



## Obian Mitiware: The “Must-Have” Application for CIOs Signing Off on Section 404 Compliance

### Why CIOs Need Obian Mitiware NOW!

Information Technology (IT) departments are facing ever tightening deadlines to demonstrate compliance with Section 404, *Management Assessment of Internal Controls*, of the Sarbanes-Oxley Act (SOX). To meet this legal requirement, wise CIOs of public corporations will provide evidence to their CEO, CFO, Board of Directors’ Audit Committee and External Auditor that their IT operations meet the judicious internal control standards described in the report, *IT Control Objectives for Sarbanes-Oxley*, May 12, 2004, jointly published by the IT Governance Institute and Information Systems Audit and Control Association (ISACA). Time is of the essence – CEOs and CFOs of public US corporations with over \$75 million in market capitalization whose fiscal year ends on or after November 15, 2004, must sign off on the assessment of their internal controls in their SEC filings.

Non-compliance, a missed deadline, or a material weakness reported in the assessment will certainly and significantly harm a company’s shareholder value, executives’ careers, and business relationships.

CIOs must professionally manage their organizations’ internal controls compliance and assessment effort to avoid such costly damage. It is their responsibility to fix any deficiencies in their internal controls in order that their external auditor can report that the corporation’s internal controls are effective. This will not be an easy task – the authors of the May 12th report believe that there will be deficiencies in the current design, documentation, risk assessment, control activities, and testing of internal controls that must be remediated in almost every IT organization.

The effort to effectively document IT internal control processes to the satisfaction of an external auditor within the time allowed is a daunting challenge for even the most capable CIO. To compound the management challenge of sheer quantity of work that must be performed, IT control assessment is not the type of effort that most IT professionals are either trained to do or like performing. And 2004 will be the first time they will be given the mandate to carry out this annually required IT internal control assessment process.

The hard questions CIOs must ask themselves, “Am I ready for this challenge? Am I truly confident that our IT organization has both the internal controls and internal control assessment process in place that I would be comfortable testifying about to a SEC regulator and about which I could defend against pointed criticism?” For CIOs relying on process-only tools – email with attachments, Excel spreadsheets summarizing tasks and status, workflow, groupware, and project management – the answer should be, “No.” These already existing process tools do not allow CIOs to be as proactively involved with the internal control document content creation and review as SOX requires. Obian Mitiware uniquely allows CIOs to manage processes and people while concurrently documenting their Section 404 internal control assessment efforts.

Obian Mitiware has been designed to meet the directives for Section 404 compliance as described in the IT Control Objectives for Sarbanes-Oxley report. Obian Mitiware will immediately provide CIOs with a framework, enterprise initiative management, and document management system that conforms to the requirements of the report while allowing the implementation flexibility to meet any corporation’s unique requirements. The same processes that are used to review internal controls can also be used to remediate any deficiencies that are uncovered. And because Obian Mitiware creates repeatable processes, including decision-making sign-offs, the IT organization will be able to get a running start on next year’s assessment based upon the previous year’s effort without losing the interrelated processes and content.

## **The Sarbanes-Oxley Act and Regulatory IT Compliance Issues for IT**

In 2002 and 2003, IT executives largely viewed SOX compliance as the sole responsibility of the Finance organization. But that attitude abruptly changed on March 9, 2004 when the SOX-created Public Company Accounting Oversight Board (part of the U.S. Securities and Exchange Commission) issued [PCAOB Auditing Standard No. 2](#). This Standard requires IT departments within public corporations to demonstrate that they have in place adequate and documented internal controls as well as an adequate framework to conduct the required assessment of their internal controls. Furthermore, the external auditor is directed to assess significant changes in the design or operation of internal controls each quarter and the effectiveness of all internal controls annually.

While the SEC relied extensively on COSO's (Committee of Sponsoring Organizations of the Treadway Commission, [www.coso.org](http://www.coso.org)) Internal Controls-Integrated Framework reports for guidance in establishing internal financial reporting controls to meet the compliance requirements of SOX Section 302, Responsibility for Financial Reports, this report was considered inadequate from an IT perspective for setting guidelines for achieving Section 404 compliance. As a result, CobiT, published by the IT Governance Institute ([www.itgi.org](http://www.itgi.org)), has become the basis for IT Section 404 compliance. The IT Governance Institute's final report, *IT Control Objectives for Sarbanes-Oxley*, placed on the Web on May 12, 2004, and developed with contributions by numerous organizations, including the Big 4 accounting firms, establishes the framework most corporations will rely upon for guidance in achieving Section 404 compliance. While this document does not have the force of law, prudent CIOs will treat it that way.

## Section 404 Compliance Requirements

Deciding how a corporation should achieve the objectives of *The IT Control Objectives for Sarbanes-Oxley* report will differ among corporate executives and professional service firms. However, many aspects of the report are very straightforward and will be subject to limited interpretation. Appendices B and C are particularly informative.

*Appendix B – Company-level Questionnaire* clearly lists COSO-established management process issues – Control Environment, Risk Assessment, Information and Communication, and Monitoring – that CIOs must have in place to avoid deficiencies in their internal control systems.

*Appendix C* lists 12 IT General Control activities for which there must be documented control objectives in place. These are:

1. Acquire or Develop Application Software
2. Acquire Technology Infrastructure
3. Develop and Maintain Policies and Procedures
4. Install and Test Application Software and Technology Infrastructure
5. IT General Controls – Manage Changes
6. Define and Manage Service Levels
7. Manage Third-party Services
8. Ensure Systems Security
9. Manage the Configuration

10. Manage Problems and Incidents
11. Manage Data
12. Manage Operations

In addition, the report also calls for the verification and documentation of internal controls for each significant business process and the applications that support them as also described in Section C. This effort requires: 1) documenting each business process and the risks associated with it; 2) stating the control objectives; 3) describing the control activities; 4) describing the approach to confirm (test) the existence and operational effectiveness of the control activities; and 5) testing the effectiveness of the controls. For many corporations, this requirement alone will require the execution of hundreds of time-consuming projects and creation of thousands of documents.

The report also describes 6 stages in its control maturity model and states that to meet Section 404 compliance an organization must be at least at Stage 3 – Defined Processes. The characteristics of a Stage 3 control quality process include:

- Controls and related policies and procedures are in place and adequately documented;
- An event and disclosure process is in place and adequately documented;
- Employees are aware of their responsibility for control activities;
- The operating effectiveness of control activities is evaluated on a periodic basis – however, the process is not fully documented;
- Control deficiencies are identified and remedied in a timely manner.

## **Obian Mitiware Manages Section 404 Compliance and Maintains the Content**

Obian Mitiware is the solution CIOs must have to manage both the processes and documents required to meet the IT control objectives for Sarbanes-Oxley. Obian Mitiware is a unique combination of enterprise initiative management and document management. It allows CIOs to establish the assessment initiatives they need and then monitor and direct decision-making compliance efforts.

Obian Mitiware comes pre-configured with the following initiatives as defined by the IT Governance Institute report:

1. Section 404 IT Compliance Planning
2. IT Control Environment
3. IT Risk Assessment
4. IT Information and Communication
5. Monitoring

6. Acquire or Develop Application Software
7. Acquire Technology Infrastructure
8. Develop and Maintain Policies and Procedures
9. Install and Test Application Software and Technology Infrastructure
10. IT General Controls – Manage Changes
11. Define and Manage Service Levels
12. Manage Third-party Services
13. Ensure Systems Security
14. Manage the Configuration
15. Manage Problems and Incidents
16. Manage Data
17. Manage Operations
18. Business Process Application Controls initiative *Template* that can be duplicated and customized for business process – such as sales, revenue to cash, purchasing, payroll, inventory, asset management, human resource – which the IT organization supports

Obian Mitiware encapsulates best practices for enterprise initiative management and document control. To do so, Obian Mitiware is role based. Individuals have privileges within the system based upon their roles.

Each initiative must have a project leader and executive sponsor, generally the CIO, who will be provided with regular status reports. In addition, it can have document reviewers and content experts who contribute their expert knowledge. All issues that must be resolved within initiatives must have a decision maker and may have a formal decision-making sign-off procedure that can be put in place using company-defined templates. The CIO, CFO, CEO, Controller, Chief Compliance Officer, their Expert Consultants, and Steering Committee members can be given the appropriate roles in order that they can fully and effectively participate in all initiatives, as they deem appropriate. In addition, a role of “anonymous” can be established to allow employees to communicate with management about possible problems for meeting compliance that they may have identified.

Since Obian Mitiware includes an enterprise-class document management system, documents that are checked-out are locked from revisions by others and versions are tracked. In addition, annotations, similar to sticky notes, can be associated with every document to avoid placing comments directly within it. In addition, every major word in MS Word, PDF, HTML, and XML documents entered into Obian Mitiware is indexed and searchable using the integrated free

text research facility. Documentation of all assessment efforts will be maintained and accessible to authorized executives, a major benefit for those charged with updating internal controls to reflect changes in business processes, applications, and IT operations.

To achieve Section 404 compliance in time, CIOs must lead and monitor the status of hundreds of interdependent, ongoing tasks under an assessment framework that defines individual participant's roles and responsibilities; structured, decision-making processes; content creation; and sequential, deadline-driven sign offs. The multiple components of each assessment compliance initiative are inextricably interrelated. Only Obian Mitiware provides the capabilities CIOs need today to manage their organizations' assessment efforts and meet their Section 404 corporate governance responsibilities.

## Obian Mitiware Is Ready for You!

Obian Mitiware is a 100% J2EE application designed for supporting a global enterprise from one installation location. With the time deadlines imposed by current SOX regulations, CIOs will greatly appreciate the ability to quickly implement and deploy Obian Mitiware with its powerful application services. These include:

- **Security:** Obian Mitiware has extensive built-in security features. A CIO can decide who will participate in which initiatives and what privileges each should have. Access control lists can be established to restrict who sees which processes and documents. All information is stored in a single, central repository that is maintained and backed-up by the IT department.
- **Fast Deployment:** Obian Mitiware will be installed in your data center in hours. It can quickly be populated with authorized users using your existing LDAP server. Named users merely need the correct URL and their password to begin working immediately – no Obian Mitiware-specific client software is required to be installed on their PCs, only MS Internet Explorer 6.0 or higher. In addition, the Obian Mitiware server license includes QuickStart support that includes one day of training and two days of initiative deployment assistance.
- **Intuitive to Use:** Obian Mitiware was designed and tested from the premise that anybody who uses email should be able to intuitively participate in an Obian Mitiware initiative. Even senior business executives can use Obian Mitiware and fully participate in compliance processes.

- **Flexible Customization:** Your organization's unique terminology, decision-making process flows, content templates, security access rules, user roles and privileges can all be quickly implemented to meet your specific needs.
- **Scalable:** Obian Mitiware is 100% J2EE compliant and built on a multi-tier architecture. It can easily manage tens of millions of documents and support thousands of online users from one central installation.

## Contact Obian Today for an Online Demonstration

CIOs have a limited amount of time to demonstrate that their organizations meet the requirements for SOX Section 404 compliance. Therefore, Obian is prepared to promptly schedule a personal online demonstration of how Obian Mitiware can help you manage both the content and the processes required. Just [click here](#) and email us your name and phone number to arrange an in-depth briefing. We will demonstrate in detail how Obian Mitiware will provide you with the assurance to sign off on your IT department's compliance with the Sarbanes-Oxley Act. We are confident that you will quickly agree Obian Mitiware does everything we say it does – and more!