

THE FUTURE OF CONTINUOUS ASSURANCE & RISK MANAGEMENT

CONTINUOUS AUDITING ≠ CONTINUOUS ASSURANCE

Tim J. Leech FCA·CIA, CCSA, CFE

CHALLENGING THE STATUS QUO

The World As I See It

Since the mid 1980s I have been an unabashed and relentless promoter of the premise that management has primary responsibility for risk and control management, including periodically assessing and reporting on its likely effectiveness. Appropriately effective risk and control management systems are necessary to produce reliable financial disclosures, prevent accidents, produce quality products, provide consistently good customer service, comply with laws, prevent internal and external fraud, and other relevant outcomes. When cost justified, management should be required to issue a representation to key stakeholders on the effectiveness of the controls in place that support important disclosures being made to stakeholders. Information on the effectiveness of controls allows users to assess the likely reliability of disclosures made by management.

A primary role of internal and/or external auditors, when cost justified, should be to report to entitled stakeholders on the reliability of management's representations on internal control effectiveness and the related primary disclosures. They should not assume primary responsibility for risk and control management or assessing and reporting on the state of risk and controls.

The Status Quo

Unfortunately, many internal and external auditors through the methods and tools they have used have not reinforced and promoted the principle of management responsibility for risk and control assessment and have, in fact, undermined this principle in a number of important ways. One can argue that "continuous auditing", a relatively new and extended form of auditing, can, if misapplied, further undermine the premise of management's responsibility for control. If management is truly responsible for designing and maintaining appropriately effective risk and control systems why shouldn't they also be responsible for periodically formally assessing and reporting on the effectiveness of those systems?

HOW DID THIS SITUATION OCCUR?

Auditors Assessing and Reporting on Control – Auditors Doing Management’s Job

Over the course of my career I have observed that in many organizations, at least prior to the advent of Sarbanes-Oxley, the only people expected to do formal risk and control assessment on a regular basis were internal auditors and consultants. Business unit managers, being generally rational people with limited time and resources, were happy not having to take on the additional task of systematically assessing and reporting on the status of risks and controls. In most cases, nobody expected them to do formal risk and control assessments, including the company’s external and internal auditors. Only rarely did internal or external auditors start an audit with a request to see the risk and control assessments prepared by management. They weren’t requested for the simple reason that the information usually didn’t exist. The more and better auditing done by auditors claiming to be “control experts”, the less inclined management was to do formalized risk and control assessment themselves – a very rational reaction.

Auditors and CAATs in 1980s and 90s – Auditors Doing Management’s Job With IT Tools

With the advent of Computer Assisted Audit Tools (“CAATs”) in the early 80s some adventurous internal and external auditors started to use these tools with widely varying levels of skill and commitment to identify potential problems, including fraud exposures and IT related problems. In many cases, what the auditors were attempting to do was create new and better detective business controls and/or become an integral part of the organization’s internal control system. External auditors, mainly in the big firms, experimented with CAATs with highly variable levels of commitment, resources and enthusiasm to improve the quality of their audit opinions on the financial statements produced by management.

Managers were usually happy to let auditors experiment and find new ways of sourcing useful information that they, as the owners of these systems, might benefit from. CAATs had the potential to produce useful information and some enlightened, ethical and secure managers were astute enough to recognize that fact. Better yet, the work to design and run CAATs was usually paid for from someone else’s budget, usually the internal audit department’s budget or it was built in to the total cost of the external audit. During this time period it was the rare business unit or controllership group that thought they should purchase, learn and use CAATs. Tools to identify gaps in internal control, fraud vulnerabilities, IT security issues, problems with the reliability of the accounts, and other unmitigated risks were, and are still today, primarily purchased and used by auditors. ACL, the dominant vendor in the space, estimates that less than 5% of their sales are made to non-auditors. The majority of the sales that have been made happened only after auditors demonstrated to business unit managers the power of CAATs.

External Auditors Have Been Happy to Do Management’s Work

In more than a few companies, year after year, external auditors in the course of their financial statement audit would identify errors in the accounts and require management book adjustments before the statements were issued. In some cases, this was because management didn’t have the skills to deal with increasingly complex and confusing accounting rules. In other cases, it was because accounting controls in place, including the quality of controllership staff, were weak and the combination resulted in recurring errors in

the accounts. In more than a few cases management knew exactly what they were doing but wanted to see if they could put one, or more than one accounting distortion, by the auditors to “make the numbers”. Few external auditors commented in management letters to the audit committee on serious control problems they saw in the course of their work or the fact that management themselves did very little formal risk and control assessment work. That would have been a revenue limiting move. Again, a very rational response.

Continuous Auditing – Extending the Approach of Auditors Doing Management’s Work

In the 1990s studies done by the CICA in Canada, the AICPA in the U.S. and the IIA began to elevate the concept of continuous auditing. In a May 2003 article published in The CPA Journal titled **Continuous Auditing: Leveraging Technology** Searcy and Woodroof summarized their view of this trend:

*Continuous Auditing leverages technology and opens database architecture to enable **auditors** to monitor a company’s system over the Internet using sensors and digital agents. Any discrepancies between the records and the rules defined in the digital agents are transmitted via e-mail to the client and the auditor. At that point the auditor can determine the appropriate action to take.*

The question isn’t whether this approach makes sense. The real question is who should have primary responsibility for doing it.

TOWARDS A NEW AUDITING PARADIGM

SOX Ushers In a New Era

The Sarbanes-Oxley Act of 2002 (“SOX”) ushered in a new paradigm in auditing. Section 404 states:

S404(b) Internal Control Evaluation and Reporting

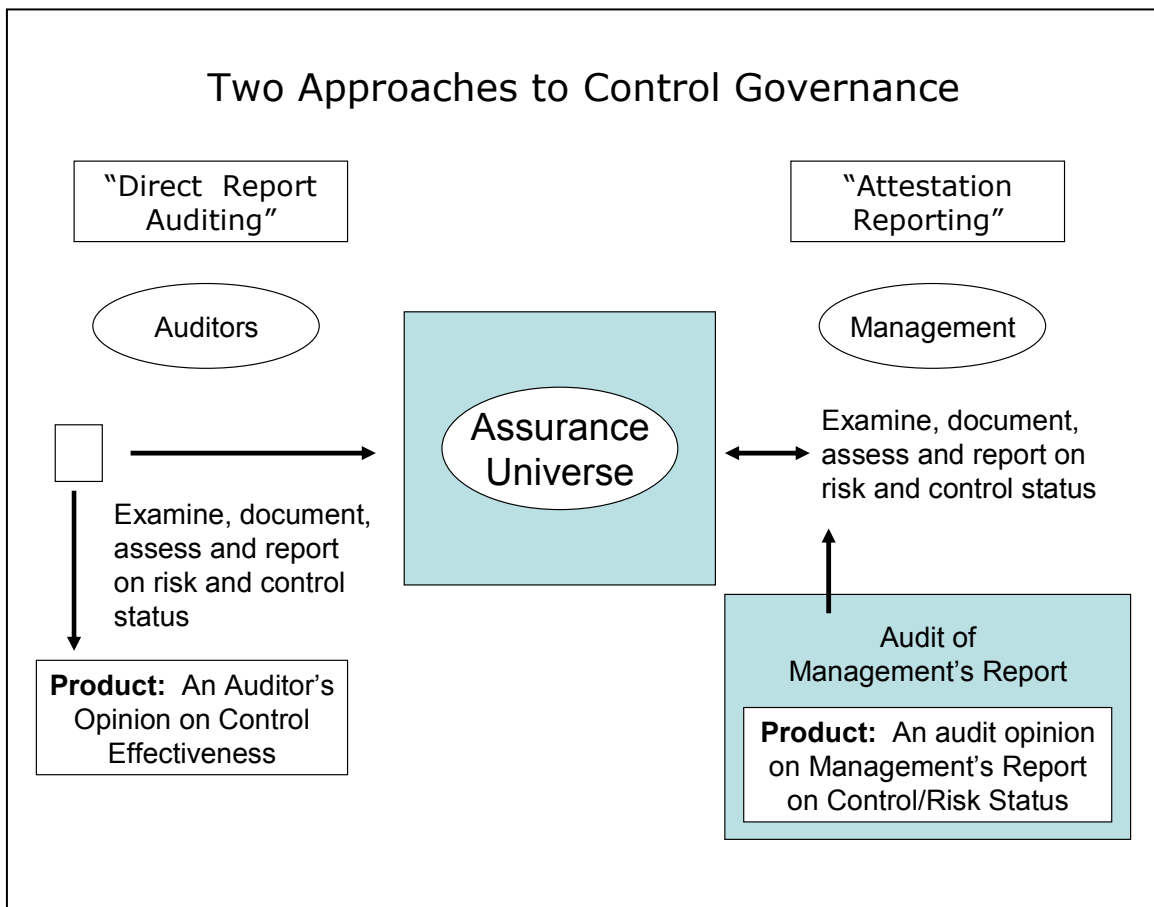
With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

SOX requires that management assess and report on the control systems in place to ensure reliable financial disclosures. The external auditor is charged with reporting on the reliability of that representation. Although the regulations enacted by the SEC and Public Company Accounting Oversight Board to give force to this new law have many serious deficiencies (see www.sec.gov/news/press/4-497.shtml for hundreds of comment letters detailing problems with the current SOX regulations), the basic concept of management assessing and reporting on control effectiveness and external auditors reporting on the reliability of management’s representation has been generally accepted by U.S. listed companies. Canada is following the U.S. lead in this area and more countries are expected to follow, at least directionally.

Direct Report Auditing vs. Attestation Reporting

Exhibit 1 below visually depicts the two primary audit approaches available to assess and report on control effectiveness. The left side of the diagram depicts the traditional approach to control assessment of an auditor examining one or more element of the assurance universe and reporting observations, conclusions and opinions. The right side of the diagram depicts management performing their own assessment of risks and controls and reporting their conclusions. The role of auditors on the right side of Exhibit 1 is to provide an opinion on the reliability of management's representation, much the same way auditors audit and report on the reliability of financial statements prepared by management.

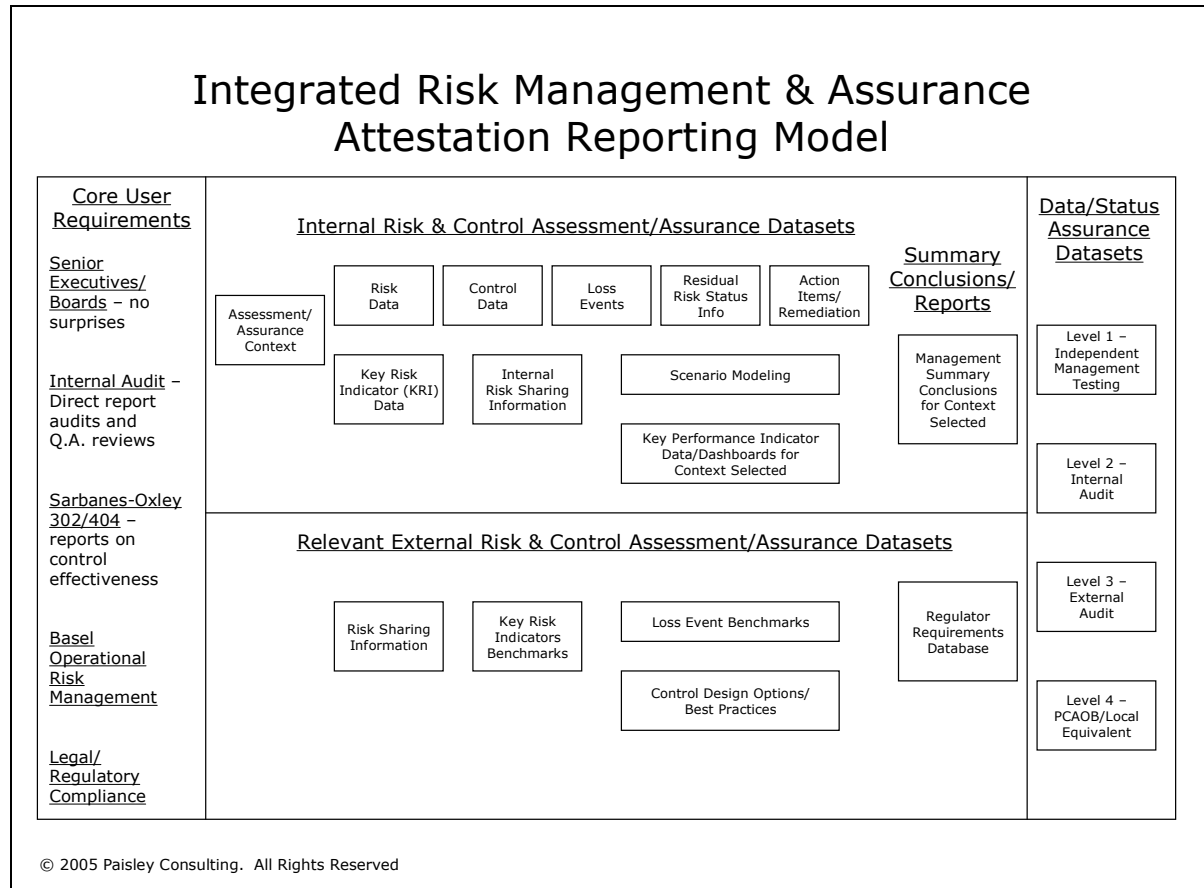
Exhibit 1



The simple visual depiction in Exhibit 1 can be significantly expanded to cope with the complexity that comes with more sophisticated approaches to enterprise risk and assurance management called for by new regulatory regimes like the Basel II Accord. A visual depiction of this type of world is shown below as Exhibit 2.

Moving away from the "Direct Report Auditing" paradigm that has been the status quo for decades to an "Attestation Reporting" approach to controls assessment has profound implications for auditors, both internal and external. It is an important and necessary step to emphasize and reinforce that periodic assessment of risks and control effectiveness should be a core management responsibility.

Exhibit 2



IMPLICATIONS OF THE SHIFT FROM DIRECT REPORT AUDITING TO ATTESTATION REPORTING

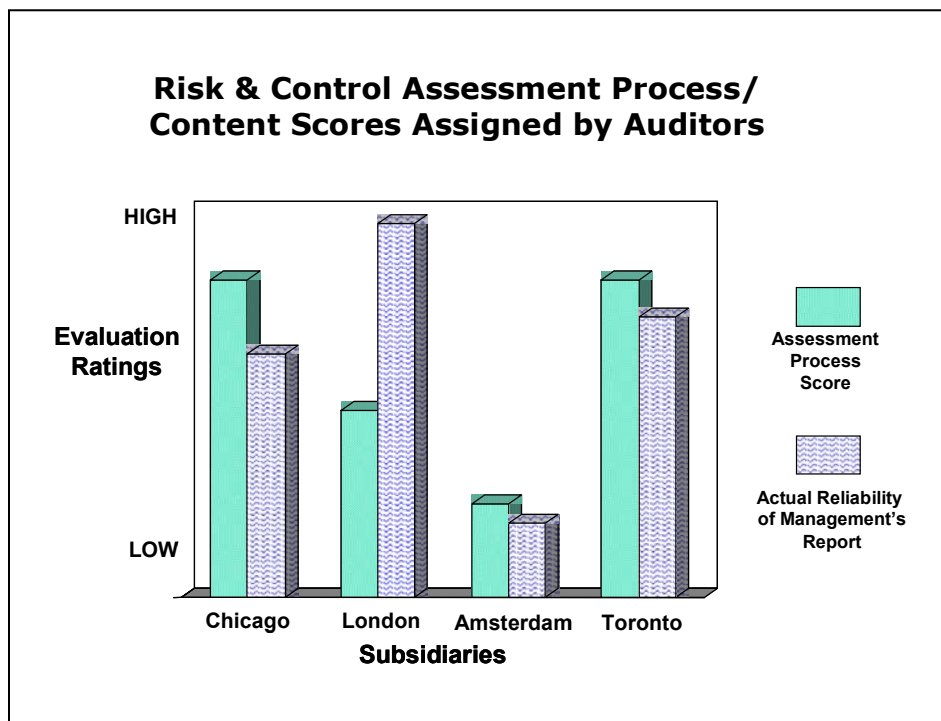
Implication #1 - For Internal Auditors

Once a move to formalized reporting on internal control by management occurs, internal auditors must radically change the approach they have traditionally used. In some companies this can mean that internal auditors become management's agents appointed to do the formal risk and control assessments and testing required to support management's representations. In other companies, internal auditors may play the role of Level 1 quality assurance and examine and evaluate the process used by management to assess and report on risks and controls and test the actual reliability of the results and conclusions produced prior to an external auditor and/or regulator commencing their review. The more involved internal auditors become preparing the management representation on control effectiveness, the less external auditors will be able to rely on their work because of independence concerns. The more internal auditors are involved doing the primary risk and

control assessments and the better at it they are the less frequently management will want to learn how to do it themselves.

The IIA has recognized the early signs of a shift from the "Direct Audit" paradigm of internal audit. In section 2110.A1 of the new professional standards issued in 2000 it states "**The internal audit activity should monitor and evaluate the effectiveness of the organization's risk management systems**". Unfortunately, for a variety of reasons many internal audit departments are currently not in compliance with this section of the IIA professional standards. An illustration of the type of report internal auditors should be delivering to senior management and audit committees on the quality of the organization's risk and control management systems is shown below as Exhibit 3. Attachment 1 to this paper outlines a conceptual framework that can be used to evaluate the quality of a company's risk management process.

Exhibit 3



Implication #2 – For External Auditors

External auditors must now learn new skills and take on radically new responsibilities and liabilities related to their new role assessing and reporting on the reliability of management's report on internal control effectiveness. During a round table on SOX hosted by the SEC on April 13, 2005 senior partners from the big 4 public accounting firms acknowledged that the first round of SOX had been a painful learning experience for them with more than a few problems. They also acknowledged that they were generally not yet performing "integrated" audits of both the controls and the financial statements but promised to work on improvements in this area to reduce costs. A large percentage of the external audit partners now required to form independent opinions on control effectiveness have only limited experience and formal training in this area. A serious concerted effort will be required to upgrade the skills of external auditors at all levels of these firms if regimes like SOX are intended to add real value at a reasonable cost.

Implication #3 - For Management

In countries where management responsibility to formally assess and report on internal control effectiveness has been legislated management should begin to show more active interest in learning how to assess and report on the status of risk and control, and the work done to date by the continuous auditing/monitoring community. Perhaps even more importantly, management teams that want to drive down compliance costs and improve risk and control management systems will show more interest in what were previously called continuous auditing tools. These tools can be used to replace expensive manual controls and perform continuous risk and control status monitoring. These tools have the potential to cost effectively provide "continuous assurance" to senior management, the board of directors, and external stakeholders that they are aware of the true state of risk and control.

Implication #4 – For Audit Committees

Audit Committees that have not been receiving the type of reports shown in Exhibit 3 should demand them. They should ask for them on all areas and aspects of the company they are responsible for overseeing. This could include reliability of accounting disclosures only, or expand to include areas such as compliance with laws, prevention of fraud, safety, environmental responsibility, product quality, customer service and more. Audit Committees should also ask the company's external auditor to quantify the amount of extra work they have performed that is attributable to deficiencies in the company's manual and automated internal control systems. In addition, they should ask what additional steps the external auditors have taken to audit the accounts when management has disclosed that material weaknesses and/or significant control deficiencies exist in the company's controls (i.e. how did the external auditor "audit around" these serious control gaps?).

Implication #5 - For the Emerging Discipline of Continuous Auditing

In the new world of attestation reporting, primary responsibility to formally assess and report on the status of internal control rests with management. It is management that should be adopting and applying the same techniques previously called continuous auditing. Continuous auditing in a world where management has primary responsibility to assess and report on control becomes relabelled as continuous monitoring. It should be done primarily by management to improve the reliability of their control effectiveness reports to stakeholders. Attachment 2 lists some sample tests ACL suggests to assess control effectiveness. In a world where management is truly responsible for internal control they should be actively considering the applicability of this type of testing and building them in to their core control systems. To date, internal and external auditors have been CAAT vendors' primary market. This is slowly starting to change as management assumes full responsibility for assessing and reporting on risk status and control effectiveness.

If internal and external auditors are to use "continuous auditing" tools and not undermine management responsibility to assess and report on control effectiveness they should develop new automated tools to analyze the reliability and completeness of the primary risk and control assessment work done by management. To the extent that internal or external auditors apply continuous auditing tools directly to the assurance universe owned by management, it should be done to refine their opinion on the reliability of management representations on risk status and control effectiveness.

THE FUTURE

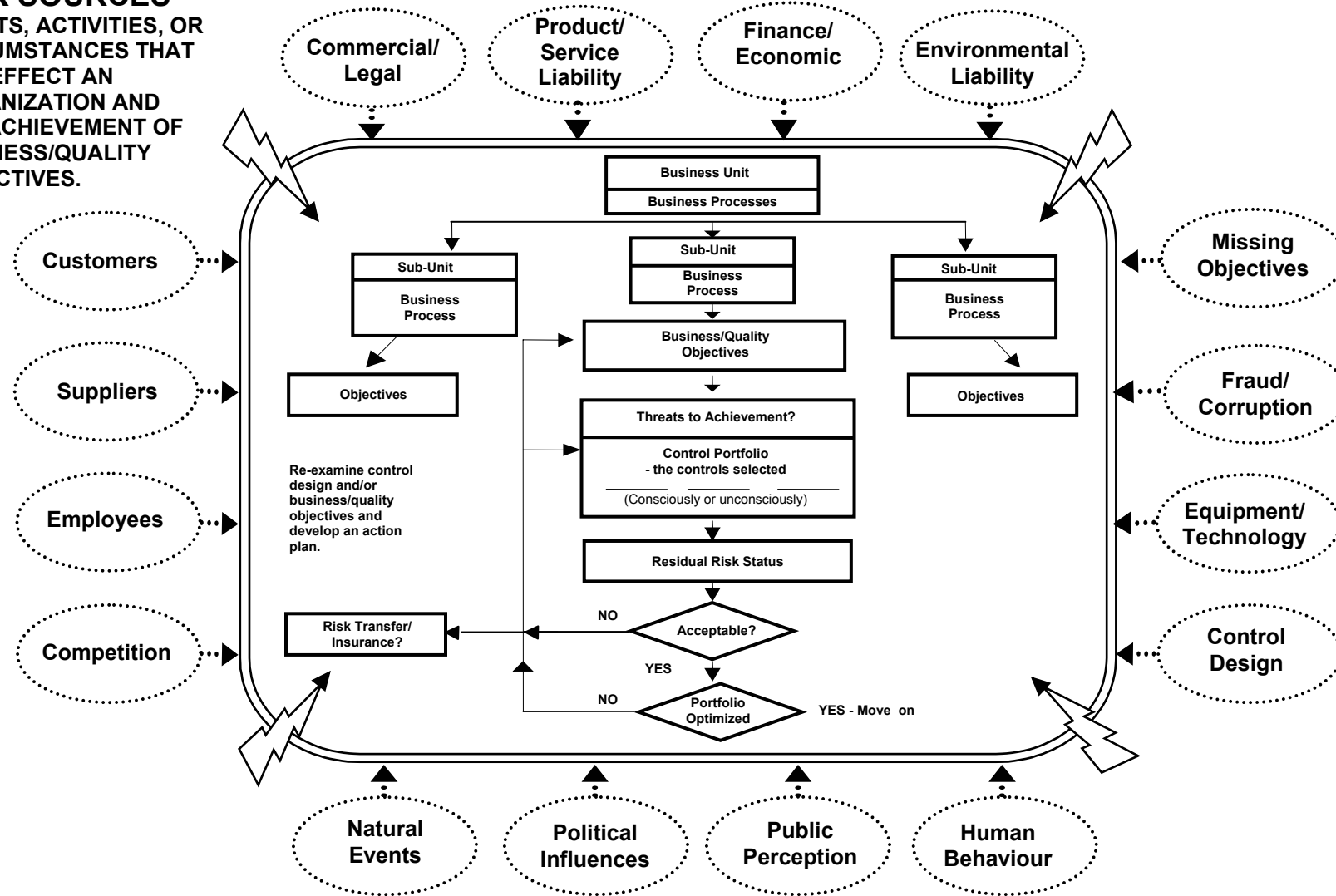
The paradigm shift from direct report auditing to attestation auditing has massive implications for the global internal and external audit communities and management. As the much larger population of business unit managers now being assigned to complete formal risk and control assessments grows, more business unit managers will show increased interest in the methods and tools used to cost effectively complete the task, including the new generation of automated tools available to continuously assess and monitor the status of risk and control. The shift in primary responsibility to formally assess and report on risk and control status from auditors to management is long overdue. The challenge will be the same as has been experienced many times before — the ability of human beings to cope with major change. Auditors, both internal and external, can help management with this transition or further delay and slow the changes necessary — but only if they themselves can cope with the major changes in methods and tools needed.

Tim Leech is Principal Consultant and Chief Methodology Officer at Paisley Consulting, the Cokato, Minnesota-based business accountability solutions software company. He can be reached at Tim.Leech@paisleyconsulting.com

RISK FITNESS QUIZ

The Business Risk Arena

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



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:

Control Assessment

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

SCORE:

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:

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:

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:

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:

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:

Regular Reevaluation

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

SCORE:

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:

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:

TOTAL RISK FITNESS SCORE:

APPENDIX 1: Sample Tests for Core Financial Controls

**PURCHASES,
DISBURSEMENTS
AND ACCOUNTS
PAYABLE**

- Invoices without matching purchase orders
- Invoice or purchase order quantities that do not match good received records
- Above average vendor unit pricing
- Duplicate purchase orders, invoices or payments
- Duplicate vendor numbers on vendor master file
- Vendors with P.O. box addresses
- Matches between vendor and employee name, address and telephone information
- Purchase orders and payments immediately under or in excess of approvers' limits
- Split purchase orders and payments that circumvent approval limits
- Invoice numbers sequenced unusually close within a given time period
- Charges to unused or dormant accounts
- Payments made to vendors with names that are similar to known vendors
- Duplicate and overlapping travel claims for the same period

**SALARIES AND
PAYROLL**

- Payroll amounts occurring for terminated employees
- Unapproved changes in payroll and salary rates
- Pay rates and timecard hours beyond limits
- Payroll data that does not match personnel file data
- Duplicate employee names, addresses and telephone numbers
- Duplicate direct deposit information
- Invalid and duplicate social insurance or social security numbers
- Payroll entries with no deductions
- Persons on payroll with no address or telephone number information

SALES AND RECEIVABLES

- High value credit notes
- Unusual amounts of credit notes by issuer
- Duplicate invoices, credits or receipts
- Credits taken beyond discount terms of payment days
- Lost revenue from unpaid carrying charges
- Accounts with oldest activity
- Gaps in invoice sequences
- Non-standard favorable discounts or credit terms
- Customer accounts with no address or telephone information
- Activity on dormant or unused accounts
- Unusually favorable pricing

INVENTORY AND STOCK CONTROL

- Products with zero quantities or prices
- Negative receipt quantities
- Duplication descriptions or product numbers
- Costs greater than sale price
- Unusually high returns and shortages
- Delivery addresses matching employee addresses
- Unusually high inventory levels and low turnover rates

Excerpt from ACL White Paper: Controls Compliance & Continuous Monitoring, 2002.
Reproduced with permission from ACL.