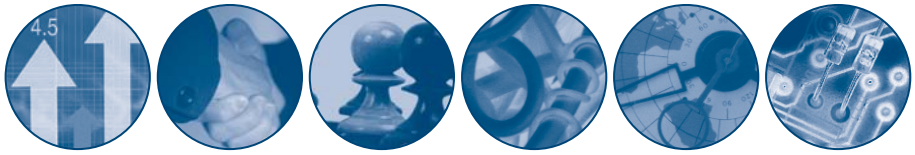

Agile Project Management
Advisory Service
Executive Update
Vol. 5, No. 23

Update

Absorbing Sarbanes-Oxley Within the Agile Community

by Charles W. Butler and Gary L. Richardson

INTRODUCTION

The US Sarbanes-Oxley Act of 2002 (SOX) could potentially rock the IT community. To this point, the IT field has struggled to understand the federal legislation, its government impact, and the risks associated with compliance (or lack of compliance). Accounting improprieties such as those of Enron and WorldCom resulted in heightened legislative initiative and public awareness. Fundamentally, the intent of SOX is to close loopholes in accounting practices that allow fraudulent financial reporting. When control of financial records is inadequate, SOX imposes regulation and defines measurable monetary and nonfinancial penalties for CEOs, CFOs, and other senior executives. As the SOX compliance process has been dissected, there is increasing recognition that the mechanics of the legislation lie within automated enterprise information systems.

SOX identifies internal control as a central objective. In reality, however, industry participants don't define internal control consistently or precisely. In addition, at the time of SOX's drafting, no published standard was available to help fill the gap. To further complicate this definitional process, it should be recognized that SOX legislation was written without the associated series of steps directing a company toward compliance. As a result, the process to achieve compliance is vague. In order to fill the definitional gap, selected national standards bodies are recognized compliance specification sources. The three prominent sources for SOX compliance guidance are the Public Company Accounting Oversight Board (PCAOB), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the Information Systems Audit and Control Association (ISACA) with its Control Objectives for Information and Related Technology (COBIT). When reviewing the content of these bodies, the software development culture is biased toward traditional methodology. The agile community, which represents a contemporary and dynamic approach, is a cultural anomaly with respect to SOX legislation. Agile principles aren't consistent with the traditional compliance specifications outlined by national standards bodies.

The goal of this article is to offer the perspective of agile development, which is significantly affected by the implementation of a SOX-compliant environment. A secondary goal is to identify potential control initiatives associated with agile projects as a result of SOX legislation. The agile community and SOX can coexist, but only with an organized effort to promote acceptable control principles that mitigate SOX regulatory concerns without undermining agile's development principles.

CUTTER CONSORTIUM

SOX REVIEW

The act contains 11 titles and some 69 total sections. Collectively, its contents establish various auditor and corporate control responsibilities plus supplemental rules for financial disclosure. (To review the text of SOX, see www.sarbanes-oxley.com.) The act includes various sections that affect IT, and two are most notable for IT strategic concerns: Section 302 on corporate responsibility for financial reports and Section 404 on management assessment of internal controls. Sections 302 and 404 are prerequisites for initial compliance and are the focus of this discussion. Section 404 is the most burdensome provision of SOX and requires establishment of extensive internal controls. Within each group, the legislative goal is to ensure that the suite of corporate operational processes delivers honest and accurate company financial reporting [2]. Specifically, the high-level requirement for a compliant system is that it handles its data in the following ways [1]:

- **Discovery.** The financial data is retrievable and recoverable.
- **Legibility.** The financial data can be read today and tomorrow.
- **Authenticity.** The financial data's originality can be verified.
- **Auditability.** Third-party review of financial data is provided.

It must be emphasized that compliance with Sections 302 and 404 represents the potential beginning of long-term operational activity.

SECTION 302

Section 302 focuses on effectiveness of disclosure controls and accuracy of the company's quarterly and annual reports [4]. In order to comply, the CEO and the CFO must attest to the following financial reporting statements:

1. The CEO and the CFO, or possibly internal staff, review the reports for compliance with documented standards.
2. Reports contain no untrue statements of material fact.
3. Reports accurately present the company's financial position.
4. The underlying control procedures for financial reports have been reviewed, and compliance is monitored.
5. Any material deficiencies affecting the stated results have been disclosed.
6. Any material changes in internal controls have been disclosed in a timely manner and the statement of corrective actions is documented.

Implicit in this portion of the act is the requirement to thoroughly document, review, and test internal controls related to the financial reporting process. Outside auditors must be able to perform similar oversight of the control structure, which indicates the presence of formal documentation of the installed control process. From an IT perspective, it is important to note that the control process encompasses more than just discrete financial systems. Many base-level systems feed data into the financial domain, so the scope of these controls can run deep in the organization's system portfolio. Because of these ancillary-type interconnections, SOX scope, from an IT perspective, is quite broad.

SECTION 404

Section 404 focuses on the internal control process. From an IT perspective, compliance with this section is complex because Section 404 deals with broad segments of IT activities. Section 404 requires that management provide in the company's annual report an assessment of internal control of financial reporting. One complex dilemma for a company is that this section does not clearly define the level of control needed. SOX is not a one-size-fits-all template, so interpretation is inherent in the compliance process.

NATIONAL STANDARD BODIES AND GUIDANCE

As discussed previously, the internal control is vaguely defined, and at the time of SOX's drafting there was no published standard to fill the gap. However, selected national standards bodies have been identified as compliance specification sources. The three prominent sources — PCAOB, COSO, and COBIT — are summarized briefly below.

- The PCAOB is a board created to provide guidance to the accounting industry. In October 2003, it released guidance and a proposed auditing standard, which was intended to assist in SOX compliance. The auditing standard *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements* addresses both the work that is required to audit internal control of financial reporting and the relationship of this audit to the audit of financial statements [3].
- Originally created in 1985 as an alliance of five professional organizations, COSO established a single voice in the financial business community concerning issues of fraudulent financial reporting. In 1992, COSO produced *Internal Control — Integrated Framework*, which was designed as a US auditing standard [5]. The original report established internal controls as a means of helping companies achieve numerous control objectives and was supported by the US Securities and Exchange Commission. This document became the accepted definitional specification for

evaluating adequacy of internal controls for SOX compliance [3].

- COBIT represents a detailed control framework for IT organizations. Initially released in 1996 by ISACA, the detailed framework was expanded in 1998 with revised control objectives and an implementation toolset. In 2003, the IT Governance Institute (ITGI) sponsored a third edition. The COBIT control definition contains a detailed IT-oriented framework consisting of four major domains, 34 IT processes, and 318 control objectives [3].

AGILE PRINCIPLES AND SOX

In the eyes of the agile community, current IT systems and application development processes may work fine, but this view doesn't equal an adequate compliance statement. Users of agile techniques should evaluate the foundation of internal controls and identify weaknesses and gaps that are directly associated with SOX compliance. SOX requires that controls for applications associated with financial reporting be formalized and documented for external review. This documentation and ongoing review process creates long-term concerns for IT organizations. More specifically, the following seven control capabilities must become part of the IT general and application control environment:

1. All employees must understand the organization's formal internal controls and reporting processes.
2. IT systems must document internal control standards.
3. Operational risks related to the identified systems must be identified.
4. Internal controls must be designed and implemented to mitigate identified risk areas and then monitored for effectiveness.
5. Installed IT controls must be documented and tested.
6. IT controls are updated and changed as necessary to maintain compliance with regulations.
7. IT controls are monitored over time to ensure proper functionality.

These seven guidelines represent an expanding discipline and culture for IT organizations. Clearly, they are a procedural departure for the agile community, which doesn't focus on formalized IT controls or on increased monitoring and updating of those controls. For example, the following agile principles are potentially affected by SOX control requirements:

- **Continuous delivery.** COBIT outlines general controls that guide application system development and maintenance controls. Fluid agile delivery does not cultivate control points identified in general control theory.
- **Collaborative businesspeople and developers.** Application system development controls rely on the principle of separation of function, which is not consistent with agile's colocated team principles.
- **Face-to-face conversation.** Formal documentation is counter to agile's principle of using face-to-face communication to convey information.
- **Sustainable development.** Formal control requirements create hurdles for sponsors, developers, and users who try to maintain a constant development pace. The answer should be found in applying agile practices in conjunction with agile control theory, which satisfies the needs of large systems (typically those associated with financial applications). These agile control practices will likely require event-based documentation practices that are not currently ingrained in the agile community.
- **Self-organizing teams producing architectures, requirements, and designs.** Specific development responsibilities are outlined in general control theory to ensure understanding of control, security, and operational objectives.

INITIAL COMPLIANCE ASSESSMENT

A first quick step in the compliance process for IT is to evaluate the current state of readiness. Table 1 contains a checklist to provide guidance on initial diagnostic focus areas. Each "no" or marginal response to these questions would constitute a further study target area [3]. Any control deficiencies should be reviewed and priority should be established by financial and audit groups. Note that questions 8 through 10 imply a degree of external oversight with regard to agile development projects.

POTENTIAL COMPLIANCE INITIATIVES

Three compliance initiatives are possibilities for the agile community. First, a SOX awareness training component provides training for staff using agile techniques. In order to satisfy SOX requirements, staff must ensure the integrity and confidentiality of information and the authentication and nonrepudiation of its electronic financial transactions. Second, the company's system portfolio is the primary compliance target because the systems codify the rules and procedures of the firm's financial reports. Within the portfolio, systems developed using agile methodologies should be identified for a high-level compliance review. Third, SOX compliance roles can

Table 1 — Sarbanes-Oxley Agile Community Diagnostic Questions

1.	Do agile development groups understand the risks inherent in financial applications and their impact on compliance with Section 404?
2.	For financial applications, do agile development groups understand the financial reporting process and its supporting systems?
3.	Does agile development leadership have advanced knowledge of the types of IT controls necessary to support reliable financial processing?
4.	Are policies governing security, availability, and processing integrity established, documented, and understood by all members of agile development teams?
5.	Do team members understand their roles and responsibilities as related to Section 404?
6.	Do agile team members understand their roles, do they possess the requisite skills to perform their job responsibilities relating to internal control, and are they supported with appropriate skill development?
7.	Has the company integrated an agile team risk assessment process with its overall risk assessment process for financial reporting?
8.	Does the IT department document, evaluate, and remediate IT controls related to financial reporting on an annual basis?
9.	Does the IT department use a formal process to identify and respond to IT control deficiencies?
10.	Is the effectiveness of IT controls monitored and followed up on a regular basis?

be assigned within existing agile teams. The role can be the focal point for policy and guidance for all compliance matters within an agile project, and its primary responsibility is to distribute policy and compliance guidance. Collectively, these three components represent a vital control-related target for agile projects. More specifically the following focus areas must be reviewed:

- **System portfolio.** Most companies' system portfolio and related databases are growing in size and value. To keep these assets vital and effective, companies must continue to invest in them by applying resources to match the effects of business and competitive changes. A company cannot hope to measure SOX compliance if it does not document the breadth and depth of its system portfolio. Two primary tiers should be reviewed to achieve minimal compliance. The first is the financial systems that perform CRUD (create, read, update, and delete) core financial transactions. The second tier involves systems that interface with first-tier systems. For example, a tier-two system might capture an input transaction that is later fed into a tier-one finance system. Alternatively, a tier-two reporting system might use extractions from a core financial system to generate company financial reports. For this class of applications, identify those that were developed using agile techniques and review them for compliance.
- **Awareness training.** After the compliance strategy is determined, a compliance program is formulated to specify the what, why, when, and how for program execution. This program must be deployed throughout the company, and staff must be aware of its content including tactics and timing. Awareness training is a critical vehicle to launch a successful compliance program. Without such training, employees may inadvertently undermine the deployment and operation of internal controls. Since internal controls evolve over time, awareness training should be conducted periodically to update employees on changing strategies.
- **Compliance roles.** While senior management is ultimately accountable for SOX compliance, a compliance manager or a coordinated team of compliance managers should be appointed as operational emissaries. When enforcing compliance requirements for operational financial systems, the compliance role should ensure that input and process data complies with SOX security and integrity guidelines and that access control lists are maintained.

SUMMARY

Sarbanes-Oxley was designed to prevent accounting fraud. While the legislation originated in the US, its principles apply globally. Today, no one knows how many problems the act has generated within US companies. Its impact does not account for potential global implications in business with international operation and alliances. In reality, the global economy could expand SOX impact beyond geographic boundaries. Section 404 requires certification of adequate internal controls, but the language is vague and provides no guidance regarding "adequacy." Since financial systems

are software-based, the internal controls are subject to general and application controls long associated with software development, maintenance, and production execution. Consequently, SOX compliance will extend to the agile community, whose projects involve financial software that affects the accuracy of financial data.

In order to respond positively to SOX compliance requirements, the agile community should take proactive steps consistent with general controls. These steps are not intended to instill the traditional control framework often associated with heavy, burdened overhead. Rather, these steps can be considered "agile control structure" integrated with agile principles:

- Awareness training to empower agile team members
- Self-organizing teams deploying agile control frameworks with agile development techniques
- Sustainable development for targeted tier-one and tier-two applications developed using agile techniques with SOX oversight
- Collaboration and face-to-face communication with risk-based events, along with demonstration and documentation to satisfy control requirements

With the uncertainty associated with compliance initiative, the key questions on senior management's mind are "What might happen if Sarbanes-Oxley requirements are rigorously enforced?" and "What is the regulation's long-term impact?" One scenario is that the perceived control problem declines in the eyes of the various regulator entities and SOX becomes a non-event. Or SOX could be rewritten in a friendlier, concise format. While only time will answer the scoping question, the required IT tactical strategy is to begin dealing with compliance now, and the agile community is not immune to its potential consequences.

REFERENCES

1. Hope, Michele. "Regulatory Compliance and Its Impact on IT." SearchStorage.com, 22 September 2003 (http://searchstorage.techtarget.com/tip/1,289483,sid5_gci928690,00.html).

2. Hope, Michele. "Sarbanes-Oxley Reading List." SearchStorage.com, 15 August 2003 (http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci919566,00.html).

3. ITGI. *IT Control Objectives for Sarbanes-Oxley*, 2003.

4. MKS Inc. "Sarbanes-Oxley and the Need to Audit Your IT Processes." MKS white paper, 2003.

5. Richardson, Gary et al. "Impact of Sarbanes-Oxley on IT." Presentation to the Information Systems Research Council, University of Houston, 19 November 2003.

ABOUT THE AUTHORS

Charles W. Butler *is a Professor in the Department of Computer Information Systems at Colorado State University. Dr. Butler teaches and conducts research in IT and collaborates with IT managers in improving management strategies and processes, software development methodologies, and metrics and QA for traditional and object software. He served in the role of Chief Software Scientist for McCabe & Associates, and completed consulting engagements in more than 50* Fortune *500 companies. His recent consulting engagements have included working with Inovant, a Visa International Solutions Company; Tactical Training Specialists; and the Defense Finance and Accounting Services. He can be reached at Charles.Butler@business.colostate.edu.*

Dr. Gary L. Richardson *currently serves as the coordinator for the graduate-level University of Houston project management certificate program. He has worked in various types of organizations during his 30-plus-year professional career. Early on, Richardson worked for Texas Instruments, the Defense Communications Agency, the US Department of Labor, and the US Air Force. Later, Richardson worked for Texaco and Service Corporation International in CIO-level positions. Mr. Richardson has published four computer-related textbooks and numerous technical articles related to IT. His current research not related to project management focuses on governmental controls and contemporary development techniques. He can be reached at gary.richardson@mail.uh.edu.*

Workshop Developers/ Presenters

Every workshop is led by one of Cutter Consortium s expert Senior Consultants — experienced IT professionals who have honed their skills and developed their methodologies over years in the field at companies like yours.

Verna Allee
Scott Ambler
Robert Austin
James Bach
Kent Beck
E.M. Bennatan
Doug DeCarlo
Tom DeMarco
Jonathan G. Geiger
Michael Guttman
Tushar Hazra
Peter Herzum
Jim Highsmith
Claudia Imhoff
Wendell Jones
Joshua Kerievsky
Tim Lister
Lisa Loftis
David Loshin
Michael Mah
Larissa Moss
Joyce Norris-Montanari
Ken Orr
Ray Pettit
Carl Pritchard
Helen Pukszta
Thomas Redman
Suzanne Robertson
Johanna Rothman
Lou Russell
Michael Schmitz
Ken Schwaber
Rob Thomsett
William Ulrich
Karl Wiig
Ed Yourdon

Cutter Consortium
37 Broadway, Suite 1
Arlington, MA 02474-5552, USA

Tel: +1 781 648 8700
Fax: +1 781 648 1950
Web: www.cutter.com
E-mail: sales@cutter.com

CUTTER CONSORTIUM

Workshops

In these times of intense pressure to make every development dollar and every development minute count, the maxim *you are only as strong as your weakest link* has never rung truer.

Moving your development organization up the productivity curve will improve the ROI of every one of your projects. Just trace this back and you'll discover the ROI in training is immense. And with training and workshops designed and delivered by Cutter Consortium's Senior Consultants, you can add to that equation the peace of mind you get from being trained by the best of the best.

Cutter Consortium offers inhouse training solutions from IT project management techniques to software development methodologies, improving data quality, architecting Web services applications, aligning business and IT objectives and more.

Workshop Topics

- Agile Development Methodologies
- Business-IT Alignment
- Data Quality
- Data Warehousing
- Enterprise Architecture
- Estimation Techniques
- Extreme Programming
- IT Strategic Planning
- Knowledge Management
- Metrics/Benchmarking
- Outsourcing
- Project Management
- Requirements Management
- Risk Management
- Software Development Practices
- Testing
- Web Services

For details about the courses offered in each of these areas, contact Dennis Crowley at +1 781 641 5125 or dcrowley@cutter.com, or visit www.cutter.com/workshops.