

CONTROL & RISK SELF-ASSESSMENT:

The Dawn of a New Era In Corporate Governance

Tim J. Leech, FCA, MBA.

Note: This article was written in 1990. Various versions of this article have appeared in a wide range of magazines and periodicals since that time.

Picture This Scene.

The chief internal auditor has just finished delivering her annual report on internal control to the audit committee of the board. She has worked for many weeks drafting and redrafting her comments. A draft of the report has been discussed with the CFO and the CEO at the "no surprises" pre-meeting. The summary document covers the significant points raised in the thirty audits conducted during the year, reports on audit coverage against plan, and indicates audits planned for the upcoming year. She is proud of the work done by her department and feels that her staff have uncovered and reported a number of relevant concerns, and made many useful recommendations.

The chairman of the audit committee extends the thanks of the board for the work done by Internal Audit in the previous year and asks two final questions that legal counsel has suggested he pose. He inquires:

"Are there any other concerns or control issues that I should be aware of?"

"Are controls adequate?"

The chief internal auditor responds:

"I have reported on the issues of significance noted in the year that I think you should be aware of. Management has, for the most part, been very cooperative and has indicated that they will take the steps they consider necessary to rectify the deficiencies noted during our audits. Although we have noted some problems in the course of our audits, overall, controls appear to be adequate in the areas we have reviewed."

All appears well. It would seem that all parties concerned are fulfilling their responsibilities conscientiously and professionally.

Assessing the Status Quo

Are they really?

In this article I set out my reasons for concluding that boards of directors, officers, managers, and auditors that use the "**historical/traditional approach**" to control and risk management should be dissatisfied and actively searching for a more effective replacement.

Having presented my case for change, a new approach to corporate governance called CONTROL & RISK SELF-ASSESSMENT is proposed as a replacement for the historical/traditional approach. Control & risk self-assessment better serves the interests of management, shareholders and other stakeholders; may have a lower overall cost; is consistent with total quality concepts; and is more defensible in an increasingly litigious world.

What is the Historical/Traditional Approach?

You may be wondering just what is the "Historical/Traditional Approach". A comparative overview of the historical/traditional approach versus a new vision of control management for management and staff and for auditors is attached as Appendix 1 of this paper.

The historical/traditional approach can be summarized as any approach where primary responsibility for analyzing and reporting on internal control and risk is assigned to auditors and, to a lesser extent, to controller departments and outside consultants. The opening scene is fairly typical of the type of report provided to directors in organizations using this approach. Aliases for the historical/traditional approach include financial auditing, comprehensive auditing, value for money auditing, inspections, efficiency and effectiveness reviews, computer security reviews, operational auditing, special studies and other titles.

How Does This Approach Work?

In organizations using the historical/traditional approach auditors and consultants document and analyze the controls and procedures in the area under review. As the work nears completion the "control findings" are discussed with management. A report is then prepared outlining

what is "wrong", or "deficient", or "warrants improvement".

Recommendations on how to correct or rectify the problems or concerns identified are developed and included in the report.

Management is usually asked to formally respond to the point raised. A summary report of findings is normally prepared each year for the audit committee of the board.

Although this approach to control and risk management has been used for many decades, recent developments suggest that the approach's deficiencies are beginning to show.

The "New Expectations"

The report of the National Commission on Fraudulent Financial Reporting published in the U.S. in 1987, better known as The Treadway Commission, focused on the topic of control governance and the expectations gap. Two of that report's most significant recommendations were:

Audit committees should be informed, vigilant, and effective overseers of the financial reporting process and the company's internal controls.

All public companies should be required by SEC rule to include in their annual reports to stockholders management reports signed by the chief executive officer and the chief accounting officer and/or the chief financial officer. The management report should acknowledge management's responsibilities for the financial statements and internal control, discuss how these responsibilities were fulfilled, and provide management's assessment of the effectiveness of the company's internal controls.

This study resulted in a four volume follow-up report on internal control commonly known as the COSO report. Similar work on control oversight and governance are currently at various stages in Canada, Britain, and in other countries around the world. In spite of this flurry of activity and attention, key questions remain largely unanswered.

How can audit committees and management demonstrate that they are "effective overseers of internal control"? How will senior management provide stakeholders with an "assessment of the effectiveness of their organization's internal controls"?

Business Objectives

Before considering these questions, it is worth reflecting on the standard objectives for profit organizations:

1. Profitability and minimization of unnecessary costs.
2. Safeguarding of assets.
3. Avoidance of unintentional exposure to risk.
4. Prevention and detection of errors and irregularities.
5. Assurance that delegated responsibilities have been discharged.
6. Discharge of statutory and contractual responsibilities.
7. Reliable financial records and external reports.

In 1987 the Treadway Commission recommended that audit committees and management formally acknowledge to regulators and the public that they are responsible for internal control, assess the effectiveness of the internal controls in place in their organization, and conclude whether they are satisfied. There was particular concern that officers and audit committees take responsibility for objectives 2, 4, 6 and 7 listed above. Developments since that time have confirmed that regulators will increasingly demand representations on control governance processes.

More Auditors=Better Controls?

The historical/traditional approach to control and risk management utilizes auditors as the primary vehicle to analyze and report on the status of the objectives listed above. Regulators, and in some cases, customers, are now calling for external

auditors and registrars to attest that stakeholder requirements are being complied with. Companies that have not had internal audit departments in the past are setting them up. More auditors are being hired to analyze and report on value for money, internal control, and quality management systems. Outside consultants are often hired to analyze and provide recommendations on specific control areas such as quality, safety and the environment. Senior officers often point to the existence of a controller's function, the use of outside consultants, existence of policies and procedures, and the existence of an internal audit department when asked to explain how they have discharged their responsibility for control management and oversight.

So what's wrong with the historical/traditional approach?

The Weakness of the Historical /Traditional Approach

IT'S NOT WORKING

- The expectations of the public are not being met. Additional regulatory intervention is imminent. The savings and loan failures in the U.S.; the failures of two major banks and a trust company in western Canada; failures of large public companies in the U.K.; and the increasing concerns of regulators everywhere are all illustrations of the deficiencies of the historical/traditional approach.

IT MAKES THE PUBLIC AND MANAGEMENT BELIEVE AUDITORS ARE RESPONSIBLE FOR CONTROL

- The historical/traditional approach has created and reinforced the belief that auditors and consultants, not management and work teams, are responsible for assessing and reporting on internal control. We often hear testimonies to this misalignment of responsibility:

I don't understand how this could have happened. The auditors were just in and said everything was fine.

We had better clean things up. The auditors are coming and they like to see controls in place.

I think we have a problem with product quality in the ABC Division. I think we should call in some consultants to find out what's wrong.

The auditors should assist in the development phase and sign-off on the controls in the new system before it goes into production.

- Auditors have mistakenly taken great pride in being the main "control" experts. Managers and employees are rarely provided with any formal control and risk management training or asked to assess and report on their responsibility area(s).

IT'S NOT VISIBLE

- Senior managers and directors are, in many cases, not able to visibly demonstrate conscious management of their control systems. Directors and officers have been the targets of mounting litigation for years in the U.S. Unhappy stakeholders in other countries are increasingly launching legal actions that require officers and directors to prove that they have met their fiduciary duties with respect to the reliability of external disclosures, statutory compliance in areas as diverse as safety, pollution, tax withholdings, employment equity, social reform, and many other areas.

IT COSTS TOO MUCH/IT PRODUCES TOO LITTLE

- The historical/traditional approach is not as efficient or effective as it could be. The approach does not satisfy very well objectives related to reporting on, or improving, corporate efficiency or effectiveness, product quality and customer service; fraud prevention and detection; statutory compliance; or accurate financial reporting.

- Managers and work teams are often not committed to implementing recommendations developed by auditors or consultants. Audits frequently produce little meaningful change.
- Although many companies are spending hundreds of thousands, and sometimes millions of dollars each year on internal audit functions, few internal audit departments have explicit and clear end result focused objectives. Actual audit coverage each year is often less than 20% of the control/risk universe. Few effectiveness measures are used to evaluate success in achieving end result objectives.
- Few chief internal auditors make it clear to the Board and senior management the areas that have not been audited or reported on during the year that could impact on them.
- Emphasis on execution of audit process and audit plans rather than results has been the order of the day for many internal audit departments.

IT DOES NOT ENCOURAGE CANDID DISCLOSURE OF THE RISKS BEING ACCEPTED

- The approach suggests, quite incorrectly, that more control is always preferable to less. The approach does not encourage managers and/or work groups to candidly admit that they regularly accept varying levels of risk relating to their objectives as a result of efforts to maximize profits; limited resources, ignorance; politics; conflicting objectives; or other reasons. There is often an unfounded belief that an "adequate" level of control can be determined for all businesses, in all sectors, at all stages of an organization's life cycle. The harsh reality is that "adequate" control is often nothing more than one person's view of how much risk he, or she, is willing to take.

IT FOCUSES ON INSIGNIFICANT ISSUES

- The historical/traditional approach to control and risk management tends to focus on

formal accounting control mechanisms such as signature approvals, reconciliations, account analysis, card access systems, passwords, system edits, documentation manuals, policy compliance, etc. History and recent research studies tell us that other informal control mechanisms such as management integrity, ethical tone, training, management competence, morale, hiring practices, communication, objective setting, risk analysis, performance measurement, officer and management reward systems and the like are far more significant. Most major losses and director lawsuits are the result of failures or inadequacies of these "informal" controls.

IT ENCOURAGES REPORTING OF SYMPTOMS NOT ROOT CAUSES

- The historical/traditional approach to control appraisal focuses on, and reports, symptoms as opposed to root causes. Many internal audit reports and external audit management letters are often extensive lists of symptoms with little indication of what is causing the real control problems.
- Auditors are often reluctant to report on the real root causes of control and quality problems such as the absence of clear objectives, management competence, performance measurement systems, incentive and reward systems, organizational design, poor training and hiring practices, inadequate management reporting systems and other "sensitive" subjects.

IT CONFLICTS WITH TOTAL QUALITY CONCEPTS

- The conventional approach is not consistent with total quality/continuous improvement concepts. Total quality theory calls for minimization of inspection in all processes. However, in organizations using the historical/traditional approach, auditors continue to perform inspection based, direct report audits of systems and/or transactions. Managers and staff are often not expected to or rewarded for performing regular, systematic analysis of their control and risk management frameworks.

IT IS OBSOLETE

- As business environments and systems become increasingly complex and dynamic, the deficiencies of the historical/traditional approach noted in this paper are magnified. The move to a global economy, the frequency of mergers and acquisitions, and rapidly changing world and business environments and the increasing knowledge skill and expectations of workers all emphasize the weaknesses of the conventional approach.

What Criteria Must the New Approach Meet?

A "wish list" might specify that the new approach:

1. Reassign primary responsibility for control assessment and reporting from auditors and outside consultants to management and staff.
2. Integrate with total quality and continuous improvement concepts.
3. Restore the confidence of the public and regulators in the integrity of the external reporting and corporate governance processes.
4. Be more effective than the current approach in terms of results and cost.
5. Recognize the need to balance profitability and levels of acceptable residual risk.
6. Recognize the interests of a broader range of stakeholders including employees, government, lenders, customers, investors and the public at large.
7. Assist officers and boards of directors in visibly discharging their control governance responsibilities and provide an effective defence in the event of civil or regulatory attack.
8. Be, and be seen to be, a practical and useful tool that will assist management, work teams and auditors to better achieve all of their business/quality objectives.

CONTROL & RISK SELF-ASSESSMENT: The Dawn of a New Era In Corporate Governance

At this point you might be saying to yourself "Nothing in this world could possibly meet that wish list. If this guy thinks there is, he probably believes there really is a Santa Claus".

After eight years of development, experimentation and tests in public and private sector organizations around the world, the evidence suggests that there is a substantially better approach to control and risk management.

Control and risk self-assessment, a new approach being tested by organizations around the world corrects many of the deficiencies of the historical/traditional approach.

Control and Risk Self-Assessment:
A process that allows work groups to identify or refine the business and quality objectives that they should be fulfilling, while assessing the adequacy of plans and controls that are in place to meet those objectives.

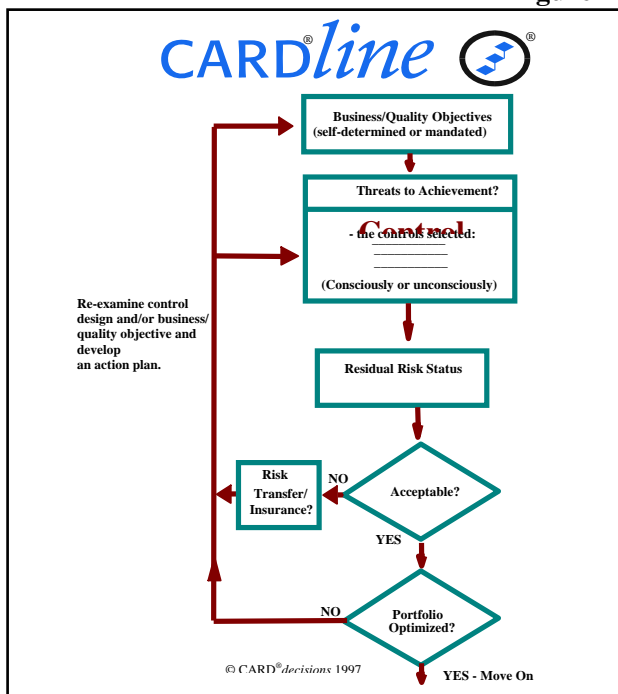
The underlying basis for self-assessment is best understood by referring to the overview of how control and risk management is managed shown below.

Control Design in Practice

Business and quality objectives exist for every private and public sector business entity. These may be self-determined or mandated. A partial listing of different types of objectives is shown on page 3 of this article. This list includes objectives such as minimizing costs, maximizing revenues, complying with the law, preventing fraud, safeguarding assets, complying with delegations from the board of directors, etc. These objectives must be customized, refined, and modified to be relevant to management. In most private sector corporations, the focus is on objectives related to revenue maximization and cost minimization. Public sector objectives focus on delivery of service, meeting departmental priorities, and cost effectiveness and efficiency.

Managers and/or work teams in private and public sectors, having arrived consciously or unconsciously at some set of business/quality objectives and priorities, assemble their "control portfolios" by consciously or unconsciously selecting specific control elements. They also choose, consciously or unconsciously, the quality and quantity of the control elements selected. Attachment 3 to this paper includes an illustrative listing of control elements. This Control Assurance & Risk Design menu ("CARD® menu") includes elements such as objective setting training, codes of conduct, performance management systems, hiring practices, communication mechanisms, and many others, in addition to more traditional financial controls such as segregation, signature authorizations, supervision and the like.

Figure 1



Illustrating the Core Model

To illustrate the core model, let's assume one of management's objectives is to minimize bad debts. A specific set of controls will be assembled that provide some level of assurance that this objective will be met.

Controls chosen might include establishing a credit function, developing a job description for the position, setting up a performance measurement system which specifically includes bad debt write-offs, buying or developing an accounting system that produces aged receivables, documenting follow-up procedures, establishing authority limits, performing customer background and reference checks, hiring a credit manager with extensive experience and qualifications, designing delivery slips and invoices to minimize the risk of having charges disqualified, etc.

Alternatively, an organization may choose not to employ any of these controls and accept a higher level of risk with respect to achieving this objective.

The core model can be applied to objectives related to customer service, product quality, compliance with the pollution laws and other statutes, cost minimization, achievement of program delivery standards, compliance with vendor agreements, compliance with business conduct codes, and other relevant business objectives.

Depending on the control portfolios selected, different "residual risk statuses" will result. Residual risk is the real or potential non-achievement of the business/quality objective. Residual risk status is a set of information that helps evaluate the acceptability of residual risk.

The Core Model is a Reality Today

This process of selecting and revising control portfolios in relation to stated or perceived objectives goes on daily in business and government. Information regularly surfaces on the level and specifics of residual risks which causes work teams, management, and sometimes even the board, to revisit and modify their control selections, and, in some cases, reconsider their business and quality objectives and/or attitudes towards risk acceptance. Unfortunately this process is often not done at a conscious level, and, is often not done optimally.

Self-Assessment Builds on Existing Skills

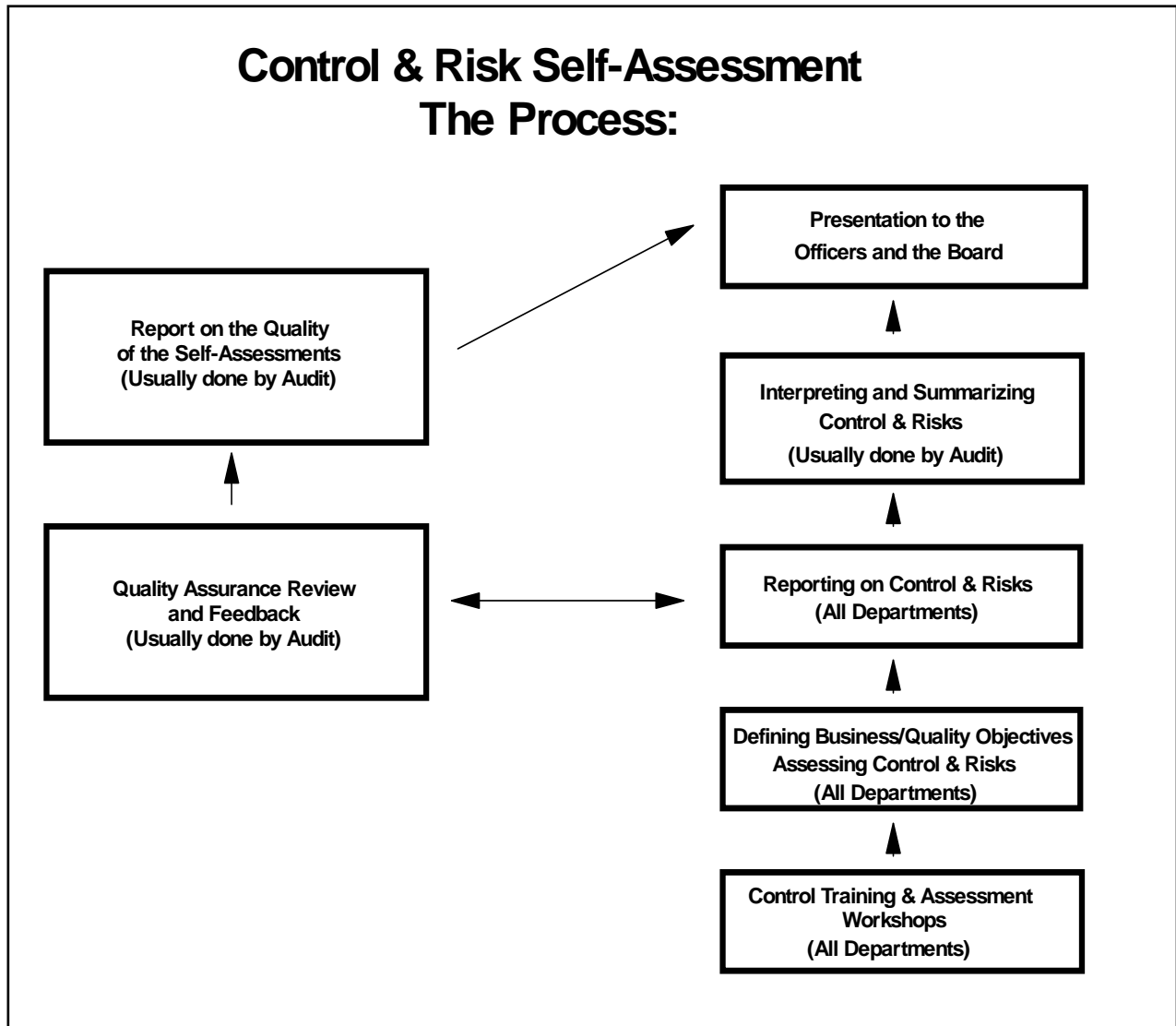
Control and risk self-assessment builds on existing control and risk management skills by providing work units and/or managers an opportunity to step back and identify or refine important business and quality objectives, identify and examine specific control selections, and consider the related residual risk statuses that result. Self-assessment also provides a tool managers and work teams can use to help them develop and maintain efficient and effective control portfolios that provide the level of risk that they, and their officers and directors, are prepared to live with.

The Self-Assessment Process

The self-assessment process starts with control training and assessment workshops for all staff. These workshops are necessary as many employees, including managers and officers, have had little, if any, formal control and risk assessment and design training. The assessment worksheets produced by work teams are eventually forwarded into a central consolidation point for synthesis and summarization. In a fully implemented system, work units are expected to update their assessments annually.

The control and risk self-assessment process takes most work units 2 or 3 days to complete in the first cycle spread over 4 to 8 weeks. The amount of time required is closely related to how well the unit has articulated their business/quality objectives. The time spent by the work groups integrates with performance measurement, planning, budgeting, and objective setting processes. The control and risk assessment and design skills learned are practical and applicable to all areas of the public and private sectors.

Figure 2



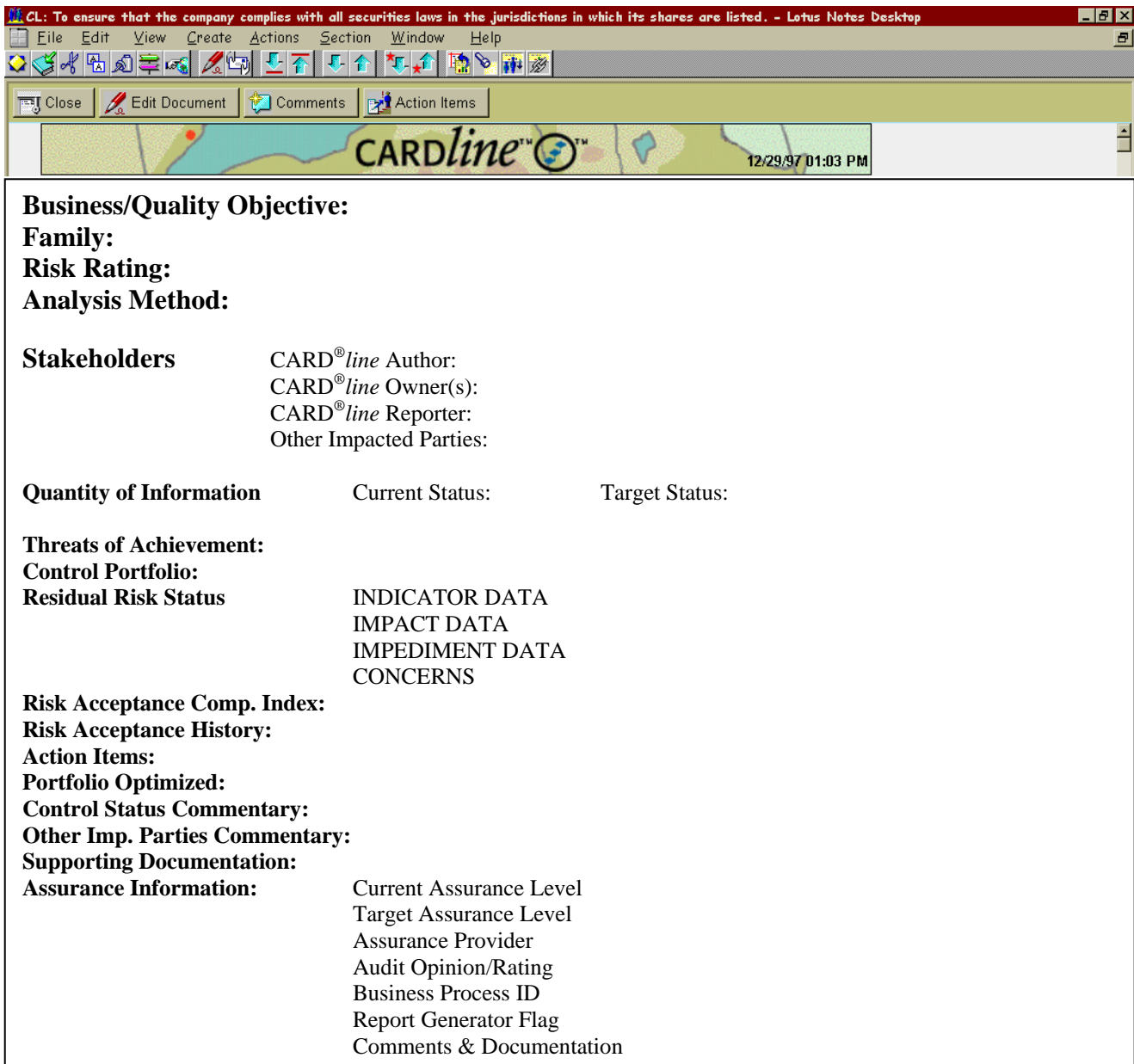
The Tools Used

THE CARD®line

The basic tool to assist management with the process is the Control Assurance & Risk Design line (CARD®line.) A template of the elements of a CARD®line is shown in Figure 3. Self-assessment requires that work groups specify their business/quality objectives; describe the threats to achievement and control elements, if any, that provide assurance that the objective will be achieved;

describe the residual risk status related to each objective; and decide whether they are willing to accept the current risk status. The process also requires the action plans, if any, the work unit intends to implement in cases where the work unit, or management personnel above them, are unhappy with the current residual risks status. Decisions on risk acceptance are formally considered and documented. A normal business unit might complete 15-30 separate assessments to cover their primary business/quality objectives.

Figure 3



Business/Quality Objective:

Family:

Risk Rating:

Analysis Method:

Stakeholders

CARD®line Author:
 CARD®line Owner(s):
 CARD®line Reporter:
 Other Impacted Parties:

Quantity of Information Current Status: Target Status:

Threats of Achievement:

Control Portfolio:

Residual Risk Status

INDICATOR DATA
 IMPACT DATA
 IMPEDIMENT DATA
 CONCERNS

Risk Acceptance Comp. Index:

Risk Acceptance History:

Action Items:

Portfolio Optimized:

Control Status Commentary:

Other Imp. Parties Commentary:

Supporting Documentation:

Assurance Information:

Current Assurance Level
 Target Assurance Level
 Assurance Provider
 Audit Opinion/Rating
 Business Process ID
 Report Generator Flag
 Comments & Documentation

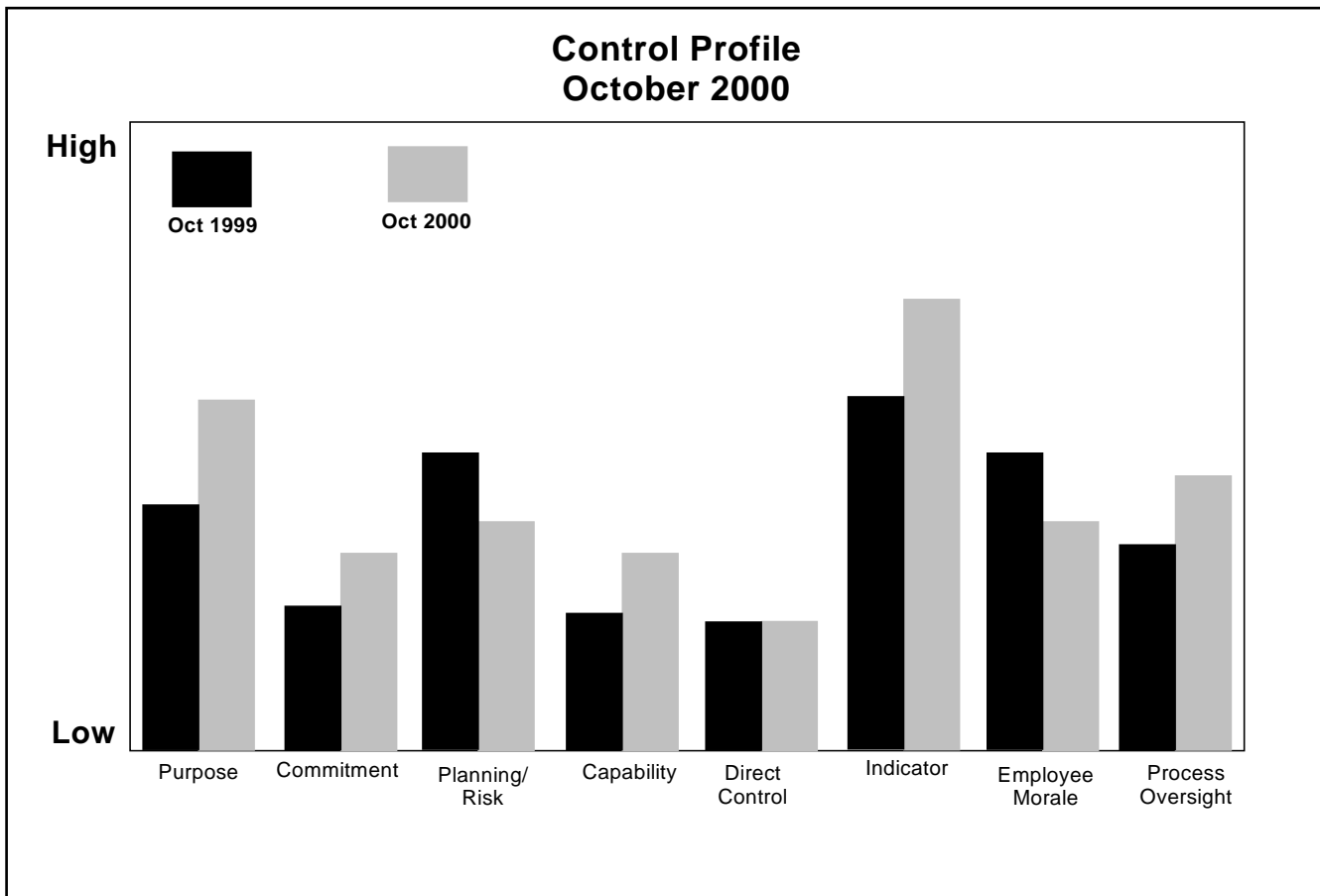
A Reporting Framework

A summary report on the status of control and risk can be produced periodically for officers and the audit committee by internal audit and another independent party with the aid of the work unit self-assessment reports, and other inputs such as consultants' reports, external disclosures and conventional audit results. The control framework shown in Attachment 2 and Attachment 3 to this paper illustrates one method of categorizing and reporting on the status of control in an organization.

Figure 4 below illustrates how a control profile graph can be developed for presentation to senior officers and the audit committee. Although this profile has been developed using the international Control Assurance & Risk Design model ("CARD® model"), national

frameworks such as COSO, CoCo or Cadbury can also be used. Other control and risk status reporting approaches are being experimented with by a number of North American organizations. The primary purpose of the report should be to communicate the status of internal control and risk and obtain consensus from senior management and senior oversight boards on the significant risk acceptance decisions being made by management and work teams. Control design decisions impact directly on customer service, cost control, revenue generation, safety, environment, fraud prevention, accounting and many other areas. The interrelationship between risks, control elements and the achievement of business/quality objectives should be explained and commented on in the consolidated annual report to the Officers and the Board.

Figure 4



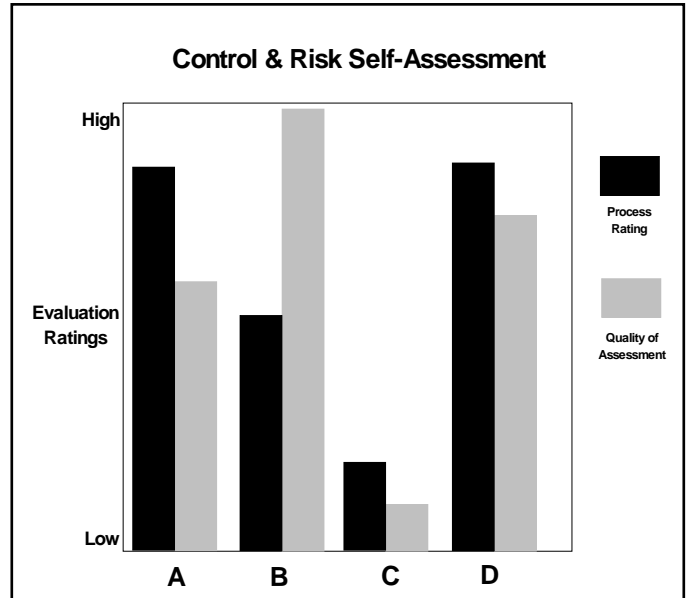
Quality Assurance - The Role of Audit

In a fully implemented self-assessment environment Internal Audit and/or external auditors can assess and report on both the process used to generate control and risk self-assessments, and the quality of the self-assessments. The quality assurance report includes commentary on the completeness of the objectives identified, the completeness and accuracy of the risk and controls descriptions, and the quality and completeness of the residual risk status disclosures. (Note: This is not a report on control weaknesses or deficiencies, but rather a report on the quality and reliability of the self-assessments produced by the work units).

Candid and complete disclosure of the control in place/use and the risks being accepted is rewarded with high ratings. An example of this type of report is shown in Figure 5.

Self-assessment quality assurance reviews can be done by internal audit, external audit, specialized consultants hired by management or the board of directors, or by combinations of environment, safety, quality, and other in-house specialists.

Figure 5



THE BENEFITS OF CRSA:

TO THE CORPORATION

Control and Risk Self-Assessment:

- Integrates risk, control and quality management.
- Integrates with self-directed team initiatives.
- Provides comprehensive coverage of all relevant objectives and areas of the company each year including important issues related to service, product quality, business ethics and social responsibility.
- Incorporates all inputs including those provided by management and staff, the results of conventional audit work done during the year and other sources such as verifiable public disclosures and reports from consultants.
- Provides balance and perspective. Control improvements and problems are both discussed and highlighted.
- Enhances accountability.
- Enhances communication at all levels.
- Makes control understandable.
- Is theoretically defensible. The process is simple in concept yet can be applied to the most complex and technical control/quality issues.
- Results in higher levels of commitment to improve.
- Responds to the expectations of regulators, shareholders, and the courts.
- Realigns responsibility for managing control and quality and places the responsibility squarely with management and staff.
- Has the potential to reduce the cost of internal audit and other specialists and produce better results, or product vastly superior results, with the same resources.

TO EMPLOYEES AT ALL LEVELS

Control and Risk Self-Assessment:

- Provides an opportunity for employees to contribute their knowledge and skill and assist their organization to survive and prosper.
- Provides an opportunity to employees who take pride in their work and/or their organization, to participate in the problem solving and decision making processes.
- Provides employees with portable control design and management training that is useful in virtually any business setting in the public or private sectors.
- Provides a forum to contribute ideas and suggestions to correct problematic and/or high risk areas that have been a source of personal annoyance or concern.
- Provides a vehicle to identify, discuss, and seek feedback on real or perceived gaps between what is being said by senior management and what is actually being done.
- Provides a vehicle to discuss and clarify unit business/quality objectives, minimizing frustration and wasted time and effort.
- Provides a vehicle to identify impediments beyond their control which are contributing to problems the unit is experiencing.
- Provides a vehicle to seek formal management endorsement of the risks that the group, and/or individual staff members are sometimes forced to take, or believe they are forced to take, in their day to day work. This ensures that the risks and consequences that flow from these risk acceptance decisions are understood and shared by those above.

THE BENEFITS OF CRSA:

TO MANAGEMENT

Control and Risk Self-Assessment:

- Provides a bottom up feedback mechanism to communicate the existence and effectiveness of controls. Departments who are not sure what their objectives are; who can't articulate the controls they have in place to achieve their objectives; and who have not thought of the current and possible risks and exposures; pose major risks to their organization, their Officers and Board and, quite often, the public.
- Provides a mechanism to consciously manage risk. Managers who have decided to install minimal controls and hope luck is on their side must be willing to defend their decisions and have their attitude to risk acceptance formally endorsed by senior management and the Board.
- Provides documentation on the level of control awareness among personnel, areas where controls have been increased or decreased, and action plans to deal with control concerns.
- Clarifies accountabilities and identifies inter-department dependencies.
- Provides an additional process for open two-way communication within the group, vertically up through the organization to the officers and the Audit Committee, and horizontally across departments within the organization.
- Focuses efforts on important issues and concerns such as values and ethics, environmental compliance, vulnerability to fraud, statutory compliance, as well as basic objectives related to profitability, cost minimization, customer service and product quality.
- Helps management to visibly fulfill their responsibilities with respect to control and quality management.
- Provides documented support for management representations on issues of particular concern to the Board such as financial reporting, environmental responsibility, regulatory compliance, fraud prevention and others.

TO INTERNAL AUDIT

Control and Risk Self-Assessment:

- Improves the efficiency and effectiveness of the department and radically increases coverage.
- Provides a powerful tool to supplement direct report audit work.
- Reduces conflict between auditors and auditees that are acting in good faith.
- Assists Internal Audit to address non- traditional areas such as customer service, product quality, environmental compliance, safety, fraud prevention and detection, and others.
- Makes it easier to attract quality staff.
- Facilitates training as it is primarily process driven, not knowledge driven.
- Produces a tangible and visible product each year for the Officers and the Board.
- Enhances objectivity and independence of audit by maintaining a strong oversight and reporting relationship.
- Improves planning and resource allocation. Departments that demonstrate that they really don't understand how they are managing control and quality, or appear to be less than candid or outright deceptive, warrant additional attention.
- Facilitates reporting to the Officers and the Board on the state of control and risk across the organization.

THE BENEFITS OF CRSA:

TO THE BOARD

Control and Risk Self-Assessment:

- Provides a comprehensive answer to many of the expectations of stakeholders and regulators related to financial reporting, environmental compliance, fraud prevention and detection, safety, regulatory compliance and other areas.
- Provides succinct, understandable information each year to the Audit Committee on the status of control and risk. Year over year changes are described along with management's plans if any, to address material risk areas.
- Provides a defensible and visible way of discharging control governance responsibilities associated with directorships and a defence in the event of civil or regulatory attacks.
- Utilizes a broader definition of internal control which produces valuable information on service and product quality, environment, safety, fraud related risks, and other key areas.

Are You Willing to Welcome The Dawn of a New Era?

Having worked with this new approach for over 10 years I have no hesitation in stating that the self-assessment approach to control and risk management is vastly superior to the historical/traditional approach used by most corporations and governments in the world today. I recognize however that the changes required in attitude, responsibility assignment, and corporate culture are significant. The transfer of primary responsibility for control assessment and reporting from auditors and consultants to management and staff is essential if the escalating expectations of stakeholders are to be met, and, if organizations are to survive and prosper in today's business environment.

Tim J. Leech, FCA
January 1998

Tim J. Leech, FCA, MBA, is a founding partner of Leech & Co GRC Inc. Leech was one of the original pioneers of the self-assessment approach developed at Gulf Canada Resources in the mid-1980's. He has continued over the last 20 years to develop, improve, and refine the implementation approach and self-assessment training tools for clients in Canada, the U.S., Europe, Africa, South America, Australia, and the Middle and Far East. Any questions on this paper, or the services that Leech & Co GRC provides should be directed to Tim Leech

Phone : (905) 337-3627

E-mail : TimLeech@leechgrc.com

CRSA: Defining a New Vision

Historical/Traditional

- Assign Duties/Supervise Staff
- Policy/Rule Driven
- Limited Employee Participation and Training
- Narrow Stakeholder Focus
- **Auditors and Other Specialists are the Primary Control Analysts/Reporters**

MANAGEMENT AND STAFF -
HISTORICAL/TRADITIONAL

- Are responsible for complying with prescribed methods and procedures.
- Receive limited training on control and quality assessment and design.
- Often consider auditors, consultants, and other specialists to be the experts on control and quality systems and design.
- Outside specialists are often called in to analyze areas where concerns and/or problems exist.
- Are often not allowed or encouraged at lower levels to analyze and make decisions relating to risk acceptance or control design.
- The personnel doing the work are often not directly responsible for selecting the controls used that help assure that their business/quality objectives are achieved.
- Candidness and full disclosure on the current state of control and risk is not encouraged and is often discouraged and punished.
- Fear and blame are sometimes utilized as strategies when problems surface.
- Internal control and total quality/continuous improvement are not integrated programs or concepts.

The New Vision

- Empowered/Accountable Employees
- Continuous Improvement/learning Culture
- Extensive Employee Participation and Training
- Broad Stakeholder Focus
- **Staff at all levels, in all functions, are the Primary Control Analysts/Reporters**

MANAGEMENT AND STAFF - THE NEW VISION

- Are accountable for designing and maintaining control systems that provide the desired level of assurance regarding the achievement of business/quality objectives.
- Are provided with adequate control assessment and design skills to properly fulfill their responsibility to report to Officers, the Board, and others on the current status of control, quality and risk.
- Consensus at all levels on relevant business/quality objectives and levels of acceptable risk is a primary goal.
- Candid disclosure of the state of control and the risks being accepted by the unit/organization is encouraged and rewarded.
- Accountability for business/quality objectives exists and is accepted by staff at all levels, in all functions.
- Employees at all levels are responsible for finding new and better ways to improve and optimize control portfolios to better achieve key business/quality objectives.
- Employees at all levels and in all functions continually reassess the adequacy and appropriateness of control choices and make adjustments when new information emerges regarding risk status, prioritization of objectives, and the control options available.
- Control and quality management are considered to be synonymous terms and are fully integrated programs/concepts.

CRSA: Defining a New Vision

Historical/Traditional

- Assign Duties/Supervise Staff
- Policy/Rule Driven
- Limited Employee Participation and Training
- Narrow Stakeholder Focus
- **Auditors and Other Specialists are the Primary Control Analysts/Reporters**

The New Vision

- Empowered/Accountable Employees
- Continuous Improvement/Learning Culture
- Extensive Employee Participation and Training
- Broad Stakeholder Focus
- **Staff at all levels, in all functions, are the Primary Control Analysts Reporters**

AUDIT - HISTORICAL/TRADITIONAL

AUDIT - THE NEW VISION

- A primary objective is to perform audits and report findings to senior management, and/or external stakeholders.
- Relations with auditees are sometimes adversarial.
- Auditors are viewed as the control "experts". Control assessment training is directed primarily to auditors and staff specialists.
- A primary audit objective is to report on whether units are complying with prescribed controls, procedures and standards.
- How auditors decide what constitutes "effective" or "adequate" control/quality management frameworks, and how much risk is considered acceptable by them, is often not explicitly disclosed.
- Auditors are measured primarily on execution of prescribed audit and review processes.
- Auditors receive limited training on control design concepts and ways to optimize control and quality frameworks.
- Internal auditors rarely examine and report on control frameworks related to customer service, product/service quality, safety, environmental compliance, and other "non-financial" areas.
- Quality auditors rarely examine or report on regulatory compliance, corporate ethics, fraud prevention and detection or the reliability of management representations to the Board and/or external stakeholders.

- Primary audit objectives are to:
 - raise the control and quality assessment and design skills of all staff;
 - provide accurate and complete information to the Officers, the Board and external stakeholders on the state of control, quality, and risk;
 - assist staff at all levels to design and maintain better, more optimal control and quality management frameworks.
- A key audit role is to foster more effective control and quality management through training, coaching, facilitation, and feedback to staff - unless quality assurance reviews suggest that representations by work units are misleading and the "good faith assumption" is not appropriate.
- Auditors help to ensure that the organization's business/quality objectives recognize a range of stakeholders, including customers and regulators, and that operative objectives are consistent with the corporate mission/vision.
- Auditors are measured on, and accountable for, achievement of the primary audit objectives noted above, not on excel lent execution of traditional audit processes.
- Auditors should be skilled and knowledgeable control design analysts and excellent technical auditors. These skills should extend to customer service, product quality, environmental compliance, fraud prevention and detection, and safety, as well as traditional financial objectives.

CARDmenu



1. PURPOSE: DEFINITION & COMMUNICATION

- 1.1 Definition of Corporate Mission & Vision
- 1.2 Definition of Entity Wide Objectives
- 1.3 Definition of Unit Level Objectives
- 1.4 Definition of Activity Level Objectives
- 1.5 Communication of Business/Quality Objectives
- 1.6 Definition and Communication of Corporate Conduct Values and Standards

2. COMMITMENT

- 2.1 Accountability/Responsibility Mechanisms
 - 2.1a Job Descriptions
 - 2.1b Performance Contracts/Evaluation Criteria
 - 2.1c Budgeting/Forecasting Processing
 - 2.1d Written Accountability Acknowledgements
 - 2.1e Other Accountability/Responsibility Mechanisms
- 2.2 Motivation/Reward/Punishment Mechanisms
 - 2.2a Performance Evaluation System
 - 2.2b Promotion Practices
 - 2.2c Firing and Discipline Practices
 - 2.2d Reward Systems - Monetary
 - 2.2e Reward Systems - Non-Monetary
- 2.3 Organization Design
- 2.4 Self-Assessment/Risk Acceptance Processes
- 2.5 Officer/Board Level Review
- 2.6 Other Commitment Controls

3. PLANNING & RISK ASSESSMENT

- 3.1 Strategic Business Analysis
- 3.2 Short, Medium and Long Range Planning
- 3.3 Risk Assessment Processes - Macro Level
- 3.4 Risk Assessment Processes - Micro Level
- 3.5 Control & Risk Self-Assessment
- 3.6 Continuous Improvement & Analysis Tools
- 3.7 Systems Development Methodologies
- 3.8 Disaster Recovery/Contingency Planning
- 3.9 Other Planning & Risk Assessment Processes

4. CAPABILITY/CONTINUOUS LEARNING

- 4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes
- 4.2 Self-Assessment Forums & Tools
- 4.3 Coaching/Training Activities & Processes
- 4.4 Hiring and Selection Procedures
- 4.5 Performance Evaluation
- 4.6 Career Planning Processes
- 4.7 Firing Practices
- 4.8 Reference Aids
- 4.9 Other Training/Education Methods

5. DIRECT CONTROLS

- 5.1 Direct Controls Related to Business Systems
- 5.2 Physical Safeguarding Mechanisms
- 5.3 Reconciliations/Comparisons/Edits
- 5.4 Validity/Existence Tests
- 5.5 Restricted Access
- 5.6 Form/Equipment Design
- 5.7 Segregation of Duties
- 5.8 Code of Accounts Structure
- 5.9 Other Direct Control Methods, Procedures, or Things

6. INDICATOR/MEASUREMENT

- 6.1 Results & Status Reports/Reviews
- 6.2 Analysis: Statistical/Financial/Competitive
- 6.3 Self-Assessments/Direct Report Audits
- 6.4 Benchmarking Tools/Processes
- 6.5 Customer Survey Tools/Processes
- 6.6 Automated Monitoring/Reporting Mechanisms & Reports
- 6.7 Integrity Concerns Reporting Mechanisms
- 6.8 Employee/Supervisor Observation
- 6.9 Other Indicator/Measurement Controls

7. EMPLOYEE WELL-BEING & MORALE

- 7.1 Employee Surveys
- 7.2 Employee Focus Groups
- 7.3 Employee Question/Answer Vehicles
- 7.4 Management Communication Processes
- 7.5 Personal and Career Planning
- 7.6 Diversity Training/Recognition
- 7.7 Equity Analysis Processes
- 7.8 Measurement Tools/Processes
- 7.9 Other Well-Being/Morale Processes

8. PROCESS OVERSIGHT

- 8.1 Manager/Officer Monitoring/Supervision
- 8.2 Internal Audits
- 8.3 External Audits
- 8.4 Specialist Reviews & Audits
- 8.5 ISO Review/Regulator Inspections
- 8.6 Audit Committee/Board Oversight
- 8.7 Self-Assessment Quality Assurance Reviews
- 8.8 Authority Grids/Structures & Procedures
- 8.9 Other Process Oversight Activities