



# THREE PRINCIPLES FOR BETTER INTERNAL

A true top-down, risk-based approach to internal control will require integration with overall governance, risk, and compliance activities and the measurement of financial process performance.

## CONTROL OVER FINANCIAL REPORTING

BRUCE MCCUAIG

**N**ew Sarbanes-Oxley Act (SOX) implementation rules proposed in December 2006 by the SEC and the PCAOB are being fiercely resisted. Almost five years since the initial SOX legislation was passed and three years after the adoption of the PCAOB's Auditing Standard No. 2, debate is still raging over a number of fundamental issues.

This far into a regulatory regime, having spent billions of dollars and reported thousands of deficiencies, consensus between regulators, auditors, investors, and public companies should begin to emerge. There should be agreement on how to assess internal control over financial reporting (ICFR), who should do it, what constitutes effective control, and what should be reported.

Instead, based on the public responses to the December 2006 guidance proposed by the SEC and the revisions to Auditing Standard No. 2 proposed by the PCAOB, the most fundamental regulatory issues remain unresolved. No one seems to be blinking and the debate continues.

### The proposed new rules will not solve the problems

Investors, who the initial SOX legislation was presumably designed to protect, are unhappy.

A response from a group led by Barbara Roper, Director of Investor Protection, Consumer Federation of America, stated, "The guidance is so vague as to be unenforceable. The only clear message it sends is that it is intended to drive down costs. As a result, and particularly if the SEC brings that mind-set to its enforcement, managers are likely to be able to claim compliance with the guidelines, and the safe harbor that it provides, for even the shoddiest of internal control assessments."

Moody's, the credit-rating agency, responded to the proposed new auditing standard, lamenting the lack of emphasis on controls over "cooking the books."

In its response, the Institute of Internal Auditors, a founding member of COSO, commented that "making statements about ICFR is not the job of auditors," referring to the continued PCAOB requirement for a separate external audit opinion on ICFR.

The Institute of Management Accountants, another founding member of COSO, observed in its response that the new SEC guidance and the proposed new auditing standard were based on audit risk concepts ver-

---

*BRUCE MCCUAIG, CA, CIA, CCSA, is a principal consultant with Paisley Consulting ([www.paisleyconsulting.com](http://www.paisleyconsulting.com)), a business accountability consultancy and software provider based in Cokato, Minnesota. He can be reached at [bruce.mccuaig@paisleyconsulting.com](mailto:bruce.mccuaig@paisleyconsulting.com).*

... sus globally accepted risk management standards and will lead to massive and unnecessary costs.

... Smaller public companies remain concerned that they bear a disproportionate burden for SOX compliance and that the new rules are not really scalable. They continue to plead for exemption.

... Yet in a speech on March 14, 2007, Chairman Olson said the PCAOB had received 170 comment letters on its proposed Auditing Standard No. 5—over 1,200 pages of comments—and that most are supportive of the proposal, with some recommended improvements.

### What needs to change

... The contentious issue here is not the original SOX legislation. Legislation designed to provide more reliable financial information and better ICFR is not inherently objectionable.

... The source of the debate is the set of rules developed by the SEC and the PCAOB providing guidance for management and standards for company auditors in assessing and forming an opinion on ICFR. By default, the original Auditing Standard No. 2, the standard developed by the PCAOB for auditors, was used by management as the framework for management's mandatory ICFR assessment. Both audit and management costs spiraled upwards.

... Responding to these criticisms, the SEC and the PCAOB, in their proposed December 2006 new guidance and auditing standards, claimed to endorse a top-down, risk-based approach to assessing ICFR that would simplify SOX compliance, drive down costs, and remove some of the most onerous provisions of the original PCAOB Auditing Standard No. 2.

... As many responders pointed out, the proposals fail in whole or in part to meet many of these promises.

... Repairing SOX will require more than tweaking Auditing Standard No. 2 and providing new guidance for management's assessment of ICFR. The underlying paradigms behind the auditing standard and the SEC guidance are fundamentally flawed. Changing the rules does not require legislation. But the SEC and the PCAOB have promised to fast track the release of final

guidance and auditing standards. Fast tracking suggests significant change from the proposed guidance and standards may be unlikely at this point. Without significant change, widespread dissent is likely to continue. Resistance has not abated since the initial implementation rules. It is not likely to decrease without significant change.

### Three principles for repairing SOX

Any fundamental revision of the SOX regulatory regime needs a fresh start based on some clear, simple principles:

1. Balance the quantity and quality of information required on risk and control and balance the use of top-down versus bottom-up approaches in assessing ICFR effectiveness.
2. Improve the reliability of financial processes by measuring and reporting financial process performance as an element of ICFR.
3. Integrate ICFR assessment tools and methodologies with management's overall governance, risk, and compliance activities.

These principles are consistent with and supportive of sound, cost-effective regulation.

#### Balancing risk and control information.

Achieving a better balance of risk versus control information will drive up the quality and quantity of information available to assess the reliability of ICFR and lead to better financial disclosure.

A balanced approach to ICFR evaluation would provide guidance to support far more extensive risk identification and risk assessment, including the identification and categorization of specific current and historic risks to financial reporting in each company, industry, and disclosure, their root causes, indicators of their likelihood, and their significance. This approach would support tracking details of incidents where risk events have occurred.

In short, the quality and quantity of information gathered and analyzed regarding risk and its attributes and characteristics should be balanced with that now gathered and analyzed on controls.

Management guidance and auditing standards should include more information about risk and the attributes of risk.



**LEGISLATION  
DESIGNED TO  
PROVIDE MORE  
RELIABLE  
FINANCIAL  
INFORMATION  
AND BETTER  
ICFR IS NOT  
INHERENTLY  
OBJECTIONABLE.**

## EXHIBIT 1 Characteristics of Top-Down vs. Bottom-Up Risk and Control Frameworks

→ Shifting from Risk Mitigation to Business Improvement →

↑ Shifting from Bottom-Up to Top-Down Orientation ↑

<p style="text-align: center;"><b>Q2—Top-Down Control-Based Characteristics</b></p> <ul style="list-style-type: none"> <li>❑ Focused on control identification and assessment at the organization entity level.</li> <li>❑ Significantly more controls than risks are identified and described (risk:control ratio of 1:3 or greater).</li> <li>❑ Significantly more emphasis on describing important attributes of control (preventive, detective, operating and design effectiveness, automated, manual, primary, secondary, etc.).</li> <li>❑ Internal audit provides assurance on reliability of management control effectiveness assessments.</li> </ul>	<p style="text-align: center;"><b>Q1—Top-Down Risk-Based Characteristics</b></p> <ul style="list-style-type: none"> <li>❑ Focused on identifying and assessing plausible entity-level risks.</li> <li>❑ Typically identifies more risks than controls (risk:control ratio of 3:1 or greater).</li> <li>❑ Significantly more emphasis on identifying important attributes of risk (e.g., source, category, inherent, residual and target significance and likelihood; risk indicators, residual risk status, root cause of failure, etc.).</li> <li>❑ Management is accountable for directing work unit assessments of risk and control.</li> <li>❑ Internal audit provides assurance on reliability of risk and control assessment processes.</li> </ul>
<p style="text-align: center;"><b>Q3—Bottom-Up Control-Based Characteristics</b></p> <ul style="list-style-type: none"> <li>❑ Focused on control identification at the process, system, or transaction level.</li> <li>❑ Gathers extensive information on attributes of controls (preventive, detective, operating and design effectiveness, automated, manual, primary, secondary, etc.).</li> <li>❑ Identifies far more controls than risks (ratio of 5:1 or greater).</li> </ul>	<p style="text-align: center;"><b>Q4—Bottom-Up Risk-Based Characteristics</b></p> <ul style="list-style-type: none"> <li>❑ Focused on risk, incident and cause of failure identification at the process, project or system level.</li> <li>❑ Typically identifies far more risks than controls (ratio of 5:1 or greater).</li> <li>❑ Significant emphasis on identifying all attributes of risk (e.g., inherent, residual and target significance and likelihood; risk indicators, residual risk status, root cause of failure, etc.).</li> <li>❑ Work groups are accountable for assessing and reporting on risk and control.</li> </ul>

This will reduce SOX implementation cost by focusing managements' and auditors' attention on specific risks known to cause financial reporting errors and on the most cost-effective controls proven to be effective in their mitigation.

A close reading of the proposed management guidance and auditing standard suggests that not only are controls emphasized more than risks, but more attribute information is gathered about controls than about risks. For example, inherent risk, residual risk, risk indicators, risk cause, risk models, and risk tables are not mentioned or considered in the proposed amend-

ments. These and other risk attributes are the currency of true risk-based approaches. On the other hand, the SEC guidance seeks to gather such attributes of control as prevention, detection, operating effectiveness, and so forth.

**Focusing on the top.** Increasing the emphasis on top-down approaches and the involvement of management and staff in the assessments will drive down long-term costs and increase sustainability. Top-down assessments will drive down management certification costs, enhance accountability, identify problems earlier, and lead to more resilient solutions to ICFR issues. Man-

**EXHIBIT 2** The Quantity and Quality of Governance, Risk, and Compliance Information

→ **Increasing Governance, Risk, and Compliance Participation of Management vs. Specialists** →

↑ Increasing Quality and Quantity of Reliable Governance, Risk, and Compliance Information ↑

**Q2—Proactive Specialist-Driven Assurance Reporting**

- ❑ Audit or other specialists create reliable assurance data for the business.
- ❑ Focus on residual risk assessment across the entity.
- ❑ Risk-acceptance decisions made by managers and work teams.

**Q1—Proactive Management-Driven Assurance**

- ❑ Work teams create and own residual risk data.
- ❑ Work team data quality is ensured by internal auditors or other specialists.
- ❑ Audit reports on the reliability of management processes.

**Q3—Reactive Specialist-Driven Effectiveness Reporting**

- ❑ Auditor or specialist creates assurance data to support its opinions.
- ❑ Deficiencies and exceptions are subjective.

**Q4—Reactive Management Exception Certification**

- ❑ Management certifies processes as required.
- ❑ Deficiencies and exceptions are defined for management.

agement can focus on company-level assessments and manage ICFR strategically.

Current and proposed SOX rules do not go far enough toward balancing a top-down with a bottom-up approach. They fail to require management to gather sufficient information and draw appropriate conclusions from company-level information.

Exhibit 1 illustrates a framework for assessing top-down vs. bottom-up approaches. The SEC guidance has strong elements of high Q3/low Q2 characteristics.

True top-down approaches would seek to form more and stronger conclusions on the overall health of the organization from entity-level information. The inability to do so should be considered a deficiency in itself. Entity-level assessments would focus on risk and vulnerability but would also focus on company-level controls and culture, specifically on the control environment, monitoring, and risk assessment. More balance is required. Far more guidance is nec-

essary on how to assess, grade, report, and remediate the conclusions that flow from an entity-level assessment.

The root causes of most material SOX deficiencies are discernable at the entity level. More assessment work and stronger conclusions should be required and reported at that level. Governance, risk, and compliance software is capable of providing senior managers with aggregated knowledge about risk and the reliability of controls at every level of the organization.

Shifting more direct accountability for risk and control assessments to work groups supported by quality reviews by internal audit will enhance accountability and improve the quality of information available for ICFR assessment by management. Reliable work group information on risk and control aggregated for management analysis is essential for reliance on entity-level controls. Governance, risk, and compliance software can support this shift.

**Measuring financial process performance.**

Regulations requiring measurement and improvement of financial processes will provide tangible benefits for SOX compliance and link to other governance, risk, and compliance initiatives.

SOX compliance should result in and must not impede business process performance improvement. Good SOX regulations and related auditing standards must recognize strong, reliable financial process performance rather than merely reporting control deficiencies. Whatever the other merits of SOX, businesses will also expect economic benefits. In fact, the huge net cost of SOX compliance is the largest single criticism companies have expressed. Without a linkage to improved financial and other process performance, SOX will not be sustained, or will be sustained only grudgingly and at great expense. SOX regulations and software must embrace and support improved financial process performance reporting and the use of business process improvement tools in order to add value.

SOX rules would be far stronger if they required management analysis and reporting of business process performance in reaching a conclusion on ICFR. A focus on the performance of financial processes would include guidance on setting performance indicators, process performance measurement, event and incident tracking, and process benchmarking within an enterprise and across industry groups.

**Recognizing and promoting the integration of governance, risk, and compliance.** Regulation that recognizes the comprehensive, integrated nature of corporate governance, risk, and compliance will produce more reliable, consistent information and be of significant value to all corporate stakeholders.

Over the long haul, integration of governance, risk, and compliance, including SOX, must involve collaborative and interactive participation of management, specialists, auditors, and work teams to produce rich, detailed, reliable information on ICFR and other governance, risk, and compliance topics and contexts. ICFR assessment tools and technology must support work flow and collaboration across the organization, from its highest reaches to its front lines. The tools and technology must be com-

patible with the goals of integrated governance, risk, and compliance.

Governance, risk, and compliance knowledge must be created by and accessible to managers, professionals, and auditors throughout the organization. It must integrate with other assurance information developed in the organization. The quantity and quality of governance, risk, and compliance information must improve, and the participation by work teams in the SOX process must increase.

Exhibit 2 describes four quadrants differentiated by the quantity and quality of governance, risk, and compliance information and the extent of participation and ownership of management and work teams versus specialists, such as auditors. Over the years, businesses around the world have made substantial progress in improving quality, safety, and environmental compliance by shifting towards a Q1 approach, shifting accountability to work groups as much as possible. To a large degree SOX regulations surrounding ICFR certification and audit have been approached from a Q3 perspective.

The role of internal and external audit is critical in a Q1 approach. Their role is to ensure the quality of management's assurance data and to report on the reliability of management's assessment processes. This is a far more sophisticated and demanding role than now played by most internal or external audit groups but completely consistent with the intended role of a professional internal audit organization in an integrated governance, risk, and compliance environment. Achieving and sustaining the benefits of integrated governance, risk, and compliance require the active, knowledgeable participation of management and professional staff across the organization, supported by internal audit in a quality assurance role.

SOX guidance and related auditing standards should clearly recognize and reward, and must not penalize, the use of accepted, globally recognized standards and terminology for identifying risks and controls as they relate to ICFR and must provide guidance on assessing and reporting ICFR effectiveness that is clear, practical, and

**WITHOUT A LINKAGE TO IMPROVED FINANCIAL AND OTHER PROCESS PERFORMANCE, SOX WILL NOT BE SUSTAINED, OR WILL BE SUSTAINED ONLY GRUDGINGLY AND AT GREAT EXPENSE.**

unambiguous to operating managers and professionals. To do so, they must recognize proven tools and the best practices of management in all governance, risk, and compliance assurance professions, rather than embody practices, concepts, and tools unique to the accounting and auditing worlds.

SOX rules should be broad and flexible enough to be understood and used for the collection and assessment of reliable infor-

mation on risk and control for a variety of purposes and should reflect the input of risk and control experts in other areas of governance, risk, and compliance.

Reliable financial reporting and increased accountability of management is a realistic goal and should be achievable in a cost-effective way. Let's hope SOX regulators, the SEC, and the PCAOB, along with all the stakeholders, have the courage to make or accept the changes that are required. ■