

Self-Service SOX Auditing With S3 Control

The Sarbanes-Oxley Act (SOX), passed by the US Congress in 2002, represents a fundamental shift in corporate governance norms. As corporations come to terms with the implications of SOX to their businesses, one thing is clear: a SOX compliance program is not a one-time project but a sustained effort to gain visibility and accountability into business processes that affect the accuracy of financial reporting. Most IT controls are manual, error-prone and resource intensive. This paper lays out the problem and suggests a radical solution: build a self-service, automated IT control framework in which all the information required to verify compliance is available in a single reporting system, at the click of a button. Solidcore S3 Control has helped a large number of customers do just that, and we explain how we helped them do it.

Complying with Sarbanes-Oxley.

The Sarbanes-Oxley Act (SOX), passed by the US Congress in 2002, represents the most fundamental shift in corporate governance norms for many decades. In particular, section 404 is often talked about as being the core provision of SOX as it deals with executive management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company. It requires management to certify the adequacy and effectiveness of its internal controls and to disclose any material weaknesses found.

The key to a successful compliance program is to recognize the fact that Sarbanes-Oxley (SOX) does not simply require that adequate controls be established – it requires the annual review of the effectiveness of those controls. In other words, achieving compliance is not a one-time event; rather it must be part of an ongoing process that needs to be sustained

over time. Corporations that view the compliance provisions of Section 404 as a burdensome legislative mandate may not be making the necessary investments for a sustained compliance program. Corporations that view compliance as a means to establish and maintain good process through a well defined set of internal controls and the automation of those controls are the ones that will be more likely to have a successful long-term compliance program.

IT Controls Testing and Verification are Largely Manual

The conventional approach to establishing and maintaining IT controls is to exhaustively document IT processes and policies and increase the frequency of review. This approach is costly, inefficient and error-prone. A sustainable compliance program will need to automate the verification and enforcement of IT controls in a manner that causes low

operational overhead and decreases the documentation burden on systems administrators and audit personnel.

The primary issue faced by IT departments in meeting their compliance requirements today lies in the difficulty of controlling IT systems. Most companies have some form of change approval process, whether formally captured in a workflow system, or informally captured via email exchanges. However, there is a gap between the changes documented through the formal process, and actual change activity on infrastructure elements. Consider a situation in which an annual audit is coming up. People on the staff of the CIO know that because of SOX, they will need to convince the auditors with good answers to questions about who modified data when and for what purpose. How can they reconcile every change on a system with its purpose and authorization? How can they demonstrate that their change process was followed, and that every exception to the process is accounted for in a manner satisfactory to the audit team? The typical answer to questions of this sort is to talk about access and change control policies the company has put in place. However, this is not satisfactory without adequate mechanisms verify that the process was followed. We come back to the core issue: there is a gap between change processes and actual changes in the infrastructure. It is this gap, which we call the Change Control Gap, which causes the manual effort in meeting compliance requirements. If organizations could bridge this gap, self-service compliance audits could become a reality.

Requirements for self-service compliance.

Meeting the IT requirements for compliance is an onerous task. The information required to verify IT controls is unavoidably very large, exists in many different forms and is scattered widely across a complex IT infrastructure. Reconciliation across these information sources is a largely manual, tedious, error-prone and expensive process. In general, it is very difficult for the IT personnel to use such scattered information to construct documentation demonstrating the capability to detect policy violations. For example, leaders in SOX compliance practices include large financial services companies in which every fiscal quarter, dozens of people suspend their usual job duties for several

days in order to collect data and create documentation in the “quarterly compliance fire drill.”

In order to get to the automated control framework we discussed earlier, let us examine what the requirements for a self-service control framework would be. The key capability for a self-service control framework is automated and comprehensive documentation tied to the change process. Demonstrating to auditors that adequate IT controls are in place require coming gaining visibility into the change process, establishing accountability for changes, and selectively enforcing limits on how systems may be changed. In other words, a company’s IT controls should, at a minimum, address the following requirements:

Visibility: Provide extensive logging capabilities that track all relevant program and data changes, as well as categorize and report on them in a useful and actionable manner.

Accountability: Reconcile every change with its authorization and purpose to verify that policies have been followed. Report on exceptions to the change process.

Change Policy Enforcement: A mechanism to enforce these policies selectively where appropriate to prevent breaches from occurring.

Automating compliance with S3 Control

Solidcore Systems is the leading provider of real-time change control solutions. Solidcore S3 Control software improves IT service availability and compliance by closing the change control gap between IT service management and the IT infrastructure.

Solidcore S3 Control gives customers the ability to automate the validation of controls, thereby eliminating the expensive, time consuming and error-prone manual processes that consume IT time and resources. Solidcore’s real-time change detection capability along with its automated and highly accurate change reconciliation provides an automated way to validate changes against authorizations. Out of process changes (for example, emergency fixes) are automatically documented and reconciled for easier

auditability. Customers using S3 Control for Sarbanes-Oxley auditing have realized significant benefits both in terms of reduced risk as well as reduced cost. In most cases, the first phase of benefits comes in the form of automating currently manual controls. The second phase of benefits comes from rationalizing and reducing the control set, based on demonstrating to auditors that control capabilities are built into the fabric of the environment.

The Solidcore benefits include:

- Significantly less manual effort required to comply with SOX audits.
- Reduction in frequency of testing due to demonstrable automation.
- Reduction in number of controls due to process enforcement capabilities.
- Reduction in risk due to completeness of coverage.

We have divided these benefits into two phases. The first phase will consist primarily of automating the large number of manual controls currently in the framework. Audit requirements can be demonstrated on-demand with a self service audit portal consisting of the required reporting and documentation. The second phase will consist of reducing the number of controls by demonstrating that the process enforcement capabilities of S3 Control render periodic validation redundant. Determining which controls may be eliminated from the framework will require discussions and approval from a customer's internal and external audit team as well.

To quantify the benefits of this approach, *Figure 1* summarizes this two phased approach to the SOX Control framework, as implemented by an actual customer. The customer expects that in phase 1 the percentage of automated key controls will increase to 67% from 27%. In phase 2, they expect a 36% reduction in the total number of controls required for SOX compliance.

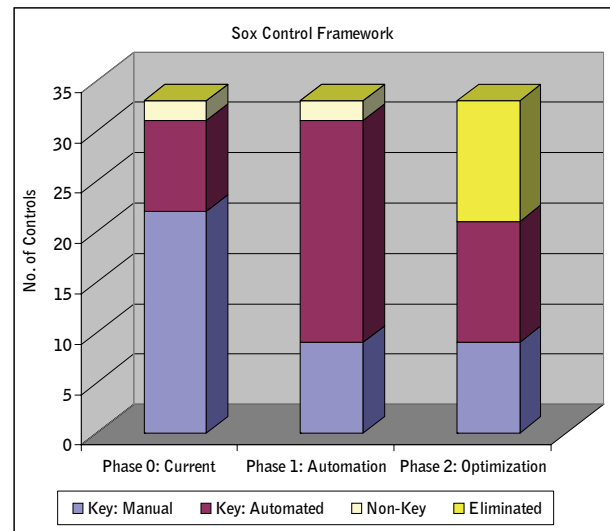


Fig 1: Towards self-service SOX auditing.

The cost savings and risk reduction in moving to this control model are enormous and they expect to recover their investment in less than six months.

What improvements can we make in your SOX Control framework?

Summary

Solidcore S3 Control gives customers the ability to automate the validation of controls, thereby eliminating the expensive, time consuming and error-prone manual processes that consume IT time and resources. Customers using S3 Control for Sarbanes-Oxley auditing have realized significant benefits both in terms of reduced risk as well as reduced cost. In most cases, the first phase of benefits comes in the form of automating currently manual controls. The second phase of benefits comes from rationalizing and reducing the control set, based on demonstrating to auditors that control capabilities are built into the fabric of the environment.

Appendix A: Mapping S3 Control to the Cobit Framework

To map Solidcore capabilities to specific internal controls required by SOX we will use a widely used controls framework, the COBIT framework, which identifies thirty-four specific IT controls that must be satisfied for SOX compliance.

Cobit Requirement	COSO Component					Solidcore Capability
	Control Environment	Risk Assessment	Control	Information	Monitoring	
Plan and Organize (IT Environment)						
IT strategic Planning	●	●		●	●	Gain visibility into change process and create action plan for process improvement.
Information architecture			●	●		
Determine technological direction						
IT organization and relationships	●			●		
Manage the IT investment						Leverage existing IT investments with Solidcore, and connect disparate silos of change information.
Communication of management aims and direction	●			●	●	
Management of human resources	●			●		
Compliance with external requirements				●	●	Monitor policy breaches, produce audit trails and reports to verify compliance.
Assessment of risks		●				Real-time alerts to gain up-to-the-second visibility into changes occurring on production systems.
Manage projects						
Management of quality	●		●	●	●	Maintain systems in a verified state for reduced unplanned downtime.
Acquire and Implement (Program Development and Program Change)						
Identify automated solutions						
Acquire or develop application software			●			
Acquire technology infrastructure			●			
Develop and maintain policies and procedures			●	●		Reconcile deployed changes with actual changes thereby providing verification that policies were followed. Maintain policies by enabling selective enforcement mechanisms.
Install and test application software and technology infrastructure			●			Quicken test cycles by maintaining staging servers and production servers in a consistent state.
Manage changes			●		●	Complete trail of all changes across the enterprise, categorized and reconciled with authorization and purpose.

(table continued on next page)

(table continued from previous page)

Cobit Requirement	COSO Component					Solidcore Capability
	Control Environment	Risk Assessment	Control	Information	Monitoring	
Deliver and Support (Computer Operations and Access to Programs and Data)						
Define and manage service levels	●		●		●	Lower unplanned downtime by maintaining systems in a known and validated state. Meet or exceed SLA's through improved visibility.
Manage third-party services	●	●	●		●	Reconcile third party changes with work orders to ensure consistency and completeness of service.
Manage performance and capacity			●		●	Maintain throughput and computing capacity with a solution that incurs a low CPU and network overhead.
Ensure continuous service						Ensure that production and disaster recovery or backup systems are kept in a consistent state and alert on any deviation.
Ensure systems security			●	●	●	Selectively enforce process and ensure that no changes made outside of approved process may be implemented.
Identify and allocate costs						
Educate and train users	●			●		
Assist and advise customers						
Manage the configuration			●	●		View reports on deviations from a "gold" image and get alerts for changes to configuration.
Manage problems and incidents			●	●	●	Utilize Web-based ad-hoc search tool for forensics and quick remediation.
Manage data			●	●		Protect critical data by preventing unauthorized change to it; report on all changes to a given set of data.
Manage facilities		●				
Manage operations			●	●		Enforce process for a proactive change control stance.
Monitor and Evaluate (IT Environment)						
Monitoring				●	●	Get real-time alerts on any change in the environment.
Adequacy of internal controls					●	Demonstrate adherence to published processes and controls through validation reports.
Independent assurance	●				●	Record changes in a tamper-proof, comprehensive Independent System of Record.
Internal audit					●	Automate reconciliation and verification of approved changes with deployed changes.

Appendix B: Other regulatory standards

Although we focus on the provisions of the Sarbanes-Oxley Act in this white paper, there are other regulatory measures that seek to impose better governance and oversight as well. The table below summarizes a few of these compliance regimes.

HIPAA (Health Insurance Portability and Accountability Act, 1996)

HIPAA established privacy requirements and security standards for protecting the confidentiality and integrity of individually identifiable health information. It governs healthcare information of many kinds, ranging from clinical information to billing.

GLBA (Gramm-Leach-Bliley Act, 1999)

The Gramm-Leach-Bliley Act Safeguards Rule requires financial institutions to prevent unauthorized access to non-public personal information. Financial institutions must take steps to ensure the security and confidentiality of non-public personal information, which includes name, address, social security number and credit history.

CA 1386 (California Senate Bill 1386, 2003)

California enacted legislation that regulates personal financial information over and above the requirements of GLBA. Specifically, this bill requires any firm to disclose to California residents any case of their unencrypted customer data being compromised, regardless of where or how the breach occurred. Because many companies do business in California, CA 1386 is effectively a national regulation, at least within the financial services industry.

Basel II (Basel Capital Accord, 2004)

The Basel Capital Accord (Basel II) updates the international bank capital accord (Basel I) to improve consistency of capital regulations, make regulatory capital more risk sensitive, and to promote risk-management practices among large international banking organizations. Compliance requires all banking institutions to have sufficient assets to offset any risks they may face.

Payment Card Industry (PCI) Data Security Standard

Introduced by Visa, MasterCard, American Express, Discover and other credit card issuers. All processors of credit card information are required to adhere to its twelve requirements which are geared towards protected cardholder information

The Federal Information Security Management Act (FISMA), 2002

FISMA is intended to bolster computer and network security within the Federal Government and affiliated parties by mandating yearly audits. FISMA requires each federal agency to develop, document, and implement an agency-wide information security program for the information and information systems that support the operations and assets of the agency.

About Solidcore Systems

Solidcore Systems is the leading provider of real-time change control solutions. Solidcore S3 Control software improves IT service availability by closing the change control gap between IT service management and the IT infrastructure.

Solidcore's innovative solutions enable comprehensive control of the computing environment of an enterprise. Solidcore's solutions are operationally-friendly, low-touch, and low overhead; they can be deployed on a wide range of enterprise infrastructure including servers, databases and network devices,

Solidcore facilitates real-time visibility and enforcement of control to realize immediate value in change control, compliance and security. Leading Fortune 500 companies and U.S. government organizations use Solidcore to understand and control change. Solidcore is a private, venture-backed enterprise software company with its headquarters in Palo Alto, California.

solidcore®

Solidcore Systems, Inc.
3408 Hillview Avenue, Suite#180
Palo Alto, CA 94304

Email: sales@solidcore.com
Web: <http://www.solidcore.com>
Tel: 888.210.6530