Why ISO Embracing Organizations Have a Leg up on SOX Compliance

The target audience of this paper is the reader who is familiar with the concepts of the ISO 9000/14000 family and has an appreciation for the benefits of adhering to a standard. This paper describes how an organization that has learned to leverage and benefit from the ISO family of standards is well positioned to extend this learning to conform to the new Sarbanes Oxley regulations.

Sarbanes and Oxley are two US senators that sponsored new laws, named after themselves, in response to the series of corporate and accounting scandals that began with Enron in 2000. The Sarbanes Oxley Act of 2002, referred to as SOX from hereon, consists of 130 pages. The two most commonly referenced sections are §302 and §404. Each section consists of only a few paragraphs and is followed up by a rather large and detailed definition by the SEC.

§302 states that the CEO and CFO (or the functional equivalents) must sign off on the company financials and misstatements are punishable by imprisonment. Although CFOs have always been required to signoff on financial statements, the new law demands that CEOs signoff as well. §404 states that management must assess the company's internal controls over financial reporting. Accelerated filers have to comply with the new regulations with their year-end reporting for 2004. Due to the limited time available most companies have chosen to use simple databases (e.g. Excel) to comply. Companies have found that these database tools are inadequate for efficient record keeping of SOX related data. We believe companies who follow ISO standards have a twofold advantage; first, the company culture is already adjusted to a carefully monitored approach, and second, database tools are already in place that help document and monitor activities.

Section 404 Implementation Process

§404, *Management Assessment of Internal Controls*, is one of the most challenging aspects of the SOX Act. According to the SEC, the SOX regulatory body, §404 requires publicly traded companies and their external auditors to report quarterly on the design and effectiveness of the company's internal control over financial reporting. This process requires several steps to be implemented, including: definition of a framework to be adopted; documentation of internal controls; testing of internal controls; and evaluation and reporting of internal control deficiencies.

COSO framework

The COSO Internal Control framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission in the early 1990's. This framework, which is one of the SEC accepted frameworks and widely used by US companies, serves as the basis for reporting under §404. Companies are required to have external auditors sign off on their financial statements as well as their control documentation in compliance with §404.

150 Federal Street Suite 2650 Boston, MA 02110 p 617.345.0222 (800-599-7794) www.globalatlanticpartners.com

The COSO Enterprise Risk Management framework that was revised and released in September 2004 is designed to address a broader set of requirements than just SOX, however for the sake of brevity we will not go into detail here. The framework consists of eight interrelated components that enable management to deal with uncertainty, risks, opportunities and capacity to build value for its stakeholders. The eight components are:

1. **Internal Environment** is the COSO term that describes the corporate philosophy of risk management. It sets the basis for how risk is viewed and addressed, how control activities are designed, how information and communication systems operate and how activities and functions are monitored. In other words, the internal environment is the basis for all other components of the COSO framework.
2. **Objective Setting** is the COSO term that describes how an organization goes about setting objectives. This component is also part of a process that helps management ensure that a strategy can be successfully implemented.
3. **Event identification** refers to the process of identifying events that may have positive or negative effects on the achievement of an objective. Positive effects are seen as opportunities, while negative effects represent risks.
4. **Risk assessment** refers to the process of attributing a measure of risk to the negative events that may occur. According to the COSO framework, risks must be assessed from two perspectives, likelihood and impact. Both the likelihood and the impact are further analyzed on an inherent basis (assuming no controls are in place) and on a residual basis (risk that remains after management has put controls in place.)
5. **Risk response** is management's choice of accepting, sharing, reducing or avoiding risks. Management will then focus on building or improving the control environment for those risks that are beyond a tolerable acceptance level.
6. **Control activities** are the controls that management defines in order to help ensure that risk responses are appropriately carried out. Examples of control activities include top-level reviews, physical controls, segregation of duties, and controls over information systems.
7. **Information and communication** describes how information is communicated throughout the organization as well as to and from external parties.
8. **Monitoring** is the process of assessing the aforementioned items in their functioning and presence over time. Monitoring can be performed through ongoing activities, separate evaluations, or both.

150 Federal Street Suite 2650 Boston, MA 02110 p 617.345.0222 (800-599-7794) www.globalatlanticpartners.com

Companies that have already embraced regular periodic self assessments and understand how to respond to these assessments should find the COSO framework familiar and relatively easy to adopt. In particular companies that are effectively engaged with ISO 9000/14000 practices will find that they have already overcome many hurdles and are therefore well positioned to embrace and implement COSO. A number of important improvements introduced during the ISO implementation process can be leveraged and rolled-out to the SOX compliance process. Such improvements include:

1. **Reporting Effectiveness:** Quality conscious companies have the advantage of understanding what and how to effectively report issues from layer-to-layer of management. The similarities between a company that has embraced quality and a risk conscious company are striking. The same fundamental concepts apply whether one is expending valuable resources on quality management or risk management.
2. **Software Tools:** ISO certified companies already have software tools in place to aid employees in tracking and reporting deficiencies as well as strengths. These tools can be easily adapted or expanded to satisfy SOX requirements.
3. **Communication:** Clear communication channels between employees and management, thus creating an environment where corporate goals are clearly understood by everyone.
4. **Documentation:** Documenting processes is a well understood discipline and the corporate culture rewards individuals for this work. (In contrast, organizations that have not developed a documenting culture have a large hurdle to overcome, since this type of work is often viewed as tedious and carries a stigma).
5. **Employee Training:** ISO certified companies already have system in place to define employee training requirements and to track employees' qualifications against these requirements.
6. **Assessment & Mitigation:** Assessment, correction and continuous improvement and the systems that support them are cornerstones of ISO certification.
7. **Management Involvement:** The level of top management's involvement in the process is enhanced by both ISO certification and SOX compliance requirements.
8. **Monitoring:** Continuous monitoring of activities is a SOX requirement and is a concept that ISO embracing organizations already do well and it is engrained in the corporate culture.

Table 1 in the appendix illustrates a few of the natural connections between the ISO 9001 Quality Management Systems Requirements and the COSO framework specification.

Conclusion

Organizations that have worked through and implemented the ISO standards are well on their way to supporting the COSO framework and therefore SOX regulations. The most difficult part about either of these standards is getting people to understand and value the approaches. Further, organizations that have adopted an ISO standard also have software tools in place that can be naturally extended to satisfy SOX requirements. Moreover, much of the data that is already in the system for the ISO implementation can be reused in the SOX process.

150 Federal Street Suite 2650 Boston, MA 02110 p 617.345.0222 (800-599-7794) www.globalatlanticpartners.com

Appendix

ISO #	ISO 9001	COSO category Map	COSO#	Notes
4.1	General Requirements - Quality Management System	All of COSO	All	Similar approaches are used during the preparation of ISO readiness and COSO implementation.
4.2	Documentation	Part of Control Activities	VIII	The ISO discipline of documenting processes and procedures serves as a good cornerstone for COSO's evidence of control.
4.2.2 5.3	Quality Manual; Quality Policy	Internal Environment Statements in Risk Manual / Risk Policy	I	ISO's concepts of quality parallel COSO's concepts of Risk. This is evident by the need for quality manuals and policies vs. risk manuals.
4.2.3 4.2.4	Control of Documents Control of Records	Control Activities	VI	Both ISO and COSO place great emphasis on controls.
5	Management Responsibility	Internal Environment Information and Communication	I VII	Both ISO and COSO stress the importance of having top level management intimately involved in quality/risk analysis.
5.2	Customer Focus	COSO focus on all stakeholders	All	The same emphasis Quality Management gives to customers, Risk Management gives to stakeholders.
5.4 5.4.1	Planning Quality Objectives	Objective Setting	II	Clearly defining quality and risk objectives play a critical role in both standards.
5.5.1	Responsibility and Authority	Internal Environment Information and Communication	I VII	Both standards place great importance on clear ownership and accountability.
5.5.2	Management Representative			This is not explicitly called out under COSO, but a Chief Compliance Officer (CCO) is instrumental in implementing COSO.
5.5.3	Internal Communication	Internal Environment Information and Communication	I VII	Again, both standards place great importance on clear channels of communication.
5.6	Management Review	Monitoring	VIII	To ensure that the planned quality and risk management approaches are working, both standards require careful monitoring.
6	Resource Management;	Internal Environment	I	Quality resource planning emphasizes Human capital and infrastructure, while risk planning also considers negative events and their impacts on the same resources.
6.2.2	Competence, Awareness and Training;	Information and Communication	VII	
6.3	Infrastructure;	Event Identification	III	
6.4	Work Environment	Internal Environment	I	
7.1 7.2.1	Planning of Product Realization; Determination of requirements related to the product	Objective Setting; Event Identification	II III	Both standards focus heavily on extensive planning and fault analysis.
7.2.2	Review of Requirements	Risk Assessment	IV	ISO demands a review of the requirements, while COSO requires risk analysis.
7.2.3	Customer Communication	Information and Communication	VII	In addition to internal communication mentioned earlier, external communication is key to both standards.
7.3 7.3.4 7.3.5 7.3.6	Design & Development Design, Development & Review Design, Development & Verification Design, Development & Validation	Objective Setting; Monitoring	II VII VIII	Under ISO, Design & Development needs to be planned and monitored, while under COSO objectives need to be set and monitored.
8	Measurement Analysis and Improvement	Monitoring	VIII	Measurement/monitoring plays an important role in understanding how an organization is meeting its objectives.

Table 1: Shows a mapping between sections of the ISO 9001 Quality Management Requirements and the COSO Framework.

150 Federal Street Suite 2650 Boston, MA 02110 p 617.345.0222 (800-599-7794) www.globalatlanticpartners.com