite</li> </ul>
<p><b>AI6 – Manage changes</b> 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"> <li>▪ Magic Change Management</li> </ul>

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

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. Magic IT Service Support can help you address COBIT control objectives that focus on application change management, as shown in Table 3.

## 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.

Magic IT Service Support provides numerous solutions to assist you in meeting COBIT control objectives focused on operations and problem management, as shown in Table 4.

Table 4

<p><b>DS1 – Define and manage service levels</b> 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"> <li>▪ Magic Service Desk Suite</li> </ul>
<p><b>DS10 – Manage problems and incidents</b> 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"> <li>▪ Magic Service Desk Suite</li> </ul>
<p><b>DS13 – Manage operations</b> 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"> <li>▪ Magic Service Desk</li> </ul>

Table 4: 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, 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.

Magic IT Service Support helps you demonstrate that process and systems are in place to control asset and configuration management, as outlined in Table 5.

**Table 5**

COBIT Control Objective	BMC Software Solutions
<p><b>DS9 –Manage the configuration</b>                      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"> <li>▪ Magic Desktop Automation</li> <li>▪ Magic Change Management</li> </ul>

Table 5: Solutions that map to asset management control objectives

**Strong Controls Bring Benefits Beyond Compliance**

Magic IT Service Support 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 Magic, 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. Magic products 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. Magic 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 Magic IT Service Support, may offer a more compelling cost-benefit equation than manual processes and controls.

Companies can use Magic products to automate controls that support Sarbox compliance. These products can improve general IT controls and increase the efficiency of the ongoing compliance process. Furthermore, Magic IT Service Support 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.remedy.com/magic](http://www.remedy.com/magic).

## Appendix: Product Overviews

Product	Overview
Magic Desktop Automation Suite	<ul style="list-style-type: none"> <li>▪ Offers a complete solution that tracks and manages enterprise assets, their configurations and standard configurations in configuration/asset database</li> <li>▪ Ensures that software meets configuration and software-licensing requirements</li> </ul>
Magic Change Management	<ul style="list-style-type: none"> <li>▪ Provides a single consolidated change management system that automates planning and managing all application and system change requests</li> <li>▪ Ensures that all application and infrastructure change requests follow standard documented procedures and change</li> <li>▪ Provides a comprehensive integrated solution that enables discovery of software assets and management of standard configurations</li> <li>▪ Monitors software licenses, and provides patch management and virus detection system; forces virus definition updates based on standard configurations</li> </ul>
Magic Service Desk Suite – Management Center Console	<ul style="list-style-type: none"> <li>▪ Provides a monitoring solution that presents key metrics from Magic applications graphically, dynamically and in real time</li> <li>▪ Offers visual alerts that conditions are outside of acceptable ranges</li> </ul>
Magic Service Desk	<ul style="list-style-type: none"> <li>▪ Provides a comprehensive IT service management solution that supports integrated ITIL incident and problem management processes</li> <li>▪ Provides automatic escalations through built-in workflows, while incident and problem tickets create a complete audit trail of steps taken, approvals, and resolution</li> <li>▪ Offers a complete IT service level agreement solution</li> <li>▪ Defines and manages service level agreements between business users and internal or outsourced IT service providers</li> <li>▪ Offers solutions that allow users to define service level agreements (SLAs) and then measure, manage, monitor and report on SLA status to ensure proactive service level management</li> <li>▪ Includes SLAs relating to system response time, system availability and other service and support functions</li> </ul>
P-Synch	<ul style="list-style-type: none"> <li>▪ Eliminates security issues that arise from ineffective password management</li> <li>▪ Maintains a record in Magic Service Desk every time a user resets his/her password</li> </ul>

## 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 Remedy

Remedy 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 mid-sized businesses to global enterprises, have chosen Remedy's IT Service Management and Customer Service and Support software to automate their support processes, improve service levels, manage assets, and lower costs. As part of BMC Software, Remedy's highly flexible, best-practice applications enable enterprise-wide Business Service Management, and allow customers to easily adapt to unique and changing requirements. Learn more at [www.remedy.com](http://www.remedy.com).

### 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](http://www.bmc.com).



1030 West Maude Avenue  
Sunnyvale, CA 94085 USA

#### Contact the Magic Team

Tel: 800.96.MAGIC / 800.966.2442  
[www.magicsolutions.com](http://www.magicsolutions.com)