

After Year One - Systematizing IT Controls for Sarbanes-Oxley Compliance

An MKS White Paper

Introduction

Not since the securities acts of the 1930s following the 1929 market crash has there been legislation with a level of impact as significant as The Sarbanes-Oxley Act. Today, IT organizations in publicly listed companies race against deadlines to implement effective IT controls as a central part of their company's overall compliance effort. For the most part however, IT organizations have tackled round one of compliance in a manual way – reallocating human and financial resources to the challenge. Audit firms, SOX consultants and CIOs understand that the issue of compliance is not one that will pass with the strike of the New Year's clock, as was the case with Y2K. Compliance is now a part of business life, and CIOs recognize that they need to put in place a system of controls to automate the effort of compliance, get IT projects back on track, and once again, focus their IT organizations on delivering long term value to the business. This white paper explores the issue of IT Controls, one of the significant compliance sticking points, discusses ways in which IT organizations can free themselves from the manual compliance effort, and finally, examines the long term benefits automated compliance can bring to an IT organization.

The Compliance Sticking Point - IT Controls

Section 404 of the Sarbanes-Oxley Act requires management of public companies over \$75 million in market capitalization to prepare and present an annual report on the state of internal controls as they relate to financial reporting. Management must assert to the adequacy of the internal controls, and an independent audit firm must attest to this information. Such information is then disclosed through the filing of a Form 10K and made available to shareholders and the public at large. Management is obligated within this report to disclose any material weaknesses; in other words, elements of the control environment that are not sufficient to prevent or detect material misstatements (of) in the financial statements. To effect its role in this process, the auditing firm in question must follow Auditing Standard No. 2 of the Public Company Accounting Oversight Board, a standard that provides guidance to the audit firm, and requires that the firm ensure that management's assessment is fairly stated and that the company has an effective control environment on the date in which an opinion is rendered. As software and systems are today at the core of business operation, IT controls figure substantially into this auditing effort, and insufficient IT controls can have a serious negative impact on management's assessment of internal controls.

As compliance to Sarbanes-Oxley deadline becomes an ongoing part of life, consultants and auditors are finding that IT controls are a particular area of concern for a number of reasons:

- Companies have not devoted sufficient time to (or quite honestly in some organizations, have ignored) the documentation and testing of IT controls. Until recently auditors themselves documented processes up to the door of IT, and picked up the effort on the other side.
- IT organizations have resisted the compliance effort due to its potential for resource drain, and some organizations do not yet have an appreciation for the severe implications of non-compliance.
- IT organizations have had little in the way of specific guidance on the scope of control required, or have received conflicting guidance resulting in confusion. The COSO framework for corporate governance does not address IT in any detail. COBIT, the control frameworks for IT governance, provides high level guidelines but is found by many organizations to be too broad and lacking in specifics.
- IT organizations have fallen into the historical practice of treating internal auditor concerns with respect to internal control deficiencies lightly and have equated the SOX initiative as "more of the same" that can be ignored without consequence.

As a result, SOX experts all agree, IT controls is a specific area likely to produce 'significant deficiencies' by many companies. This is a serious matter. Significant deficiencies must be reported to the Audit Committee and multiple deficiencies may in fact constitute a material weakness in control. And, under SOX law material weaknesses must be disclosed to investors. The consequences of loss of investor confidence are grave indeed – drop in stock price, decline in company valuation, and damage to the reputation of the CEO and the entire organization.

So how can companies move from a defensive to an offensive position on the matter of IT Controls?

They need to:

Adopt a recognized general IT Controls Framework for Section 404 such as COBIT, or a framework prescribed by a big 4 accounting firm. Second they must look inward, and conduct a self-audit of the state of IT controls in their organization, identifying areas of potential weakness. And finally, they must set about to correct these weaknesses through improved documentation and testing of the controls in place, and remediation in areas where there are gaps.

But still, CIOs and IT managers are faced with the challenge of applying abstract frameworks to their business. As they wade into the compliance effort they are asking themselves, 'are these systems in or out of scope for compliance?', or, 'am I documenting and testing the right process?' and, most importantly, 'what am I missing?'

Key Control Objectives

1. Maintain a complete secure versioning & audit history of software, process, policy, and processes change.
2. Develop a formal systems development methodology.
3. Implement requirements management with user and IT approvals.
4. Ensure maintenance and versioning of project documentation.
5. Define systems requirements.
6. Develop a system acquisition and change approach addressing security risks and data conversion.
7. Ensure separation of development and production activities.
8. Model and automate processes.
9. Engage in rigorous testing including use cases.
10. Control movement of applications by development personnel from test to production.
11. Automate approval process ensuring management review and approval of IT solutions prior to implementation.
12. Construct an implementation review process for system modifications made in an emergency.
13. Enforce formal policies and procedures defining system security.
14. Ensure user account security parameters are in place and enforced.

Beyond the First Year – Recommendations for the Future

It is likely that any IT organization that has survived round one of Sarbanes-Oxley compliance is uttering the phrase "never again." The majority of organizations approached the first round of compliance with little appreciation for the effort required, using manual brute force to meet their SOX obligations. They are now aggressively seeking ways to approach compliance in a more systematized way. One of the most disruptive side effects of Sarbanes-Oxley compliance for CIOs has been the interruption of day-to-day IT business. In a recent survey by accounting firm Ernst & Young, 30% of large companies surveyed reported that effort around SOX compliance was nearly 50% more than originally estimated, and more than half of the large companies (>\$20 million) surveyed indicated they would spend more than 100,000 hours on compliance.

Looking ahead, Section 302 of the legislation demands quarterly compliance, and within its scope includes assessing the impact on internal controls of systems changes and process changes, and requires testing on an ongoing basis.

CIOs of large, complex organizations are also recognizing the need for standardized processes and tools to knit together disparate groups and projects into a common reporting system, and build a sustaining model for compliance. It is nearly impossible for an organization with hundreds of packaged applications and hundreds, even thousands of custom developed software applications to monitor access, change and surrounding processes on an ongoing basis if every project has a different set of tools, a different approach to reporting, and a different way of 'doing things.' The move toward enterprise standardization of process and management tools for the software and application development lifecycle had already begun. The catalyst of compliance will undoubtedly turn this move into a landslide.

Sustaining Compliance

As earlier indicated, Sarbanes-Oxley compliance is an ongoing process, with certification required every quarter. While auditors expect the effort required to produce adequate documentation to be less in following years, there will be a continued need to test and certify controls on an annual basis, and under Section 302, there will be a quarterly reporting of significant change to internal controls spanning change to systems, processes, and people.

So how do organizations build a cost effective and sustainable approach for compliance, and get business back on track? The key will be transitioning away from a manual approach of self-assessment, to employ analytics and continuous monitoring, says Ernst & Young. In the past, IT audits were considered random or point in time occurrences and the risk to business as a result was high. The significant cultural change for IT is to move away from reacting to random audits, to continuous and proactive monitoring of IT controls, which will over time reduce business risk. Automation of the monitoring effort coupled with standardized processes will actually enhance IT productivity as well over time.

Ernst & Young Key Attributes of an Effective Controls Automation Program

- Consistent processes
- Highly automated business processes
- Effective IT general controls
- Tightly defined configurable controls for financially significant processes
- Process owner accountability
- Control self-assessment process

Therefore, over the next 12 to 24 months, audit firms are urging organizations to seek out solutions for continuous controls that include controls automation to reduce manual effort associated with compliance; role management and monitoring to ensure segregation of duties; configuration monitoring for key financial applications, and real time notification via workflow should there be a contravention of established business rules.

Using Maturity Models as a Foundation

Many organizations have reviewed the requirements for SOX have wondered, how in the world they would be able to completely redo their IT departments to accommodate the changes prescribed in the legislation. Some organizations, however, have realized that over the previous few years they had invested thousands of man hours and hundreds of thousands of internal funds building foundations for process improvement, IT efficiencies, and often even other compliance situations. Wise organizations are realizing there is significant parallel between these efforts and the requirements for Sarbanes Oxley. The answers to regulatory compliance may just lie in the use of industry standard Maturity Models.

In the USA, the most common IT maturity model is the Capability Maturity Model (CMM®) or its modern revision called Capability Maturity Model® Integrated (CMMISM). These are part of Carnegie Mellon's Software Engineering Institute (SEI) and focus on process improvements surrounding the various development and delivery life cycles IT departments follow for everyday business needs. Key focus areas include requirements management, project management, tracking and metric activities, quality assurance needs, and configuration management. Many of these same areas of concentration are required for SOX compliance as well, so companies who have previously focused on improvement projects in these disciplines found themselves far ahead of the game for complying with SOX.

Other models such as ISO for standards across software organizations, or COBIT, which analyzes 34 software organization control objectives, along with ITIL (Information Technology Infrastructure Library), a model popular in Europe, but gaining rapid acceptance in North America, have also helped organizations establish a foothold for compliance. So does it mean that companies cannot fully be compliant without one of these models? Not at all! But imagine the edge for today and for future compliance needs when organizations have established and maintained the disciplines surrounding any of these models on a daily basis.

Many organizations are taking the time while they have a funded regulatory need like SOX to complete or advance existing maturity models. It is definitely an enhancement to the overall workings of an IT group to have the processes and disciplines for the maturity models tied in with the processes specific to the compliance needs, and have all of these complimented with an enterprise change and process management solution to measure and control the successes they will realize.

***"We don't have a budget for SOX, or extra headcount. Compliance has added a significant workload on top of our regular day to day duties."
- IT control and security manager for a major manufacturing company***

Is There a Silver Lining?

While the manual effort IT organizations are currently undertaking to ensure compliance appears to offer little reward, CIOs who have accepted that compliance is a way of life and who are seeking to automate control see significant business value in the undertaking. Few senior IT managers will argue with the need for more formalized process around the development and maintenance of mission-critical software systems. However, the effort to build more formal processes and procedures has been hampered in the past by a lack of executive support; 'CMM? What does that do for the business?', or by development and operation team resistance. Sarbanes-Oxley has in fact, become the impetus for formalized control and standardized process across the organization. And no longer is process maturity a nice to have, in this new world it is a must have.

In a recent article from InformationWeek entitled "Time is Running Out", writer Tony Kontzer says the following "Even as they curse Sarbanes-Oxley, IT executives say compliance ultimately will help their



companies by creating leaner, more focused business processes.” CIOs are beginning to see that automated IT controls will not only provide them with compliance on an ongoing basis, but more importantly, will formalize – and improve – their process for building, maintaining and changing systems and applications, and provide them with an unprecedented level of visibility across the IT organization.

MKS Enterprise Change Management Solution and Six-Step Delivery Model for Sarbanes-Oxley Compliance Readiness

MKS provides specialized expertise in the area of IT controls, a significant compliance hurdle faced by many organizations.

MKS’s solution for compliance readiness couples enterprise software change management technology with a six-step delivery model, aimed at putting in place systematic and automated IT controls governing change to applications that are material to disclosure in the financial statements in your organization.

MKS can aid companies in meeting their Sarbanes-Oxley obligations, and more importantly, can put in place a systematized approach to compliance, that not only automates the effort of compliance, but provides long-term business benefit through more repeatable and efficient process, and higher levels of development maturity.

MKS’s solution can provide answers the following questions:

- Who has access to core applications tied to revenue?
- What process if any, does a developer follow when making a change? Can that process be circumvented?
- What was the requirement for change in the first place?
- Do we keep an historic record of changes made to revenue generating applications?
- What is my assurance development is not done on production platforms?
- Can I offer evidence of any of this to an auditor?
- How do I get my IT staff out from under the compliance burden and get this business back on track?

MKS and Enterprise Software Change Management

For financial applications and applications tied to revenue generation MKS’s enterprise software change management solution:

- Enables the assessment of the impact of proposed change.
- Ensures only planned software change is deployed to production.
- Enables quick recovery of a system should errors be introduced.
- Ensures outsourcers work on only the critical project at hand and that access to source code and intellectual property is secured at the individual, file, and project levels.
- Supports a variety of processes – relaxed through to rigid.
- Ensures releases and configurations are repeatable, secure and protected.

MKS achieves the above through the through the following technology:

- **Requirements Management** – offering administration of business requirements and traceability of requirements through to development task and line of code change.
- **Process and Workflow Modeling and Automation** - providing automated, repeatable processes, in addition to authorization (including e-signature) and approval cycles for change requests and separation of functions and duties.
- **Software Configuration Management** – enabling versioning, audit history of all artifacts,

versions and configurations.

- **MKS Federated Server™ Architecture for Offshore and Outsourced Team Management** - enabling compliance to related regulations such as SAS70.
- **Build and Deployment** – enabling complete control over deployment of application change to production environments.
- **Management Dashboard** – offering management level visibility and reporting with drill down ability.

MKS's enterprise change management system is supported by a six-step delivery model aimed at establishing software development best practices and a higher level of process maturity coupled with IT controls to provide a solid and automated environment for compliance. MKS's six-step delivery model consists of the following phases:

Phase 1 – Requirements Development

MKS consultants will engage with your organization's IT team to develop a complete and thorough understanding of the compliance demands placed on the IT organization, and the timelines for compliance. Requirements for the project will be scoped and established at this time. This phase may require collaboration between the MKS team, internal auditors, the Sarbanes-Oxley project team, and/or Sarbanes-Oxley consultants.

Phase 2 – Process and Maturity Model Assessment and Gap Analysis

Once clear requirements for the establishment of IT controls are in place, MKS consultants will inventory all applications and related business processes, and engage in an assessment of these processes against standard IT framework guidelines and established best practices for IT controls. Concurrently, the consultant will assess existing company maturity efforts – such as ITIL and CMM. The consultant then will develop a gap analysis to identify areas for specific focus and an ensuing action plan.

Phase 3 – Action & Implementation

With requirements established, and a gap analysis complete, the consultant will work to a mutually accepted implementation plan, which spans software installation and configuration, process definition, refinement, workflow set up, and reports and dashboard set up and configuration. Many organizations utilize tool solutions for various aspects of their operations and the MKS consultant will assist in the integration efforts of the various tools involved in completing the implementation framework.

Phase 4 – Testing and Validation

Working with the company's internal audit team and/or Sarbanes-Oxley consultants, MKS will test all established processes and validate they are indeed, documented and working as required. These processes will include foundation models like CMM or ITIL as well as integration processes with other areas of the organization outside the central IT group. The main focus will be on compliance as it relates to SOX or other internal audit requirements.

Phase 5 – Audit Support

During the duration of an external audit of a company's IT controls, MKS will make available hotline support assistance and provide a consultant onsite to respond to questions specific to change management IT controls and perform system fine-tuning as required. The MKS solution includes templates and checklists both inside and outside the MKS tools themselves.



Phase 6 – Health Check

As companies mature in their IT controls and compliance efforts, they will require routine health checks to ensure processes continue to be tuned to business needs, and operate as documented. Under Section 302 of the Sarbanes-Oxley Act, companies will also be asked to re-test processes impacted by any significant change (people, system) on a quarterly basis. MKS consultants will conduct quarterly health checks to examine and fine tune processes as required, and review their working operations to ensure continued, systematic compliance is achieved.

In Summary

Many companies are now nearing the finish line for year one of Sarbanes-Oxley compliance, however the job is far from done. They likely face a long list of remediation projects, many in the area of IT controls, and CIOs will be actively seeking ways to automate the compliance effort in order to minimize manual effort and get the business of IT back on track.

Above all else, one thing is certain – there is a need for organizations to move beyond manual compliance to ensure that tools and processes put in place to move beyond manual effort to an environment of preventative controls and continuous monitoring. If the effort of systematization encompasses standardizing on a maturity within an accepted framework (CMM, ITIL), and involves implementation of good development best practices, not only will the task of compliance be easier, the resulting solution will be more robust and applicable to the entire organization actually delivering significant business benefit beyond compliance itself.

Structured properly, remediation efforts can result in a positive payback for the organization. Your teams will spend less time on compliance and focus their effort instead on achieving higher levels of productivity and the construction of higher quality applications to solve real business need.

About the Author

Robert J. Dietrich is Chief Financial Officer for MKS, and is responsible for all financial, administrative and legal functions within the company.

Prior to joining MKS, Rob was with Cedara Software Corp. where he served as CFO and Vice President Finance and Administration from September 1997 to June 2001. Mr. Dietrich also gained significant financial and operational experience in a wide variety of roles at Mitel Corporation in Ottawa, including assignments as Vice President Corporate Affairs, General Manager Network Products Division, Vice President Corporate Planning, Corporate Controller and Treasurer.

Rob Dietrich served eight years in the Audit practice of Ernst & Young, and four years in the company's mergers and acquisitions practice. Most recently he joined the Corporate Governance Task Force for the Issues and Policy Advisory Committee, Financial Executives International Canada, where he serves as Chair.