IN SEARCH OF UTOPIA:
What Should An Audit Committee Want from Internal Audit?

prepared for:
Auditor General of Alberta
Oversight of Internal Audit in the Public Sector Forum

prepared by:
Tim Leech, FCA·CIA, CCSA, CFE
Chief Methodology Officer

PAISLEY CONSULTING
Business accountability solutions.

2655 North Sheridan Way, Suite 150
Mississauga, Ontario, Canada, L5K 2P8
Tel: 905 823 5518 Fax: 905 823 5657
Tim.Leech@paisleyconsulting.com
www.paisleyconsulting.com

March 2, 2006

Speaker Profile

Tim J. Leech, FCA·CIA, CCSA, CFE, MBA

Tim J. Leech is Principal Consultant & Chief Methodology Officer with Paisley Consulting, the world's leading provider of integrated business accountability software and training solutions. From 1991 to 2004 Tim was CEO and founder of CARD®*decisions*, a global pioneer in the ERM and CRSA areas. Paisley acquired CARD®*decisions* in June of 2004. Other positions he has had include Managing Director of a subsidiary of the Hambros Bank, Director Control & Risk Management Services with Coopers & Lybrand Consulting, and a range of comptrollership and internal audit roles with Gulf Canada. Tim was elected Fellow of the Institute of Chartered Accountants Ontario in 1997 in recognition of distinguished service to the auditing profession.

Leech's responsibilities include providing design advice on all Paisley software products; consulting and training services related to Sarbanes-Oxley, Basel operational risk management, enterprise-wide risk and assurance management; Collaborative Assurance & Risk Design™ ("CARD®") training and software development; control and risk self-assessment ("CRSA") training and implementation services; specialized litigation support services; business ethics advisory services; internal audit training and consulting; and control/risk governance consulting services. He has provided training for public and private sector staff located in Canada, the U.S., the EU, Australia, South America, Africa and the Middle and Far East. Leech has received worldwide recognition as a pioneer and thought leader in the fields of enterprise risk and assurance management and control and risk self-assessment.

Some of Leech's experiences and achievements include:

- pioneering and developing Collaborative Assurance & Risk Design ("CARD®") an integrated, enterprise-wide risk and assurance management and reporting approach that has been recognized globally as a leading edge corporate governance best practice;
- developing workshops and e-learning training modules on ERM, Sarbanes-Oxley, Basel and Internal Audit skills;
- numerous T.V. appearances, a national radio show, and scores of articles in professional journals on risk management, internal control, business ethics, and fraud related topics;
- authoring technical papers in response to exposure drafts of risk and control governance studies and frameworks in the U.S., the U.K., and Canada including Sarbanes-Oxley regulations and reports by the Treadway Commission, COSO Committee, Cadbury, and CoCo internal control research projects;
- contributing technical material related to CSA/CRSA including the IIA report CSA: Making the Choice and the IIA research study CSA: Experience, Current Thinking and Best Practices;
- co-author of an FEI Research Foundation research study Control Deficiency Reporting: Review and Analysis of Filings During 2004, and a new book published by Risk Books - Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response;
- delivery of expert witness services and testimony during civil and criminal actions related to fraud, secret commissions, conflict of interest, breach of contract, and officer/director due diligence;
- member of the IIA's ERM & CSA Conference Advisory Panel since the conference's inception and author of a practice exam for CSA specialist certification;
- primary author of CARD®*map* software - the world's first Collaborative Assurance and Risk Design™ groupware. At Paisley Tim has responsibility for providing input and advice on the design and features available in all Paisley software and training products including the company's flagship product, Risk Navigator, as well as CARD®*map*, Focus, and Auto Audit;
- served as a board member of the Canadian Centre for Ethics and Corporate Policy, authored a column titled Duty of Care and has written a wide range of articles and made presentations on ethics related issues;
- provides expert opinion responses to SOX questions for Compliance Week's Remediation Center; and
- contributor to articles on Basel II and SOX to the U.K. publication Global Risk Regulator and the National Post in Canada.

PAISLEY CONSULTING

Business accountability solutions.

IN SEARCH OF UTOPIA:
What Should An Audit Committee Want from Internal Audit?

Auditor General of Alberta
Oversight of Internal Audit in the Public Sector Forum

March 2, 2006

PAISLEY CONSULTING

Business accountability solutions.

IN SEARCH OF UTOPIA:
What Should An Audit Committee Want from Internal Audit?

Agenda

- Session Objectives
- Evolution of the Relationship between Audit Committees & Internal Audit
- Current Views on Audit Committee/I.A. Best Practice
- Defining the Relationship – Key Principles

PAISLEY CONSULTING

Business accountability solutions.

IN SEARCH OF UTOPIA:
What Should An Audit Committee Want from Internal Audit?

Agenda

- Defining an Assurance Universe & Clear Expectations
- Deciding What / How / & Why to Audit – Options Available
- Internal Audit in the Public Sector
- Understanding Reporting Options – Traditional & Next Generation

PAISLEY CONSULTING

Business accountability solutions.

IN SEARCH OF UTOPIA:
What Should An Audit Committee Want from Internal Audit?

Agenda

- Understanding Audit Opinions & Options
- The #1 Thing Audit Committees Should Want from Internal Audit
- Questions

PAISLEY CONSULTING

Business accountability solutions.

Session Objectives

Objective #1

Provide an overview of the evolution of the relationship between Audit Committees and Internal Audit

PAISLEY CONSULTING

Business accountability solutions.

Session Objectives

Objective #2

Introduce what "authoritative bodies" are saying about what the relationship and terms of reference should be between Audit Committees and Internal Audit

PAISLEY CONSULTING

Business accountability solutions.

Session Objectives

Objective #3

Provide some personal perspectives based on 25 years of observations, interaction and research on Audit Committee/Internal Audit Relationship Utopia
→ "a place or state of ideal perfection"

Tim The Utopian —
"given to dreams or schemes of such perfection"

(Random House Dictionary of the English Language)

PAISLEY CONSULTING

Business accountability solutions.

The Evolution of the Relationship between Audit Committees & Internal Audit

No relationship — neither party existed

↓

Knew each other enough to say hi

↓

Dated but on an infrequent and somewhat distant basis

↓

PAISLEY CONSULTING

Business accountability solutions.

The Evolution of the Relationship between Audit Committees & Internal Audit

Relationship progressed to a few dates/year but limited intimacy

↓

Closer relationship forced/organized by outside forces

↓

PAISLEY CONSULTING

Business accountability solutions.

The Evolution of the Relationship between Audit Committees & Internal Audit

Relationship generally improving — better in some areas than others. Failure rate of relationships still high

↓

Confusion on roles and relationship status still prevalent on both sides

PAISLEY CONSULTING

Business accountability solutions.

Current Views on Audit Committee / I.A. Best Practice

No shortage of guidance

- CICA – 20 Questions Directors Should Ask About Internal Audit
- AICPA – Internal Audit and the Audit Committee
- IIA – Audit Committees and Governance – Dozens of titles

PAISLEY CONSULTING

Business accountability solutions.

Current Views on Audit Committee / I.A. Best Practice

No shortage of guidance

- Auditor General of Canada (see Attachment 1)
- Alberta Government Proposed Guidance for Audit Committees
- Private sector studies (see Attachment 2)

PAISLEY CONSULTING

Business accountability solutions.

Defining the Relationship – Key Principles

Audit Committee Chair & Chief Audit Executive

- Clear expectations – easier said than done
- Candid full disclosure expected and encouraged
- CAE should see Audit Committee as #1 Client
- Regular and "as required" contact
- Audit Committee should be knowledgeable, demanding, "street smart", and discriminating. Quality not the quantity of questions is key

PAISLEY CONSULTING

Business accountability solutions.

Defining an Assurance Universe & Clear Expectations

- What does the Audit Committee want assurance on? (see example Attachment 7)
- From whom? I.A. only, Mgmt. & I.A., Others? How often?
- With what level of assurance/confidence? – A little or a lot? A lot costs more.

(See Attachment 7)

PAISLEY CONSULTING

Business accountability solutions.

Deciding What / How / & Why to Audit

- In your assigned group from the list of 9 options pick what you think is the best way to utilize limited internal audit resources (Use Attachment 6). You have 10 minutes to discuss and agree.
- Appoint a spokesperson to report your group's choice.

PAISLEY CONSULTING

Business accountability solutions.

Understanding the I.A. Options Available

Historic Approach #1	
Internal Audit audits for compliance with policies, rules or prescribed audit criteria.	
Coverage:	Very limited
Cost:	High for broad coverage
Effectiveness:	High failure rate

PAISLEY CONSULTING

Business accountability solutions.

Understanding the I.A. Options Available

Historic Approach #2	
Internal Audit picks topics/units/subjects, performs audits and reports on whether they think controls are adequate/effective	
Coverage:	Very limited
Cost:	High for broad coverage
Effectiveness:	Creates high friction/disagreement on how much control/what type of control

PAISLEY CONSULTING

Business accountability solutions.

Understanding the I.A. Options Available

Emerging Approach #1	
Reporting on conformance with defined control model criteria (e.g. COSO 1992, CoCo, CARD®*model*, Modern Controllership)	
Coverage:	Extensive
Cost:	Low
Effectiveness:	• Canadian federal public sector experience in its infancy • Private sector adoption very limited to date but growing rapidly • Conceptually valid

(See Attachment 5)

PAISLEY CONSULTING

Business accountability solutions.

Understanding the I.A. Options Available

Emerging Approach #2	
Reporting on the Quality of Risk Management	
Coverage:	Extensive
Cost:	Low to medium
Effectiveness:	• Growing global acceptance in public and private sectors • Accepted as valid by bank regulators worldwide • Required by IIA professional standards

PAISLEY CONSULTING

Business accountability solutions.

Understanding the I.A. Options Available

Emerging Approach #3	
Senior management and business unit self-assessment with a report on reliability of process from internal Audit	
Coverage:	Decided by board/senior management
Cost:	• I.A. cost low • Organization cost medium to high
Effectiveness:	Best technique if unit ownership/ continuous improvement is important

PAISLEY CONSULTING

Business accountability solutions.

Understanding the I.A. Options Available

Emerging Approach #4	
Enterprise-wide risk management. Involves deciding on optimal mix of the 10 primary assurance methods available and coverage (See Attachment 3)	
Coverage:	Extensive
Cost:	High
Effectiveness:	Jury still out

PAISLEY CONSULTING

Business accountability solutions.

Understanding Audit Opinions

- Wide variations in approach
- "Apples to apples" comparisons not possible
- New IIA Guidance on internal audit opinions (Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control)
- Sarbanes-Oxley wants consistent grading of "Material Weaknesses" and Significant Deficiencies
- No public sector requirement for standardized reporting yet

(See Attachment 9)

PAISLEY CONSULTING

Business accountability solutions.

Understanding Audit Opinions

Utopia State —

- Management makes formal declaration to Audit Committee on current quality of risk and control management and residual risk status. A standardized rating system should be used (See Attachment 9)
- Internal Audit provides independent opinion on the quality and reliability of risk and control management processes in place (i.e. grades the quality of risk management) and the current reliability of management's status reports

(See Attachment 8)

PAISLEY CONSULTING

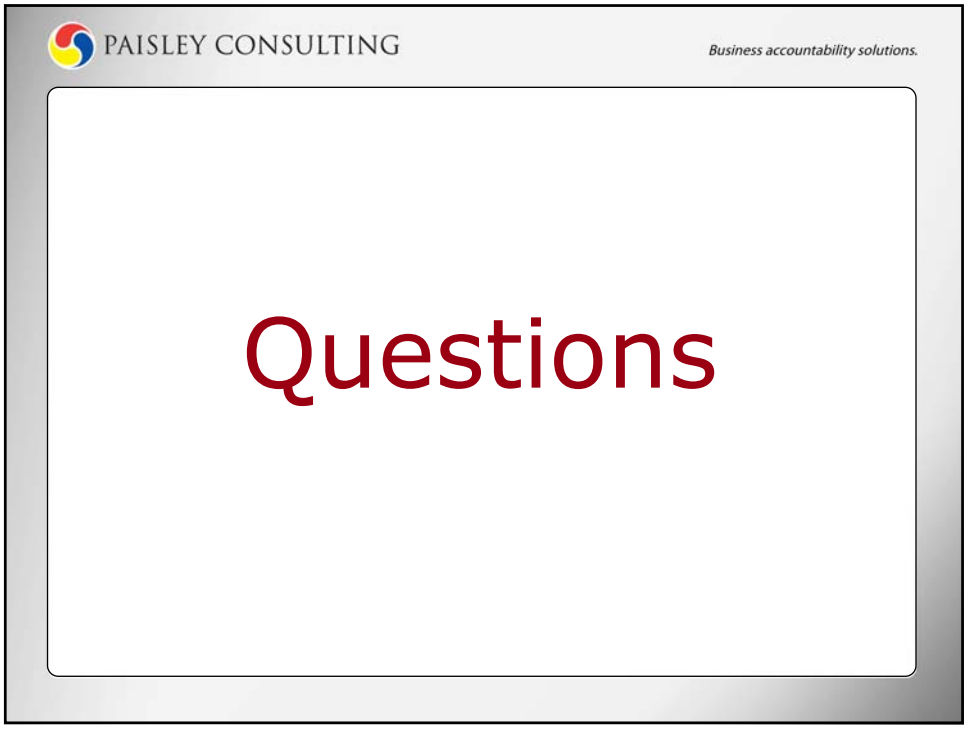
Business accountability solutions.

The #1 Thing Audit Committees Should Want from Internal Audit

Assurance from Internal Audit the Audit Committee is getting materially complete and reliable information on the state of "Residual Risk" for areas of responsibility/ interest/personal liability/potentially damaging to Audit Committee members

and

Candid disclosure from Internal Audit on what isn't being covered and reported on and why it isn't being covered and reported on


PAISLEY CONSULTING
Business accountability solutions.
Questions

IN SEARCH OF UTOPIA:
What Should An Audit Committee Want from Internal Audit?

List of Attachments

Attachment 1

Appendix C — Selected best practices for audit committees

Best practices since 2000 are highlighted in italics

The audit committee should ensure financial oversight by

- critically reviewing the interim and annual financial statements, the auditor's report, and the management discussion and analysis section of the annual report;
- *ensuring that presentation of financial statements is fair, appropriate, and clear, and that it meets generally accepted accounting principles;* and
- actively soliciting the external auditor's judgments about the acceptability and the quality of the corporation's accounting principles as applied in its financial reporting. This discussion should include such issues as the clarity of financial disclosure and the aggressiveness or conservatism of the corporation's accounting principles and estimates.

The audit committee should ensure oversight of corporate books, records, financial and management control and information systems, and management practices by

- reviewing the special examination plan and report prepared by the external examiner;
- actively soliciting information about significant risks and exposures and reviewing the adequacy of internal controls to manage those risks;
- reviewing the integrity and effectiveness of the management information systems;
- reviewing internal audit plans and reports and management's subsequent actions; and
- reviewing significant findings and recommendations made by the external auditor and examiner and following up on management's subsequent actions.

The audit committee should

- ensure ethical oversight through the annual review of management's compliance with the corporate code of conduct;
- actively solicit all sensitive information (for example, senior management expenses, significant litigation, non-compliance with laws and regulations, misuse of corporate assets, illegal activities);
- *oversee the resolution and investigation of complaints of wrongdoing (audit committee mandates should include the requirement for a process to investigate and resolve all complaints, including those made anonymously);*
- *ensure that internal audit is adequately resourced and that it has adequately covered the major risks and activities of the corporation; and*

7.2—Telefilm Canada—Most of its activities are not consistent with its constituting legislation

7.3—A process used to clarify expectations between the government and a Crown corporation

7.4—Values and ethics for public office holders—key principles

- *recommend external auditors and their compensation, and pre-approve all non-audit services by external auditors to ensure that their objectivity and independence are preserved.*

Membership and competencies

- *Audit committees should be composed of at least three members. Each member should be an independent director, who should not be an officer or an employee of the corporation.*
- Although a variety of skills and experience is beneficial to an effective and balanced audit committee, all members should be financially literate and at least one member should have accounting or related financial management expertise. Financial "literacy" signifies the ability to read and understand fundamental financial statements, including a balance sheet, income statement and cash flow statement, and the ability to ask probing questions about the corporation's financial risks and accounting. "Expertise" signifies past employment experience in finance or accounting, requisite professional certification in accounting, or any other comparable experience or background that results in the individual's financial sophistication (experience as a chief executive officer, for example, or other senior officer with financial oversight responsibilities).

Operating procedures

Terms of reference. Audit committees should have clear, written terms of reference and operating procedures that specify the scope of the committee's responsibilities and how it carries them out, including its structure, processes, and membership requirements.

Meetings. The frequency of audit committee meetings should be tailored to the responsibilities assigned, but should be at least quarterly. The audit committee should also meet periodically with management, the external auditor, and the head of internal audit, in separate private sessions.

Disclosure requirements

Audit committees should publicly disclose their charter, composition, recommendations not adopted by the board, and nature and amounts of auditor's fees, in audit and non-audit services.

Last Updated: 2005-02-15 Important Notices

Attachment 2

The CPA Journal

Print

Audit Committee Responsibilities

Focusing on Oversight, Open Communication, and Best Practices

By Annemarie K. Keinath and Judith C. Walo

The SEC first recommended that publicly held companies establish audit committees in 1972. The stock exchanges quickly followed by either requiring or recommending that companies establish audit committees. Over the years, various initiatives to strengthen and increase the responsibilities of audit committees have been made.

In 1987, the National Commission on Fraudulent Financial Reporting (the Treadway Commission) investigated ways to detect and prevent fraudulent financial reporting. The Treadway Commission made six specific audit committee recommendations aimed at deterring fraudulent financial reporting.

In 1999, the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (BRC) made 10 recommendations for improving audit committees' effectiveness. BRC also provided five broad guiding principles for audit committees to follow in devising company-specific policies. The BRC recommendations resulted in changes by NASDAQ, the NYSE, AMEX, and the SEC.

In 2002, the Sarbanes-Oxley Act increased audit committees' responsibilities and authority, and raised membership requirements and committee composition to include more independent directors. In response, the SEC and the stock exchanges proposed new regulations and rules to strengthen audit committees.

Audit Committee Best Practices

The authors obtained proxies for the 98 domestic companies in the NASDAQ 100 as of August 2002, most of which are in the technology, pharmaceutical, and communications industries. The audit committee charters in the sample were filed before the passage of Sarbanes-Oxley. The authors examined all other areas of the proxies where responsibilities of the audit committee could potentially be reported, and included these disclosures in our evidence.

Rules, regulations, and recommendations have been made to strengthen audit committee composition and authority, to increase audit committee responsibilities, and to improve the audit committee's monitoring role.

Exhibit 1 presents audit committee requirements specified by Sarbanes-Oxley. Exhibit 2 presents disclosures required by the SEC in the audit committee report filed in the annual proxy. Exhibit 3 presents preexisting and proposed NASDAQ rules beyond those in Exhibits 1 and 2. Additional responsibilities not required for NASDAQ companies are included as best practices in Exhibit 4. These additional items cover recommendations by the BRC and Treadway Commission, along with current or proposed regulations of AMEX and the NYSE. Exhibit 5 presents the compilation of best practices, organized into seven general categories, and a comparison of best practices to disclosures of actual audit committee practices.

Analysis

Exhibit 5 presents the percentage of NASDAQ 100 companies asserting responsibility for each item on the best practices list. The results show that audit committees have to significantly expand their responsibilities to just cover practices required by Sarbanes-Oxley and NASDAQ. In addition, if audit committees are to be proactive and effective, they should voluntarily expand their responsibilities to include all best practices, including those not required.

Oversee the financial reporting process. Annual and quarterly financial statements are the primary means for reporting the financial condition and operating performance to stockholders. The BRC recommended that the audit committee review these financial statements with management and the external auditors. The NYSE proposal requires that the audit committee review Management's Discussion and Analysis (MD&A), the company's earnings press releases, and earnings guidance provided to analysts.

All of the companies reported that their audit committees are responsible for reviewing annual financial statements, and 95% reported that they discuss these statements with management and auditors. Only 84% of the committees or committee chairs reviewed quarterly statements, however, and only 68% discussed these statements with management and external auditors. The SEC requires that audit committees discuss annual reports with management and disclose this discussion in the audit committee report. Although neither current nor proposed NASDAQ rules specifically address this issue, audit committees not discussing quarterly statements with management and auditors are clearly not being proactive.

As for the remaining items relating to the financial reporting process, results show a need for major improvement. Only 8% of the audit committees reviewed the MD&A, and only 1% discussed it with management and auditors. Earnings press releases were reviewed by only 14%, and none reviewed earnings guidance provided to analysts and rating agencies.

Although review and discussion of the MD&A, earnings press releases, and earnings guidance is not required of NASDAQ companies, audit committees should monitor all financial information communicated to the public to ensure that investors are not receiving misleading information. The NYSE proposal includes these reviews as audit committee requirements, and it urges audit committees to pay particular attention to earnings releases using "pro forma" or "adjusted non-GAAP" information. The SEC has expressed concern that pro forma disclosures do not necessarily "convey a true and accurate picture of a company's financial well-being." Under the direction of the Sarbanes-Oxley Act, the SEC has approved rules requiring that pro forma results be reconciled to GAAP numbers. Audit committees should ensure that the earnings releases are not in violation of SEC requirements. The fact that so few audit committees reported reviewing earnings press releases suggests that NASDAQ audit committees need to assume much broader responsibility.

Monitor choice of accounting policies and principles. The choice of accounting principles significantly affects the financial statements. The Sarbanes-Oxley Act requires that the audit committee receive a report from the auditor about the principles used and the effects of alternative choices on the financial statements. The NYSE proposal requires that the audit committee review with management and the external auditor the effects of estimates or judgment on financial reporting.

Only 63% of the audit committees in the sample disclosed that they were responsible for monitoring the choice of accounting policies and principles. Only 54% specifically indicated that they review the quality of accounting principles with their auditors. The number of audit committees that actually review quality may be greater than this, because the discussion of the quality of accounting principles is a current requirement under GAAS. Discussion of principles will be expanded under Sarbanes-Oxley to include alternative principles, the ramifications of principles used, and the auditor's preferred principle.

It is preferable that the charter explicitly state the responsibilities required by GAAS. Audit committees not acknowledging responsibility for discussing matters required by GAAS nor explicitly stating their responsibilities on critical duties such as the choice of accounting principles may be too passive in their oversight. They might leave it to the auditors to determine what the committee should know, rather than taking an active role by asking probing questions and ensuring that all items of importance are discussed.

Monitor internal control process. The audit committee's role is to ensure that management has developed and followed an adequate system of internal control. The seven best practices discussed below are important factors relating to internal control. None of these functions are currently required for NASDAQ companies, although the last two items are part of NASDAQ's proposed changes. All seven are recommended or required as a best practice by at

least one authoritative source.

Almost all audit committees asserted responsibility for monitoring the system of internal control. Oversight of the system of internal control was an audit committee best practice in the BRC report. The Sarbanes-Oxley Act elevated internal control to such importance that it requires an annual internal control report by management, including a statement about the effectiveness of the internal controls over the company's financial reporting. In 2003, the SEC approved a rule to implement this requirement.

Monitoring compliance with legal and regulatory requirements is part of the NYSE proposal. Only 60% of the audit committees in this study acknowledged responsibility for this area, a surprisingly low figure.

Risk assessment and risk management have been of particular concern since the Enron scandal. Corporate boards and their audit committees must understand the business and financial risks that may be threats to their company. An audit committee of independent and knowledgeable directors is in a good position to ask management the right questions to determine whether the company is adequately managing risk. The BRC identified risk assessment oversight and risk management oversight as an audit committee best practice. The NYSE proposal requires the audit committee to discuss with management the company's financial risk assessment and risk management policies. It is imperative that audit committees determine not just what management has done to identify the risks, but also what they have done to monitor and control the risks. Given the importance of this area, it is surprising to find that only 39% of audit committees acknowledged responsibility for this area.

The Sarbanes-Oxley Act proposed that companies adopt a code of ethics for senior financial officers. The SEC has approved regulations recommending that the code of ethics include both senior financial officers and senior executive officers. Companies would be required to disclose whether or not they had adopted such a code, and if not, why not. All three of the exchanges have proposed that companies adopt a code of ethics. In addition, all three propose that the code should apply to all employees.

A mechanism for compliance is required by the SEC and all three exchanges, but none of them specifically indicate who should perform compliance oversight. The Treadway Commission stressed that an ethical code of conduct cannot succeed without a monitoring and enforcement mechanism. It also stated that it is the board of directors' responsibility to ensure that a mechanism exists and functions as intended. The Treadway Commission recommended that this responsibility be delegated to the audit committee, supporting it as a best practice. Only 40% of the audit committees in this study assumed responsibility for this area.

The BRC stressed the importance of the internal audit function in the internal control process, along with its importance in assisting the audit committee in monitoring the adequacy of the internal control process and the extent to which management follows the control procedures. The BRC stated that it was essential for the internal auditor to be able to approach the audit committee in private, confident of receiving the necessary support and guidance. The Treadway Commission recommended that the audit committee review the internal audit's scope of responsibilities, and the NYSE proposal requires that all NYSE companies have an internal audit function, with oversight responsibility from the audit committee. Only 58% of the audit committees in this study asserted responsibility over internal audit. Given the critical importance of the internal audit function, audit committee oversight should be required for all companies.

The Treadway Commission emphasized the necessity of a mechanism, perhaps within the code of conduct, to receive complaints from employees and protect employees from reprisals. The Sarbanes-Oxley Act and NASDAQ's proposal will require that audit committees establish procedures to handle complaints on "accounting, internal accounting controls, or auditing matters" and to provide confidentiality to employees that submit complaints. None of the audit committees in this study acknowledged responsibility for such a function.

The Sarbanes-Oxley Act requires disclosure of related-party transactions between management and principal stockholders, but it does not specifically require audit committee oversight of these transactions. Both the NASDAQ and AMEX proposals require that the audit committee, or a comparable body, review and approve related-party

transactions, making it a best practice. Only 4% of the audit committees in the study asserted responsibility for this function.

Ensure open communication among management, internal auditors, external auditors, and the audit committee. The BRC recommended that the audit committee meet separately with management, internal auditors, and external auditors. The NYSE proposal requires that the audit committee meet separately with all three groups. As stated by the BRC: "Since the audit committee is largely dependent on the information provided to it by management, the internal auditor, and the outside auditors, it is imperative that the committee cultivate frank dialogue with each." It is critical that the audit committee meet in private with each group, both on a regular schedule and on an as-needed basis.

Eighty-two percent of the audit committees in the study indicated that they met in private with external auditors, 61% with management, and only 46% with internal auditors. This last result may be related to the low percentage of audit committees that took responsibility for overseeing the internal audit function. These findings lend support to the contention that audit committees have underutilized the internal audit resource.

Oversee hiring and performance of the external auditors. The passage of the Sarbanes-Oxley Act has greatly expanded the duties of the audit committee in monitoring the external audit. The audit committee will be responsible for selecting and replacing auditors and preapproving audit and nonaudit fees and services, as well as overseeing the external auditor's performance. Under Sarbanes-Oxley, the audit committee is solely responsible for hiring and firing the auditor. Only 10% of the audit committees in this study assumed this responsibility, while 87% of the committees shared the responsibility with the full board. Only 9% preapproved audit or nonaudit fees.

With respect to monitoring performance, 90% of the audit committees surveyed oversee the external auditor's performance by reviewing the audit scope or audit plan along with the audit results. Although NASDAQ has not specified this requirement, it is a best practice that all audit committees should follow. With the passage of SAS 99, *Consideration of Fraud in a Financial Statement Audit*, external auditors will be asking audit committees to discuss the company's risk of fraud. Assessing the risk of fraud will be included in the audit scope, and the audit committee should satisfy themselves that the external auditor is doing this.

In addition to the above responsibilities, there are five audit committee responsibilities related to oversight of the external audit process itself:

- The BRC recommended that the external auditor be accountable to both the audit committee and the board. This is consistent with the markets' listing rules. Eighty percent of the audit committees surveyed acknowledge this accountability. The Sarbanes-Oxley Act requires the external auditor to report directly to the audit committee, which may potentially change future accountability.
- Ensure auditor independence. The three exchanges and the SEC require that audit committees get a written statement from the external auditors on their relationships with the company, consistent with ISB 1. There is no requirement that the audit committee make a statement about the committee's conclusions concerning the external auditors' independence; however, they are required to have a discussion with the auditors regarding their independence. As required by the SEC, all audit committees in this study reported that they had received ISB 1 from their auditors, and nearly all of the audit committees indicated responsibility for oversight of the auditor's independence in their charter.
- Ensure auditor qualifications. The NYSE proposal requires that the audit committee receive a report from the external auditor describing the auditor's quality-control procedures, any material issues raised by the auditor's most recent internal quality-control review or peer review, and any investigation by governmental or professional authorities within the preceding five years. Although only the NYSE has proposed this requirement, it is included in audit committee best practices. Only 2% of the audit committees in our sample asserted responsibility for this function, a disappointing result.
- The Sarbanes-Oxley Act requires that the audit committee not only discuss disagreements between management and the external auditors, but also resolve those disagreements. Only 1% of audit committees indicated that they both discuss and resolve disagreements. Thirty-five percent indicated that they discuss the disagreements, but took no responsibility for resolving them. Because discussing the disagreements is required by GAAS, 35% may

be an understatement. Many audit committees included a disclaimer that they were not responsible for resolving disagreements.
- Audit committees and external auditors are required to discuss various matters required by GAAS. All of the audit committees reported discussing GAAS with the external auditors in the audit committee report, as is required by the SEC. Nonetheless, many did not explicitly list this as a responsibility in their audit committee charter, leaving open the possibility that this is the external auditor's responsibility only. A proactive audit committee should explicitly state their responsibility for this function in their charter.

Composition. The Sarbanes-Oxley Act requires that all audit committee members be independent and that one member have accounting or financial management expertise. NASDAQ, the NYSE, and AMEX all proposed independence criteria similar to the SEC rule changes. The NYSE added a waiting period before a former officer or employee may be a director. In addition to the expertise requirement, the three stock markets require that the committee consist of at least three members and that all members be financially literate.

Nearly all of the audit committees surveyed required all audit committee members to be independent, although a few indicated that one nonindependent member would be allowed under exceptional circumstances. Over 90% indicated that the committee would include at least three members. Almost 90% stated that one member must have accounting or financial management expertise and that all members must be financially literate or become financially literate within a reasonable time after appointment. Some companies were explicit regarding independence and financial knowledge, while many companies merely stated that committee members were required to meet the qualifications required by NASDAQ.

The fact that all requirements were acknowledged by the vast majority of the companies is reassuring. Sarbanes-Oxley has tightened the criteria for independence. Therefore, NASDAQ companies must review the criteria they are currently using. In addition, the NASDAQ proposal requires that audit committee members must be financially literate at their time of appointment, with no opportunity to become financially literate on the job.

Other requirements. The following are additional best practices of audit committees:

- Sarbanes-Oxley requires that the audit committee have the authority and funding to use outside experts in their investigations. The NASDAQ, NYSE, and AMEX proposals all include this requirement. The study results indicate that 63% of audit committees already have this authority. It is essential that companies not currently granting this authority to their audit committees do so as soon as possible in order to be in compliance with both the Sarbanes-Oxley and the NASDAQ listing requirements.
- The audit committee charter should disclose the scope, structure, and audit committee process. This is required by all three stock exchanges. All of the audit committee charters surveyed met this requirement and are in compliance with NASDAQ requirements.
- As specified in Exhibit 2, the SEC requires an audit committee report to be included in the company's annual proxy. All of the companies provided this report, and all included the required disclosures. Only 49% of the audit committees acknowledged responsibility for this item in their charter.
- The charter should be reviewed annually; the SEC requires that it be provided to stockholders at least every three years. NASDAQ, the NYSE, and AMEX all require an annual review of the charter.

Seventy-eight percent of the audit committees indicated that they were responsible for reviewing their charter annually.

The remaining items are neither required nor proposed by any regulator, but are considered to be best practices:

- The BRC recommended that the audit committee have the authority to investigate any matter considered necessary. Just 69% of audit committees surveyed had the authority to investigate any matter within the scope of their responsibilities. In order for them to be effective monitors of the financial reporting process, this authority should be granted to all audit committees.
- The NYSE proposal requires an annual performance evaluation of audit committees. Only 2% of audit

committees asserted responsibility for performing an annual evaluation of their performance.
- The BRC recommended that the audit committee report annually about whether it has fulfilled its responsibilities as listed in its charter. None of the committees studied said they were responsible for reporting annually as to whether or not they had fulfilled the responsibilities assumed in their charter.

Implications and Recommendations

Audit committees are not assuming all of the responsibilities that would lead to effective, proactive oversight. Very few of the best practices surveyed were assumed by all of the audit committees, and the practices with the highest reported percentages were those that were required. With the passage of the Sarbanes-Oxley Act and the proposed NASDAQ listing requirements, audit committees will be required to provide even greater oversight.

The study's results indicated that audit committees currently are not fulfilling oversight responsibilities for which they will soon be responsible. Audit committees reported little or no authority for providing a mechanism to report whistle-blower complaints, approving related-party transactions, and preapproving audit and nonaudit fees. Audit committees should be proactive in complying with the new requirements, and should seek any necessary advice and training in order to fulfill these new responsibilities.

Individual audit committees should consider adopting all of the audit committee best practices that apply to their situations, even those that are not required, such as oversight of internal audit, oversight of company compliance with the code of ethics, and increased monitoring over financial reporting. The results imply that audit committees are very good at taking on responsibilities when required. On the other hand, their record for assuming nonrequired best practices is mixed, at best. If audit committees do not voluntarily assume best practices, regulators may find it necessary to intervene. The effectiveness of the audit committee should be evaluated at least annually in order to ensure continued compliance with best practices requirements and recommendations.

Second, the audit committee is accountable to the shareholders it represents, and must make significant improvements in their communication and disclosure to shareholders. They must disclose responsibilities that they have assumed, and they also must disclose the extent to which they have fulfilled these responsibilities. In order to ensure that shareholders can easily determine audit committee responsibilities, all audit committee responsibilities should be disclosed in a single place in the proxy, preferably in the audit committee charter. The findings suggest that the audit committee charters do not always include all of the assumed audit committee responsibilities, which are sometimes listed in the audit committee report, sometimes in the description of the board committees, and sometimes with the information on the audit fees. The audit committee should disclose all of its duties in its charter. Boilerplate charters should be not be used; charters should be written to address the individual needs of the specific company.

Finally, to improve accountability to the shareholders, as recommended by the BRC, the audit committee should report whether the responsibilities assumed in the charter have actually been carried out. The current audit committee report required by the SEC mandates only minimal disclosure and does not provide complete and adequate disclosure of audit committee responsibilities actually performed. In order to provide complete disclosure, audit committees should follow the BRC's advice and communicate to shareholders both their assumed responsibilities and the extent to which these responsibilities have been carried out.

***Annemarie K. Keinath, PhD**, is an associate professor of accounting at Indiana University Northwest, and **Judith C. Walo**, PhD, CPA, is a professor of accounting at Central Connecticut State University.*

Close

EXHIBIT 1
SARBANES-OXLEY AUDIT COMMITTEE REQUIREMENTS

Requirement	Comments
External Audit	
■ Preapprove audit and nonaudit services.	■ This is a new requirement that should increase scrutiny on auditor independence issues.
■ Receive reports from auditor on critical accounting policies; receive reports from auditor on discussions with management on alternative GAAP, their effects, and the auditor's preference; receive reports from auditor on material communications with management.	■ These requirements expand the communication between the committee and external auditors to include the auditor preferences and all material discussions with management affecting financial reporting.
■ Oversee the auditor engagement (engaging, compensation, and resolving disagreements with management on financial reporting). Auditor reports directly to the audit committee.	■ This requirement greatly expands the responsibility of the committee for the audit. Now the committee is not only responsible for discussing disagreements auditors had with management but is responsible to resolve them.
Composition and Authority	
■ Members must be independent.	■ Independence criteria are heightened.
■ Authority to engage special counsel or expert to advise, with funding for the advisor provided by the company.	■ Not new requirement for many companies, but it explicitly refers to the funding provision.
Internal Control	
■ Provide procedures to receive, retain, and treat complaints; provide procedures to confidentially handle employee complaints (whistle-blower protection).	■ These are new requirements for the audit committee.

EXHIBIT 2
CURRENT SEC REQUIREMENTS FOR THE REPORT OF THE AUDIT COMMITTEE

A Report of the audit committee must be included in each annual proxy.

Required disclosures in the report:

- Whether or not the audit committee discussed the annual financial statements with management.
- Whether or not the audit committee discussed with external auditors the matters required to be discussed by SAS 61 as may be modified or supplemented.
- Whether or not the audit committee received the external auditor's disclosure regarding independence which is required by ISB 1 as may be modified or supplemented.
- Whether, based on review and discussion of the above three items, the audit committee recommends to the board of directors that the audited financial statements be included in the company's annual report.

The company must also disclose in the proxy whether or not the audit committee has a charter (they are not required to have a charter, however). If they have a charter, they are required to provide a copy of the charter in the proxy at least every three years.

EXHIBIT 3
NASDAQ ADDITIONAL REQUIREMENTS

Responsibility	Proposed or Preexisting NASDAQ Requirement	Other Sources
Approve all related-party transactions.	Proposed	AMEX
Committee Composition:		
At least three members.	Preexisting	NYSE, AMEX
Members must be financially literate at time of appointment.	Proposed. Preexisting allows after appointment.	NYSE, AMEX at time of appointment. BRC allows after appointment.
One member must be a financial expert.	Preexisting	NSYE, AMEX, BRC
Oversight of External Audit:		
Ensure that external auditor is accountable to both board and audit committee.	Preexisting	NYSE, AMEX, BRC
Ensure auditor independence.	Preexisting	NYSE, AMEX, BRC
Audit Committee Charter:		
Charter must be reviewed annually.	Proposed	AMEX, NYSE
Charter contains the audit committee's scope, structure, and process.	Preexisting	AMEX, NYSE, BRC
Must have a written charter.	Preexisting	NYSE, AMEX, BRC

EXHIBIT 4
BEST PRACTICES FROM OTHER SOURCES

Responsibility	Source
Financial Reporting:	
Review and discuss annual and quarterly statements and MD&A with management and auditors.	NYSE, BRC, (except MD&A)
Review earnings press releases and guidance provided to rating agencies.	NYSE
Internal Control:	
Monitor system of internal control.	NYSE, BRC, Treadway
Monitor system for compliance with legal and regulatory requirements.	NYSE
Monitor system of risk assessment and risk management.	NYSE, BRC
Oversee internal audit function.	NYSE, BRC, Treadway
Oversee system for compliance with ethical codes.	Treadway
Ensure open communication and information flow with management, internal auditors, and external auditors.	NYSE (audit committee meets separately with each), BRC
Oversight of External Audit:	
Ensure auditor qualifications.	NYSE
Oversee performance of external auditor.	NYSE
Other Responsibilities:	
Must prepare the report SEC requires in annual proxy.	NYSE
Annual evaluation of the audit committee.	NYSE
Must have authority to investigate any matter.	BRC
Must report annually on whether the committee has fulfilled its responsibilities under the charter.	BRC

EXHIBIT 5
AUDIT COMMITTEE RESPONSIBILITIES, NASDAQ 100
(98 U.S. COMPANIES)

Oversee Financial Reporting Process:	
Review annual financial statements.	100%
Discuss annual financial statement with management and auditors.	95
Review quarterly statements.	84
Discuss quarterly statements with management and auditors.	68
Review Management Discussion and Analysis (MD&A).	8
Discuss MD&A with management and auditors.	1
Review earnings press releases.	14
Review earnings guidance provided to rating agencies.	0
Monitor Choice of Accounting Policies and Principles:	**63**
Discuss quality of accounting principles with the auditors.	59
Monitor System of Internal Control:	**98**
Monitor system for compliance with legal and regulatory requirements.	60
Monitor system of risk assessment and risk management.	39
Oversee system for compliance with codes of ethics.	40
Establish procedures for receiving and investigating whistle-blower complaints.	0
Oversee the internal audit function.	58
Approve all related-party transactions.	4
Ensure Open Communication with Management, Internal Auditors, and External Auditors:	
With management.	61
With internal auditors.	46
With external auditors.	82
Oversee Hiring and Performance of External Auditors:	**98**
Select and replace external auditors:	
Solely audit committee.	10
With full board of directors.	87
Preapprove audit or nonaudit fees.	9
Approve audit fees.	38
External auditor is accountable to the board and audit committee.	80
Oversee auditor independence.	100
Ensure auditor qualifications.	2
Discuss and resolve disagreements between external auditors and management.	1
Discuss only.	35
Discuss matters required by GAAS.	100
Review audit scope, audit plan, and results.	90
Composition of the Audit Committee:	
One member has accounting or financial management expertise.	89
All other members must be financially literate.	89
All members must be independent.	99
At least three members.	94
Other:	
Scope, structure, and process of committee included in charter.	100
Charter reviewed annually.	81
Authority to use outside experts.	66
Authority to investigate any matter.	69
Prepare report required by the SEC in the annual proxy.	54
Perform an annual evaluation of the committee.	2
Report annually whether the committee has fulfilled its responsibilities under the audit committee charter.	0

PAISLEY CONSULTING

Business accountability solutions.

Direct Report Assessment Approach Options:

Assurance Specialists:

DR #1 COMPLIANCE FOCUS

Review and report on compliance with rules/ policies.

DR #2 PROCESS FOCUS

Examine and document business processes and provide opinions on control adequacy.

DR #3 OBJECTIVE FOCUS

Select one or more end result objective(s) for assessment and provide opinions on controls and/or residual risk.

DR #4 RISK FOCUS

Select a context. Identify and assess the risks and effectiveness of controls.

DR #5 CONTROL FRAMEWORK FOCUS

Review the control framework in place against defined control criteria in one or more control models. (e.g. COSO ERM)

Direct Report

Assurance Specialist(s)

Examines, documents and verifies controls and/or risk status

Risk Arena Overview

Regulators

The Board of Directors

RISK SOURCE: EVENTS, ACTIVITIES, OR CIRCUMSTANCES THAT CAN EFFECT AN ORGANIZATION AND THE ACHIEVEMENT OF BUSINESS/QUALITY OBJECTIVES.

Commercial/ Legal

Product/ Service Liability

Finance/ Economic

Environmental Liability

Customers

Suppliers

Employees

Competition

Missing Objectives

Fraud/ Corruption

Equipment/ Technology

Control Design

Natural Events

Political Influences

Public Perception

Human Behaviour

Assurance Universe

Assurance Functions

External Audit	*Internal Audit/ Evaluation*	*Health & Safety*	*Environment*	*Quality*	*Legal*	*Regulatory Compliance*	*Risk & Insurance*

Self-Assessment

Management/ Work Units

Analysis of risks, processes, controls relating to business objectives

Product: Assurance Specialist's report/ opinion on control effectiveness/status

(Direct report auditing)

Assurance Approach

Product: Specialist assurance related to management's report on control/risk status

(Attestation auditing)

Self-Assessment Approach Options:

Work Units:

SA #1 COMPLIANCE FOCUS

Self-assess their state of compliance and report on conformance with rules/policies.

SA #2 PROCESS FOCUS

Self-assess business processes and report opinions on adequacy.

SA #3 OBJECTIVE FOCUS

Select one or more end result objective(s) for assessment and report opinions on adequacy of residual risk.

SA #4 RISK FOCUS

Select a context such as business unit, process, or topic. Identify and assess the risks and the effectiveness of the controls.

SA #5 CONTROL FRAMEWORK FOCUS

Review the control framework in place against defined control criteria in one or more control models. (e.g. COSO ERM)

www.paisleyconsulting.com

Technology: Risk Navigator™, Focus™, CARD®*map*, AutoAudit®

Capability: Sarbanes-Oxley, ERM, Basel and Internal Audit Training

RISK FITNESS QUIZ

Risk Assessment

1. How well do we identify, measure and document the threats/risks that could impact on the achievement of our business objectives?

SCORE: /10

Control Assessment

2. How well and how often do we reevaluate the effectiveness of our control frameworks?

SCORE: /10

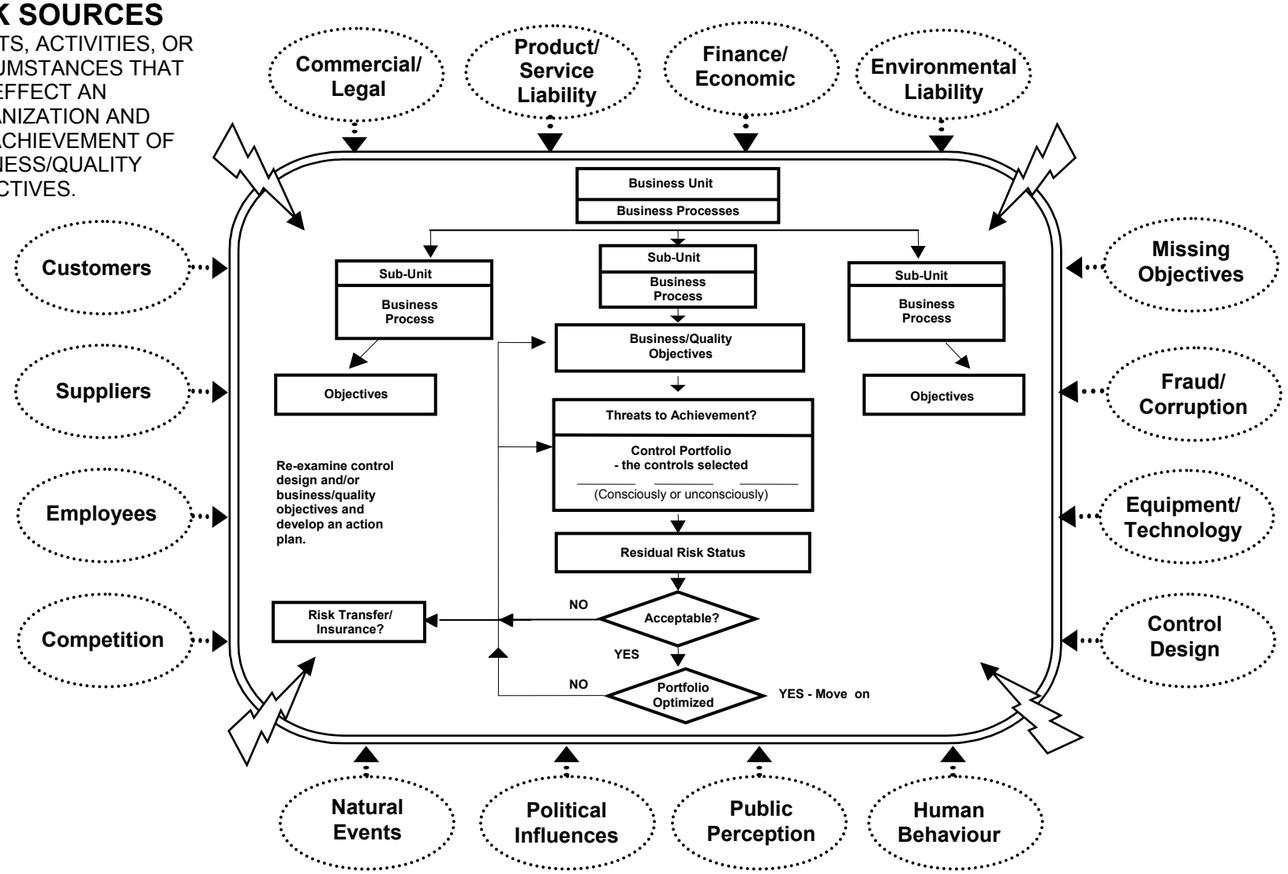
Control Cost Optimization

3. How good are we at identifying opportunities to eliminate controls while still maintaining an acceptable residual risk level at a lower overall cost?

SCORE: /10

The Business Risk Arena

RISK SOURCES
EVENTS, ACTIVITIES, OR CIRCUMSTANCES THAT CAN EFFECT AN ORGANIZATION AND THE ACHIEVEMENT OF BUSINESS/QUALITY OBJECTIVES.



Risk Testing the Future

4. How good are we at documenting and evaluating risks when making important business decisions, launching new products/services, and preparing strategic business plans?

SCORE: /10

Planning for Serious Risk Situations

5. Do we have contingency plans in place to deal with potentially high risk but low probability situations that could cripple business units or the organization? Do we periodically revisit these plans to reassess their adequacy?

SCORE: /10

Worst Case Scenarios

6. How good are we at considering the possibility of high risk situations which, if they occurred together, could have a devastating impact on the organization?

SCORE: /10

Oversight Process

10. How well briefed is Senior Management and the Board of Directors on major risks the organization faces? Have they taken steps to ensure work units are identifying, measuring, controlling and monitoring significant risks?

SCORE: /10

Regular Reevaluation

9. How effective is our corporate process to periodically reassess the acceptability of risk acceptance decisions?

SCORE: /10

Risk Transfer/Financing Options

8. How effective are we at identifying risk sharing and insurance options to avoid or reduce the consequences of specific threats/risks to your business objectives?

SCORE: /10

Early Warning Systems

7. How good are we at regularly monitoring our risk status using early warning signs that indicate changes might be needed to controls and/or objectives?

SCORE: /10

TOTAL RISK FITNESS SCORE:

CONTROL FITNESS QUIZ

1. Purpose: Definition & Communication

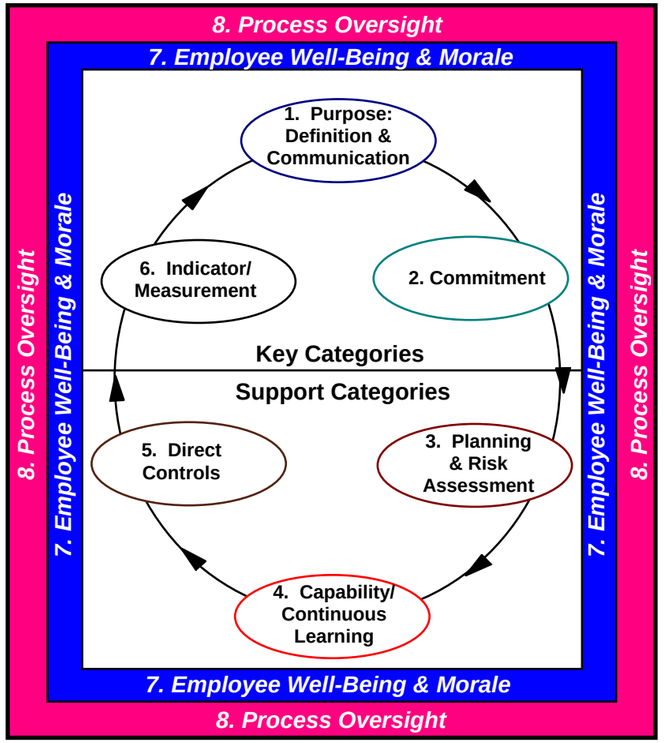
Do we know the end result business/quality objectives we must achieve to be successful? Have we formally defined and communicated these to the people that must support them?

SCORE /15

2. Commitment

Are the people that are important to the achievement of our business objectives committed to the achievement of those objectives?

SCORE /15



8. Process Oversight

Are there demonstrable processes in place to oversee that the organization's risk and control management systems are actually resulting in an acceptable level of residual risk? (i.e. the risk of not achieving objectives)

SCORE /15

7. Employee Well-Being & Morale

Is employee well-being and morale negatively or positively impacting on the achievement of objectives? How well are we managing this area?

SCORE /10

3. Planning & Risk Assessment

Are we thinking about what lies ahead and the barriers and obstacles we may have to deal with? Have we considered how we will deal with problems?

SCORE /10

4. Capability/Continuous Learning

Do we have the necessary knowledge and skills in place to achieve specified objectives?

SCORE /10

5. Direct Controls

Do we have effective direct controls including methods, procedures or devices to help assure the achievement of objectives?

SCORE /10

6. Indicator/Measurement

Do we know how well we are, or are not, achieving our business objectives? Are we measuring progress in all key areas?

SCORE /15

TOTAL SCORE /100

Allocating Assurance Resources – What's Best Practice?

GROUP EXERCISE

In your assigned group pick what you think would be the best, most effective way to allocate limited assurance resources. Be prepared to report your conclusion to the Forum.

Assurance Resource Allocation Options	Ranking
1. Straight cyclical coverage. All parts of the assurance universe covered over some predefined time period.	
2. Based on requests from senior management.	
3. Using a scoring formula maintained by internal audit which allocates points based on: (1) Annual sales volume (2) Assets at risk (3) Time since last audit (4) Previous audit rating	
4. Based on a scoring formula maintained by internal audit which allocates risk points related to the following categories: (a) Property risk (b) Monetary assets (c) People risk (d) Commercial risk (e) Information (f) Legal Regulatory Risk (g) Political (h) Operational	
1. Based on a scoring formula maintained by internal audit that scores each business unit on their overall "Risk Fitness". 10 questions are scored individually from 1 to 10 possible points. Each score indicates the degree with which the organization manages or completes each activity or process describing the question (i.e. the quality). The maximum possible Risk Fitness score is 100. The questions to be scored are: (1) How do you identify and measure the threats/risks that could impact on the achievement of your business objectives? (2) How healthy are your control frameworks? How do you know? How long has it been since you evaluated their effectiveness? (3) Could you eliminate some controls and still have an acceptable residual risk level at a lower overall cost? How do you monitor this?	

Allocating Assurance Resources – What's Best Practice?

Assurance Resource Allocation Options	Ranking
(4) Do you consider and evaluate risks when making important business decisions and preparing strategic plans? How? (5) Do you have contingency plans in place to deal with low probability, high risk situations that could cripple your unit or the company? Do you periodically revisit these plans to reassess their adequacy? (6) Have you considered the possibility of high risk situations that, if they occurred together, could have a devastating effect on the company? How? How often? (7) Do you regularly monitor your risk status for early warning signs that changes are needed to your controls and/or objectives? How? (8) Have you considered risk transfer and insurance options available to avoid or reduce the consequences of specific threats/risks to your business objectives? (9) Do you periodically reassess the acceptability of your risk acceptance decisions? How? (10) Does Senior Management and the Board of Directors understand the major risks the company faces and take steps to ensure work units are identifying, measuring, controlling and monitoring risks? Business units with lower scores are allocated more audit resources than those with high scores.	
6. Based on results derived from anonymous voting workshops. In the workshop people in the business unit vote on the degree to which they believe their unit manifests control criteria in a specified control model such as COSO, CoCo, CARD® *model*, (see example page 29) and discuss any concerns identified. This results in a score for each control category in the model and an overall score. Units with low control model conformance scores receive more assurance attention than those with higher scores.	

Allocating Assurance Resources – What's Best Practice?

<table>
<tr><th>Assurance Resource Allocation Options</th><th>Ranking</th></tr>
<tr><td>7. Based on a risk formula developed by internal audit that uses 19 variables. The variables used are listed below. Ratings are assigned by internal audit judgementally based on available knowledge and information.

(1) Quality of Internal Control
(2) Competence of Management
(3) Integrity of Management
(4) Size of Unit ($)
(5) Recent Change in Accounting System
(6) Complexity of Operations
(7) Liquidity of Assets
(8) Recent Change in Key Personnel
(9) Economic Condition of Unit
(10) Rapid Growth
(11) Extent of Computerized Systems
(12) Time Since Last Audit
(13) Pressure on Management to Meet Objectives
(14) Extent of Government Relations
(15) Level of Employees' Morale
(16) Audit Plans of External Auditors
(17) Political Exposure
(18) Need to Maintain an Appearance of Independence by Internal Auditor
(19) Distance from Main Office</td><td></td></tr>
<tr><td>8. Based on performance indicator information on how well objectives are currently being achieved. This information may be input into an integrated risk management system by work units and/or assurance personnel. Performance Indicators input by work units are quality assured by assurance staff independent of the work unit. Objectives with "Very Negative" performance indicator status and high risk to the organization ratings are allocated the most assurance resources.</td><td></td></tr>
<tr><td>9. Based on the quality assurance reviews of control and risk self-assessments generated by work units. Units which generate highly reliable, candid self-assessment disclosures are allocated less assurance resources than units that produce incomplete and/or untruthful self-assessments.</td><td></td></tr>
</table>

Defining The Assurance Universe

Category of Objectives	Include in Internal Audit Scope Yes/No	Assign to Another Specialist Group? Who?	Require Work Unit Reports on Risk Status Yes/No	Assurance Level Required on Risk Status Information Low/Medium/High	Frequency of Update
Product Quality (PQ)					
Customer Service (CS)					
Minimizing Unnecessary Costs (MUC)					
• Salaries					
• Program Costs					
• Admin. Costs					
• Capital Costs					
Revenue/Profit					
• Sales/Revenue Growth					
Reliable Business Information (RBI)					
• Reliable External Reporting of the Financial Statements					
• Reliable Production Reporting					
• Reliable Operating Statistics					
• Reliable Budget to Actual Reporting					
Asset Safeguarding (AS)					
• Cash					
• Inventory					
• Corporate Information					

Defining The Assurance Universe

Category of Objectives	Include in Internal Audit Scope Yes/No	Assign to Another Specialist Group? Who?	Require Work Unit Reports on Risk Status Yes/No	Assurance Level Required on Risk Status Information Low/Medium/High	Frequency of Update
• Intellectual Property					
Safety (S)					
• Employee					
• Contractor					
• Community					
• Customer					
Regulatory Compliance (RC)					
• Environment					
• Health & Safety					
• Securities					
• Human Rights					
• Other					
Fraud Prevention (FP)					
• Employee Fraud/Theft					
• Vendor Fraud/Theft					
• Corporate Fraud/Theft					
• Other Fraud/Theft					
Continuity of Operations (COO)					
• Ensure Adequate Feedstock/ Raw Material Supply					
• Ensure Availability of Critical Business Information Systems					

Defining The Assurance Universe

Category of Objectives	Include in Internal Audit Scope Yes / No	Assign to Another Specialist Group? Who?	Require Work Unit Reports on Risk Status Yes / No	Assurance Level Required on Risk Status Information Low / Medium / High	Frequency of Update
• Ensure Availability of Critical Plant Operating Computer Systems					
Unintentional Risk Exposure (URE)					
• Compliance with Laws					
• Compliance with Ethical Standards					
• Compliance with Company Policy					
• Compliance with Customer Contracts					
• Compliance with Vendor Agreements					

Utopia Assurance Certification

We, the undersigned, acknowledge to the Audit Committee that we have:

(1) Responsibility for developing and maintaining internal controls that provide reasonable assurance that ABC's significant business objectives will be achieved.

(2) Responsibility for overseeing that the organization has cost effective risk and control management systems that provide reasonable assurance ABC's business objectives will be achieved.

(3) Reviewed the significant control and risk issues identified by work units and management through our control and risk self-assessment process, and the significant issues identified by our Internal Audit department and our External Auditor, Smith & Jones that have been brought to our attention. We have initiated steps to adjust controls in areas where the error rates and/or residual risks identified related to the non-achievement of ABC's disclosure objectives were considered to be excessive and/or unacceptable by us.

(4) Reviewed our process to assess and manage risk and control and this year's report on our risk management processes and results prepared by our Internal Audit for the Audit Committee. We are satisfied that our risk and control assessment framework process provides you, our Audit Committee, and our External Auditors, Smith & Jones, with a reliable and materially complete report on the status of risk and controls across the organization.

CEO	*CFO*

I have reviewed the process used and information produced by management on the current state of risk, control and residual risk, for the Audit Committee. In my opinion the Audit Committee has been provided with a reliable and materially complete report on the status of risk and controls across the organization.

Chief Internal Auditor	*Date*

CARD® Quick Reference Sheet

BUSINESS/QUALITY OBJECTIVE FAMILIES

1. Product Quality (PQ)
2. Customer Service (CS)
3. Minimizing Unnecessary Costs (MUC)
4. Revenue/Profit Maximization (RPM)
5. Reliable Business Information (RBI)
6. Asset Safeguarding (AS)
7. Safety (S)
8. Regulatory Compliance (RC)
9. Fraud Prevention/Detection (FPD)
10. Continuity of Operations (COO)
11. Unintentional Risk Exposure (URE)
12. Contract Compliance (CC)
13. Internal Compliance (IC)

Note: The families sometimes overlap. The objective should be assigned to the family most descriptive of the objective type.

RISK SOURCES

- Commercial/Legal
- Competition
- Control Design
- Customers
- Employees
- Environmental Liability
- Equipment/Technology
- Finance/Economic
- Fraud/Corruption
- Human Behaviour
- Missing Objectives
- Natural Events
- Political Influences
- Product/Service Liability
- Public Perception
- Suppliers

RESIDUAL RISK STATUS INFORMATION

Indicator Data – Any information known about how effective the current control choices are with respect to the stated business/quality objective.

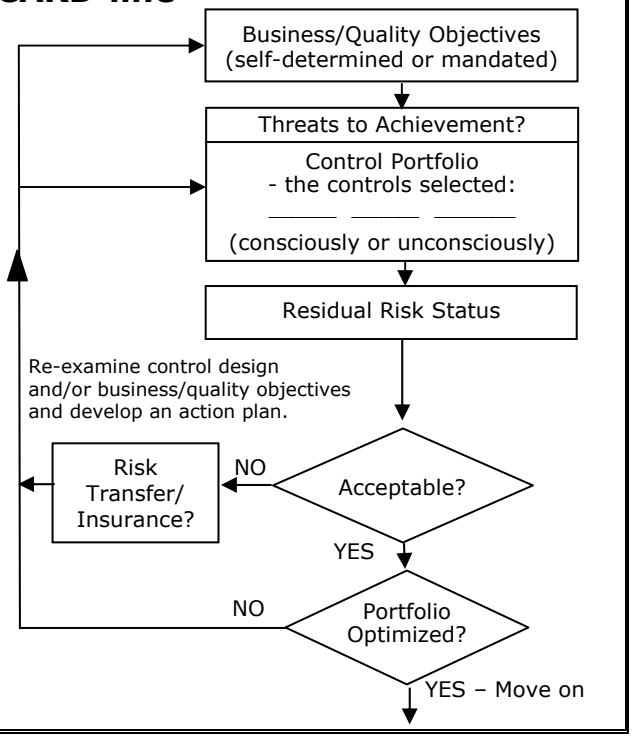
Impact Data – How bad would it be if the objective was not met in whole or in part? How would the organization, the officers, the staff, be impacted?

Impediment Data – Any situations or problems that stand in the way of the group or a group member adjusting the control element portfolio. These can relate to the lack of funds, cooperation of staff members or other departments, training deficiencies, senior management attitudes, and others.

Concern Data – Any known or suspected problems or issues related to the business/quality objective being assessed. This data is useful in assessing the likelihood of non-achievement given the controls in use or in place. This is referred to by Paisley Consulting as Residual Likelihood or the likelihood of non-achievement after considering the current control portfolio.

Risk Transfer/Insurance – Information on any risk transfer or insurance options in place that would mitigate specific threats to an objective and/or non-achievement of the objective.

CARD®*line*



RESIDUAL RISK INDEX DEFINITIONS

-1 OK Controls Excessive

0 Fully Acceptable - No unacceptable concerns. No additional attention or corrective actions required at the current time.

1 Low - Inaction on unacceptable terms could result in minor negative impacts. Routine attention required to adjust status to an acceptable level.

2 Moderate - Inaction on unacceptable items could result in or will allow continuation of mid-level negative impacts. Moderate effort required to adjust status to an acceptable level.

3 Significant - Inaction on unacceptable items could result in or will allow continuation of serious negative impacts. Attention required immediately to adjust status to an acceptable level.

4 Major - Inaction on unacceptable items virtually certain to result in or allow continuation of very major negative consequences. Analysis and corrective action required immediately.

5 Severe - Inaction on unacceptable items virtually certain to result in or allow continuation of very severe negative impacts. Senior level attention urgently required.

6 Catastrophic - Inaction on unacceptable items will result in or allow the continuation of catastrophic proportion impacts. Senior level attention urgently required to avert a catastrophic negative impact on the organization.

7 Terminal - The current status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from all key players will be necessary to prevent the total elimination of the entity.