

A RISK-BASED APPROACH TO ASSESSING INTERNAL CONTROL OVER FINANCIAL REPORTING ("ICFR")

NOTE: This chapter is a condensed version of an IMA discussion paper titled *A Global Perspective On Assessing Internal Control Over Financial Reporting* circulated for comments globally and filed with the SEC and PCAOB in September 2006. The full text can be found at: (<http://www.imanet.org/pdf/IMAmangementguidancetoSEC906.pdf>)

Institute of Management Accountants

Principal Authors

Tim J. Leech FCA·CIA·IT, CFE, CCSA
Jeffrey C. Thomson M.S.

A Risk-Based Approach to Assessing ICFR

Introduction

The SEC and PCAOB in the U.S. have repeatedly stressed that companies should apply a “top-down/risk-based” approach to assessing ICFR for SOX section 404. An IMA research project completed in 2006 titled *COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices* indicated that SEC registrants and their advisors and auditors have widely divergent views on how to actually complete a “top-down/risk-based” review of ICFR. To provide a solid basis for discussion on this topic the IMA drafted and issued for comment in September 2006 a paper titled *A Global Perspective on Assessing Internal Control Over Financial Reporting*. This chapter is a condensed version of that discussion paper. It describes a step by step approach to assessing ICFR that conforms to international risk management standards. The core assessment methodology this paper is based on is illustrated in Attachment 1.

Risk Assessment – Step by Step

Determine Key Stakeholders

When trying to solve a perceived problem it is important to take the time to identify and prioritize the key stakeholders that have a direct and indirect stake in solving it. The focus of the authors of The Sarbanes-Oxley Act of 2002 was clearly on investor protection. The stated purpose of SOX is:

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes.

All security regulators around the world that want to ensure the fairness and attractiveness of their capital markets share this goal. To date, only a few securities regulators have decided, at least at this point in time, that the frequency and magnitude of unreliable external financial disclosures in their jurisdiction by public companies is a big enough problem to their economies to warrant following the financial reporting regulatory approach implemented to date in the U.S.

In addition to capital market investors, venture capitalists, banks and other lenders, credit rating agencies, employees, pensioners, suppliers, customers, and many others rely to varying degrees on information contained in external financial disclosures. In addition to these parties, the senior management team of all organizations should care whether their internal accounting processes are producing reliable information for investors externally, and for resource allocations and strategic decision-making internally.

Establish the Risk Management Context

General

Agreeing that public companies should publish “reliable” financial disclosures is relatively easy. Agreeing just how reliable/error free the disclosures need to be and, most importantly, the consequences if they are not reliable, is far from easy. The fact that management’s motivation, remuneration, goals and aspirations can sometimes conflict with the needs of other stakeholders, at least in the short-term, further complicates the issue. **“Establishing the risk management context” simply defined means understanding the internal and external environment and the reasons why the primary overarching risk that auditor certified financial statements contain material errors should be mitigated.** Understanding the interface between management’s perspectives and motivations and those of regulators and outsiders, particularly the tolerance of both groups to the existence and/or potential of undetected errors in public disclosures is particularly important. It also means seeking agreement on how reliable or, stated another way, how unreliable/inaccurate financial statements can be and still meet the needs of relevant stakeholders. This information has major cost implications.

Risk Criteria – Big Picture Corporate Level

A primary goal of securities regulators is that public companies produce timely and reliable financial disclosures. The term “risk criteria” is defined in AS/NZ 4360 and the ISO Guide 73 *Risk Management Vocabulary – Guidelines for use in Standards* as “the terms of reference by which the significance of risk is assessed”. In this discussion draft the **key macro level risk** is that the financial statements are not reliable or, stated another way, **auditor certified financial statements contain undetected material errors in account balances and/or note disclosures.**

Important risk criteria at the big picture corporate level include the following:

1. **Implications to the company’s credit rating.** All of the major credit rating agencies have published papers in more or less detail on their attitude to control weaknesses disclosed under the current U.S. SOX regime. What they have not stated is how they obtain similar information in countries that do not require management and/or auditors make specific representations on ICoFR effectiveness, disclose material weaknesses in ICoFR, or the amount of rework of the accounts generated by the external audit. It is clear that the credit rating agencies do consider the track record of companies that have had to issue restatements of their financial statements and the reasons why these situations have occurred. One credit rating company, Moody’s, has gone so far as to categorize SOX material control weaknesses as “Category A” and “Category B” issues. When a Moody’s Category A control weakness is disclosed they have stated they aren’t particularly concerned because they believe that external auditors can effectively “audit around” the problem. However, when what Moody’s calls a Category B control weaknesses is disclosed they consider these situations to be serious because they “question the ability of the auditor to effectively “audit around” a Category B weakness”.
2. **Implications to the company’s reputation.** Companies are increasingly concerned whether the market views its financial disclosures with some significant level of distrust and/or disbelief. When this situation occurs it reflects badly on the issuing company’s senior management and board, as well as the external auditor that certifies the company’s financial statements.

3. **Implications to the company's cost of capital.** The trust and reliance lenders place in management and management representations, and the "risk premium" lenders assign to an organization is often linked to the company's track record of issuing reliable audited financial statements. There is preliminary evidence that at least some lenders are starting to take an interest in information on ICoFR, but it is also likely fair to say that lenders have not shown high levels of interest in the current state of a company's ICoFR. It is important to note however that the attitude of credit rating agencies does directly impact on the views and decisions of lenders and investors.
4. **Personal implications to senior executives and board members.** The U.S. has shown the most zeal so far in punishing executives that have knowingly and/or negligently allowed their companies to issue false or misleading financial statements. The evidence in the U.S. is seen in the jail sentences being handed down, corporate and personal fines being levied, the legal threat of requiring bonuses be forfeited, civil actions being launched, and more. The attitude of the boards of directors of U.S. listed companies towards unreliable financial statements has been variable. Regulators in countries other than the U.S. have, as a general statement, not shown the same level of focus in this area. It is important to note that at least some companies that have a track record of unreliable external disclosures are experiencing difficulty attracting high caliber senior executives and board members, particularly CFOs and audit committee members, and having to increasingly pay a premium to attract them because of the potential personal implications.
5. **Audit firm resignations/refusals.** A number of public companies have, for all intents and purposes, been "black-listed" by the big four accounting firms who have resigned or refused their business because the integrity and/or reliability of their accounting controls is questionable. These companies must resort to using lower tier audit firms willing to accept their business that have higher risk tolerances for their audit opinions. Situations like this can, in turn, impact credit ratings, cost of capital and share price.
6. **Impact on the company's share price.** Research in this area is still at a very early stage with somewhat inconsistent results. To date, the only country that has mandated public disclosure of the specifics of material weaknesses in ICoFR detected by management or auditors is the U.S. It isn't at all clear at this point that investors are discounting the price of shares in companies listed in countries that do not require disclosure of the type of information on ICoFR currently mandated in the U.S., and there is at least some evidence that absence of information on ICoFR has no impact or very limited impact on share price. A May 2006 comment paper issued by the Fédération des Experts Comptables Européens on the topic of management reporting on ICoFR reports "There is no evidence of demand for public reports on effectiveness of internal control in Europe" (Section 2 General Comments). This is an area that warrants considerable research to determine how markets react to the absence of information on ICoFR from management and/or external auditors.
7. **Personal philosophy of the company's CEO, CFO and Board of Directors.** The "tone at the top" is regularly cited as key to the issue of reliable external disclosures. The general tolerance of CEOs, CFOs and boards of directors to unreliable external disclosures and the way they personally react when evidence emerges to contrary is a key risk criteria in this area. It is important to note that even companies with excellent tone at the top can suffer instances of materially wrong financial statements because of the inherent limitations of internal control and the fact that some level of risk must be accepted to make a profit and stay in business.

8. **Likelihood External Auditor Opinion on Financial Statements is wrong.** There is a strong implicit assumption in the current U.S. SOX rules that external auditors will render less incorrect audit opinions when they are equipped with better information on the state of ICoFR. This would imply that external auditors should, on balance, have a higher audit opinion failure rate in countries that have not endorsed "SOX-like" rules related to ICoFR. This is a major consideration in the debate over the cost/benefit of the SOX regulatory regime in the U.S. that warrants serious research to prove or refute the assumption.

Risk Criteria – Subsidiary Level

A large percentage of companies, even smaller public companies, have one or more subsidiaries that are consolidated to form the financial disclosures filed with securities regulators. The degree of autonomy and the reporting lines of the personnel responsible for accounts and financial statements of these companies can vary widely. Some of the key risk criteria that impact on attitudes of executives in subsidiaries include:

1. Importance attached to reliable financial statements and accounts by head office. The overall attitude towards undetected errors in accounts at the subsidiary level is communicated in a number of important ways. This includes the importance to reliable accounts and effective ICoFR in job descriptions, the link to reliable accounts and ICoFR to compensation/reward/punishment systems, the rigor of analysis and questions posed by the head office consolidation team to the accounting personnel in subsidiaries, the interest of head office in the frequency and magnitude of errors detected by the external auditors in the course of their audit, the existence and competency of any internal audit function that exists, and others.
2. Personal implications to controllership and local operating management in terms of bonuses and promotions when conscious and/or negligent errors in the accounts filed with head office are identified.

Risk Criteria – Account/Note Disclosure Level

Although the risk criteria that exist at the corporate and subsidiary levels play major roles influencing behavior of senior controllership staff and form the macro level "risk context" for decision making, the risk criteria related to the individual accounts and notes that comprise the financial statements at the subsidiary and corporate levels are also important. These risk criteria impact on the attitudes of the staff that impact directly or indirectly on the reliability of specific accounts and/or note disclosures. The same basic elements listed above influence the perception of accounting staff regarding the importance or reliable financial disclosures.

Risk Rating & Risk Identification

When tackling the task of applying a true "top-down/risk-based" approach to assessing ICoFR, "assurance contexts" to be assessed must be established at multiple levels and risk rated before deciding where to invest the time and resources required to complete more detailed formal risk/control assessments.

As stated throughout this paper, the most important macro level assurance context for ICoFR is:

Ensure auditor certified financial statements, including the notes, are reliable.

This broad macro level assurance context should constitute the starting point for an entity's macro level risk/control assessment. **This section provides our specific views on how "top-down risk-based" ICoFR assessments should be defined for companies of all sizes to realize the value in their compliance programs.**

Since companies often have multiple subsidiaries and locations, hundreds, if not thousands and even tens of thousands of individual account balances, and scores of note disclosures, a universe of ICoFR assurance contexts cascading from the macro level context must be identified, risk-rated and the conclusions reached and documented for possible review by independent quality assurance staff. For U.S. listed companies the primary independent quality assurance agent for ICoFR is the external auditor. In larger companies the company's Internal Audit department and/or a SOX quality assurance team may also play important roles.

Risk Rating Assurance Contexts for ICoFR

A key step before embarking on more detailed granular risk/control assessments is to identify and risk rate the individual assurance contexts that support the macro assurance context at the corporate, subsidiary and account/note level. A sample of risk rating criteria that can be used when arriving at a composite risk rating on each of the assurance contexts that support the macro level or "parent" assurance context include:

1. Detected error history – external auditor
2. Detected error history – management detected after release of statements
3. Detected error history – management detected prior to release of statements
4. Complexity of accounting
5. Absolute dollar/unit of local currency value/impact of location/account
6. Detected error history – regulators/tax authorities/customers/others
7. Detected error history – internal audit
8. Detected/known errors in other companies in the same business sector
9. Amount of management judgment/subjectivity
10. Importance of account/location to security analysts
11. Importance of account/note disclosure to debt covenants
12. Susceptibility of account to fraud from insiders
13. Susceptibility of account to fraud from outsiders
14. Account/note linkage to the company's reward/compensation system

This is an area where additional research would help refine the accounts/areas in a company that would most benefit from more rigorous and formal risk and control assessment. Some companies have gone so far as to develop weighted numeric risk scoring systems that are then applied to their universe of ICoFR assurance contexts to decide the frequency and extent of analysis and testing each assurance context will receive. **The more these ratings are based on facts as opposed to unsupported guesses and subjective views, the better this system will work to actually ensure formal assurance resources are focused where they are most needed.** The ratings assigned at this stage have massive and ongoing cost implications because they should, if regulators allow it, influence the extent of risk/control design and control confirmation/operating effectiveness assessments going forward (i.e. the higher the risk rating the higher the assurance cost annuity). If the risk rating system is reliable it should allow for reduced risk and control assessment documentation and testing in areas that have low overall risk scores. These scores should be adjusted on an ongoing, real-time basis as new information emerges or, at a minimum, reassessed annually. Again, the goal is NOT to produce a one size fits all prescription;

rather, the goal is to suggest a system that can replace subjective ratings systems that are largely based on the absolute dollar size of account balances.

Identifying Risks to Assurance Contexts Selected for Additional Analysis

Once the assurance contexts to be assessed have been agreed and risk rated, the next step, using the terminology in AS/NZ Risk Management standard, for assurance contexts selected for additional formal assessment is risk identification - "the process of determining what, where, when, why and how something could happen". As a general statement this involves identifying, understanding, and documenting a list of real or potential situations at the "big picture" company level that could cause the non-achievement of the assurance context being assessed. This list should be comprehensive enough that it covers plausible, but not include "far-fetched", risk scenarios. A cardinal rule in risk-based assessments is "MISS THE RISK AND RISK BLOWING THE ASSESSMENT".

Techniques to build a "reasonable" list of plausible risks for an entity-level risk assessment for ICoFR and for more granular sub-elements include the following:

1. **Research and observation** – simply explained, this requires identification of actual situations that have already occurred in other similar public companies that resulted in materially incorrect financial disclosures. Reading newspapers, magazines and journals like Business Week and Compliance Week can produce a solid starting point. A number of relevant websites such as Audit Analytics (www.auditanalytics.com) that track all public companies that have had material control weaknesses and/or restatements of their financial statements are available to assist with this activity. The most dominant risk at the entity level that has emerged from recent scandals is "CEO/CFO/Senior executive instructs or otherwise influences staff to make entries that are fraudulent". Although this may seem to be a somewhat blunt assessment approach, there is no point denying that it was specifically this risk that resulted in SOX being enacted by U.S. Congress. Other common ones include "Compensation system, particularly the company's stock option plan, tempts senior level staff to falsify earnings", "CFO and/or accounting support staff are not current on GAAP", "Staff lack adequate knowledge of applicable federal/state tax law", "Lack of rule clarity how to deal with certain transactions/situations " and others. Every major financial statement misstatement that has been detected around the world, including Enron, WorldCom, HealthSouth, Parmalat, Nortel and hundreds of others, has a "cause of failure".
2. **Company Specific History** – as a company matures a large number of companies, as a result of internal analysis, the work of their external auditor, and the passage of time, realize that they have publicly issued financial statements that were materially wrong in one or more respects. Few companies in the world have continuously produced fault free disclosures prior to the audit/inspection process of their external auditors. Sometimes these situations result in public restatements and, in other situations, only the existence of internal knowledge on the part of one or more employees that one or more components of the publicly released financial statements were not, in fact, reliable. If these situations are analyzed and a cause of failure determined, it is generally easy to determine the key risks that caused the undetected error. For companies that, for whatever reason, place high reliance on the "end of the line" inspection ability of their external auditors, a key risk is always that "The external audit team assigned doesn't detect and/or require correction of errors that exist in the accounts". Again, the quality mantra of "building quality in, not on" (after the fact inspection) is critical in our view to the goal of cost effective assessments.

3. **Experience of senior level staff** – one of the advantages of growing older and gaining decades of experience in the accounting and control field, often in multiple companies, is that a person gains a broad experience base of what can go wrong and result in major errors in the accounts. This experience base can be used to identify plausible, company specific situations that have the potential to result in material errors in the financial statements.
4. **Industry specific scenario analysis** – this is a technique that can draw on information from the three methods above for inspiration, or be done using “pure imagination” of consultants and/or staff to produce plausible scenarios that could happen that the controls currently in use would not mitigate. The current reforms in the banking sector mandated by Basel II require that all major banks in the world demonstrate that they are regularly doing scenario analysis on the full range of operational risks, including those related to reliable financial statements. This technique is one that can help detect and prevent the next big disclosure disaster that has not happened yet elsewhere (e.g. the use of special purpose vehicles at Enron).
5. **Risk source analysis** – this technique uses a list of potential sources of risk to trigger ideas on possible scenarios that would cause a company’s financial statements to be wrong. An example of one risk source framework that can be used is included as Attachment 3. When using aids like risk source lists the general rule is they should be as granular as is necessary to pick-up the significant risks. A risk source list that contains 100 risks sources may not be as effective as one that is more summarized but still causes the assessors to identify a good list of significant risks. The example in this paper demonstrates a risk source framework that has a fairly limited number of risk source categories but has proven very effective as a risk identification tool.
6. **Industry “CHECK LISTS”** – although it is generally better to rely on the methods listed above to generate an industry specific/company specific set of risks, regulators have generally been willing to accept the use of “canned” risk and/or control assessment checklists provided by consultants, external auditors or other providers. When such aids are used care should be taken to try and validate that these assessment aids do, in fact, result in identification of the most probable, company/industry specific risks to reliable financial disclosures. When canned checklists have been employed and produce a conclusion that controls are “effective”, it is very important to monitor whether management and/or the company’s external auditors are still finding material errors in the draft financial statements. When external auditors find material errors after management and the external audit team has concluded controls are “effective”, it is at least prima-facie evidence that the assessment aid and/or current risk assessment process is inadequate.

A top-down based approach that starts with a macro level assessment on the assurance context of ensuring reliable auditor certified financial statements will often identify where the major holes in a company’s ICoFR system without the high expense and massive amount of time required to complete what many refer to as the “BOTTOM-UP” approach to assessing ICoFR. A BOTTOM-UP approach starts by documenting and assessing all the accounting processes that generate or support debits and credits regarded as material in the general ledger. More than a few companies in the first round of SOX did not start at the macro level assurance contexts and did not identify

and document the truly “key risks” that history tells us have regularly led to material financial statement errors and the mitigating controls in place to prevent them.

In addition to the type of top-down/entity level assessment described above that starts with the macro level assurance context of ensuring reliable auditor certified financial statements, the process of identifying risks for the more granular assurance contexts that must be assessed to arrive at a supportable conclusion on ICoFR must also be done.

Analyze & Evaluate Risks

Once the assurance context universe has been risk rated and plausible risks to the ICoFR assurance contexts selected for analysis have been identified and documented, the next step is to analyze and evaluate the specific risks. In cases where history clearly indicates a track record of internal or externally detected material accounting errors at the corporate level, or in specific company locations, subsidiaries, departments, and/or accounts and notes, this information needs to be carefully assessed and the relevant risks associated with the errors isolated for special assessment and evaluation treatment.

The process of analyzing risks includes assigning likelihood and consequence ratings to each risk. Generally an attempt should be made to produce these ratings before considering controls (inherent or gross risk ratings). Estimates can also be assigned for the net or residual risk that remains after considering controls although this is often difficult and costly if it is done using facts as opposed to purely subjective opinions.

Great care must be taken that the risk analysis process does not become too granular, costly and become an industry in itself. The end game is to decide which risks are not currently sufficiently mitigated given the organization’s tolerance to accounting misstatements (i.e. these are often identified as “red rated” risks). In real life people and companies frequently use an experiential, iterative approach that causes them to modify their controls after they are presented with tangible evidence that contradicts previously held views of the likelihood or consequence of a risk (e.g. the risk staff might forge signatures on sales contracts to earn a bonus in a quarter or fiscal year end gets mitigated after a major scandal where this occurs emerges). Using the risk identification techniques outlined in this chapter will help by generating risks that have already proven to be plausible and have, in fact, already resulted in material undetected errors in other public companies. In order to dismiss such risks as irrelevant, a company should be able to explain why their controls would mitigate the risk or be willing to state their current controls might not mitigate the risk and they accept the consequences.

Treat/Mitigate Risks

Treat Risks Using COSO 1992 Control Criteria

Using COSO 1992 for Control Criteria Centric Assessments

To comply with the requirement in current SOX regulations that assessments be done in accordance with a suitable control framework some companies annually, and sometimes even quarterly, have been completing a high level size-up of how their current controls compare to the type of control criteria described in COSO 1992. This approach is sometimes called the “control criteria centric” approach and it is done without explicit and direct reference to specific risks that threaten the macro level objective of reliable financial

statements. This approach involves taking the 5 primary COSO 1992 categories and sub-elements that comprise the categories and attempting to determine on a binary basis, whether the company currently demonstrates achievement of the COSO 1992 control elements for ICoFR.

To date, few, if any, companies have publicly reported material control weaknesses in their controls relative to any specific COSO control categories or sub-elements. The major challenge when attempting to use the COSO 1992 framework this way is that it was not written with the intent that it would ever be used for "pass/fail" assessments on a specific company's ICoFR effectiveness. The Malcolm Baldrige quality system in the U.S. administered by the American Society for Quality (one of the participating reviewers of this document) is an example of a framework that has been specifically developed to generate repeatable numeric assessments against the quality system evaluation criteria contained in the framework. It is important to note that the Baldrige framework does not define what a "passing" grade should be with respect to a company's quality management system, rather, in the spirit of continuous improvement, it defines quantitatively an organization's progress toward global benchmarks in various categories, categories that are refined and updated for relevance and predictability each year by Baldrige system administrators.

Whether a "control criteria centric" assessment approach that attempts to determine the degree a company conforms to control elements in COSO 1992 is what the SEC has in mind when they use the term "top-down" assessment is not known as of the date of issue of this discussion paper. It is not an approach that is currently mandated in PCAOB AS2. It is also not a "risk-based" approach (it is control criteria centric), but does reflect a "top-down" emphasis. This issue may be clarified in the new guidance for management expected in May/June 2007.

Using COSO 1992 for Risk-Based ICoFR Assessments

For companies using the COSO 1992 control framework as an assessment aid for a risk-based ICoFR assessment approach the following steps are recommended:

1. **Develop a universe of ICoFR assurance contexts** that starts with the macro level assurance context of ensuring auditor certified financial statements are reliable at the corporate level, and then moving downwards (i.e. "top-down" per the SEC) to include a macro level assessment in all significant subsidiaries that issue standalone financial statements, and on to defining assurance contexts for each of the line items and notes in external financial disclosures. The high-level summarizations line items in financial statements will then have to be further sub-divided to include assurance contexts for all significant GL accounts that comprise the financial statement line items. When grappling with what is a significant GL account or note the overriding decision criteria is encapsulated in the following question - Would a material error in the assurance context being rated result in stakeholders doing something they wouldn't have done had they known the truth? Additional assurance contexts will be required for reliability of IT general controls and can optionally be done separately for the assurance context of preventing fraud related financial statement misstatement, although the fraud related risk component can and should be addressed as an integrated element of the assessment done on all assurance contexts including IT general controls.
2. **Develop and apply a system to risk rate each of the subcomponent assurance contexts identified.** This step allows some percentage of the assurance context universe to be eliminated completely for additional formal assessment based on the risk rating generated or identified for reduced scrutiny. If the type of criteria proposed in this paper are used, even large account balances may be eliminated if

they have been error free (both internal and external) and have not been elevated based on other rating criteria such as vulnerability to fraud, industry analyst or debt covenant importance. Companies should agree the assurance context scoring system they develop with their external auditors, and local regulators may also provide input or even specific rules that must be followed. **How far down from the top level assurance context of assessing risks to reliable auditor certified financial statements companies must go, and be able to prove to outsiders that they have completed formal risk/control assessments, is a decision on which senior management, security regulators and external auditor standard setters should provide guidance because it has significant cost implications.** Although completing a robust risk assessment on the macro level assurance contexts of reliable auditor certified financial statements may provide 80 or 90% coverage of the major risks that have caused the type of major problems that led to SOX in the U.S., this may not be acceptable to one or more of the key players that input to the assurance context coverage decision, especially U.S. securities regulators and auditor oversight bodies. It is important to note that even 100% coverage of the assurance context universe including formal risk/control assessments on every account in the general ledger will not provide 100% assurance all significant residual risks that could lead to materially incorrect financial statements have been identified.

3. **Identify and analyze risks that threaten the assurance contexts selected for formal review.** For assurance contexts selected for additional formalized risk/control assessment using one or more of the type of risk identification methods outlined in this chapter identify relevant risks and evaluate the risks identified in terms of likelihood and consequence. **A five level numeric likelihood/consequence rating system is recommended to provide adequate but not excessive granularity. The key is to find a way to rank risks identified in terms of their likely impact on the assurance context.** Risks can be further analyzed in terms of risk source category, the availability and extent of statistical information available on likelihood and/or consequence of major risks, and other criteria. A major trend currently in the risk management field is to supplement subjective judgments on likelihood and consequence with facts and statistics whenever possible. A table with one of the more common systems used to assign "risk levels" based on various combinations of risk likelihood and consequence drawn from a publication titled Guidelines for Managing Risk In the Australian Public Sector is included below to illustrate the concept. Companies can alter the terminology used for likelihood and consequence or substitute simple numeric scores for the likelihood and consequence levels (i.e. 1 to 5), but should maintain the core principle of demonstrating that a reasonable attempt has been made to prioritize the set of risks identified. The main goal of this exercise is to attempt to sort risks in terms of relevance and potential impact to the ICoFR assurance context being assessed.

| Consequences | | | | | |
|--|-------------|-------------|-------------|-------------|-------------|
| Likelihood | EXTREME | VERY HIGH | MEDIUM | LOW | NEGLIGIBLE |
| ALMOST CERTAIN | severe | severe | high | major | significant |
| LIKELY | severe | high | major | significant | moderate |
| MODERATE | high | major | significant | moderate | low |
| UNLIKELY | major | significant | moderate | low | trivial |
| RARE | significant | moderate | low | trivial | trivial |
| SOURCE: Guidelines for Managing Risk in the Australian Public Sector, #22 October 1996 | | | | | |

4. **Identify important controls that mitigate risks with assessable risk levels.** Using the COSO 1992 control framework and the supporting COSO volumes that provide more details on the elements of each control category, identify, document and categorize important controls in place that mitigate the risks that have been assigned higher level risk level ratings. (NOTE: the “risk level” is the result of various combinations of likelihood and consequence.) How far down the list of risks identified that matching is done has significant cost implications. **Other COSO 1992 control sub-element “interpretations” or lists have been developed by companies, external auditing firms, and consulting firms,** however it is important to note that the five member COSO Committee has not formally endorsed any of the many summarized interpretations of the 1992 framework that have emerged over the past 14 years with the exception of their own 2006 COSO SPC guidance that defines 20 principles and sub-attributes. The view may be that as long as the approach is “COSO linked”, and companies attest in writing that they are ultimately using the core principles in COSO 1992, the use of “COSO 1992 interpretations” is acceptable to the SEC. Further clarification on this point in the upcoming SEC Assessment Guidance for Management would be useful.

Mitigating controls identified for the higher-level risks should be categorized to indicate the applicable COSO 1992 control category. This step helps support CEO/CFO representations that a ICoFR assessment has been done in accordance with a suitable control framework when national regulators require this representation be made. This is also a key step to support the need of U.S. listed companies to prove that an attempt has been made to aggregate control deficiencies to determine if, “collectively”, they constitute a reportable control deficiency. If the areas where deficient controls are identified *often* link to a specific COSO 1992 control category it may result in concluding that controls are not effective in accordance with that category of COSO 1992. To date, no guidance has been issued by regulators on the subject of how to do a control deficiency aggregation test related to a control model such as COSO 1992 and PCAOB AS2 provides no specific guidance for auditors on this issue. It is important to note that low likelihood/massive consequence risks should not be ignored since many of the major instances of false or misleading auditor certified financial statements would fall in this category.

Determine whether controls described in step 4 are, in fact, being done as described. The primary goal of this step is to confirm that controls that have been identified during the risk and control documentation step as mitigators to specific risks are, in fact, being done as described. A simple step that is sometimes overlooked resulting in significant unnecessary costs is to simply ask the person or persons most directly responsible for the control whether the control has been done as described during the period being reviewed. In cases where the control “owner” or “sponsor” indicates the control was done as described, there may be a need, depending on the level of assurance required, to have one or more independent groups verify that the employees with direct responsibility for the control are telling the truth. This step is sometimes called independently verifying “operating effectiveness” or simply “control confirmation.”

A simple example of the process of identifying a macro level risk during a top-down assessment and identifying related mitigating controls follows:

RISK: Senior management (CEO and/or CFO) override controls and improperly manipulate/falsify financial statements – Risk Level rating assigned by management: Significant (i.e. extreme consequence combined with a moderate likelihood). (NOTE: the

company's external auditor might have a very different view on likelihood based on past behavior of management related to earnings management.)

MITIGATING CONTROLS: CEO/CFO Hiring Practices – COSO Category Control Environment, Audit Committee Oversight – COSO Category Control Environment, Confidential concern reporting line – COSO Category Information & Communication, Internal Audit – COSO Category Monitoring, External Auditor audit of financial statements – COSO Category Monitoring.

If the goal is to identify only one or two of the controls as a “key” control to limit the amount of regulatory imposed management and auditor control testing this is a very difficult and subjective decision. In the U.S., the likely key control candidates would be audit committee oversight and confidential concerns reporting mechanism (the company’s “hotline”) because the U.S. rules do not allow management to view the external audit as a control. In other countries that do not require management reporting on ICoFR and are still tolerant of material undisclosed levels of financial statement adjustments as a result of the work of the external auditor, the key control currently for this particular risk is probably the external audit of the financial statements and the quality of audit staff assigned to do the audit.

Steps would also have to be taken to determine that the controls documented actually were done/completed as described.

The controls currently in use result in some level of effectiveness relative to the assurance context being assessed. **Methods to identify the current residual risk status being produced by the controls in place for any given assurance context are outlined later in the chapter.** We view the step of identifying and evaluating residual risk status as significantly more important than massive amounts of independent control verification and testing.

Treat Risks Using CARD[®] model, A COSO Linked Framework

Attachment 2 to this discussion draft is an example of a public domain control model that the IMA will be using for ERM skills training called CARD[®] model that is linked to the original COSO 1992 and COSO SPC frameworks and has been referenced in a number of Institute of Internal Auditor and IMA publications. CARD[®] stands for Collaborative Assurance & Risk Design. It uses 8 control categories versus the 5 primary control categories in COSO. This model puts higher importance on “Commitment”, “Indicator/Measurement”, and “Process Oversight” controls relative to the attention given in COSO 1992. Each of the eight control categories in this model relates to an element of an organization’s control framework. Beneath each of the 8 categories there is a “menu” of the specific control elements that an organization could use to achieve the core control category objective. (see Attachment 3) Supporting each sub-element of control is a “trigger” question available from the IMA that helps people understand the purpose of the control. This framework has been developed and tested over the past 20 years and draws on COSO 1992 and the other national frameworks covered in this paper, as well as the Malcolm Baldrige Quality framework, and other control models including the Modern Comptrollership framework developed in the Canadian public sector. All control elements in COSO 1992 and COSO SPC frameworks are included in this COSO linked framework although they are organized under different control category headings.

This reference aid can be used to identify existing or possible controls available to mitigate a particular risk and indicates to readers at a glance the mix of the type control design

elements that are currently being used (e.g. a control design that lacks Measurement/Indicator controls or Commitment controls).

An illustration of how this CARD[®] *model* methodology can be used for the same example used in the COSO 1992 section follows:

RISK: Senior management (CEO and/or CFO) override controls and improperly manipulate/falsify financial statements – Risk Level rating assigned by management: High (i.e. extreme consequence with a moderate likelihood).

MITIGATING CONTROLS: CEO/CFO Hiring Practices – Element 4.4 Capability and Continuous Learning, Audit Committee Oversight – Element 8.6 Process Oversight, Confidential concern reporting line – Element 6.7 Indicator/Measurement, Internal Audit reviews – Element 8.2 Process Oversight, External Auditor audit of financial statements – Element 8.3 Process Oversight, 6.1. Results and Status Reports/Reviews.

The CARD[®] *model* framework was specifically designed to help people with the task of identifying the controls currently in use that mitigate specific risks identified to a given macro or micro level assurance context and help them to understand what controls they could use if current performance or error rate for any assurance context is unsatisfactory.

Treat Risks Using COBIT/ISO 17799/ITIL

Common risks that emerge when identifying and evaluating risks to the overall reliability of the financial statements and the line items and notes that comprise them relate to the following broad areas:

1. Software program do not correctly calculate/allocate/handle transactions that impact on the financial statements.
2. Accidental or intentional unauthorized/inappropriate modifications to software programs.
3. Unauthorized/inappropriate/fraudulent modification of data in the system that is used to calculate/process accounting entries.
4. Unauthorized/inappropriate/fraudulent creation and submission of data to the accounting system.
5. Spreadsheets used to feed or produce accounting entries or notes are inaccurate/unreliable/not secure.

The controls that mitigate the type of risks identified above are most generally called IT general controls.

For U.S. listed companies PCAOB AS2 mandates that external auditors must independently assess IT general controls that impact on the financial statements when completing SOX 404(b) assessments. In the absence of any guidance from the SEC on the subject management has, by extension, used the general IT controls assessment requirements outlined in PCAOB AS2 related to IT general controls. The area of IT general controls external auditor evaluation has been an area that has attracted a high number of complaints with a common theme that registrants believe that their external auditors and/or consultants have required an excessive amount of work on this dimension of control resulting in high ongoing costs.

A precedent setting paper calling for convergence and integration of competing IT standard setting bodies titled **Aligning COBIT, ITIL and ISO 17799 for Business Benefits: A Management Briefing from ITGI and OGC** suggests that:

*Every organization needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. All three can play a very useful part – COBIT and ISO 17799 helping to define **what** should be done and ITIL providing the **how** for service management aspects.*

Treat Risks Using the OCEG Foundation Framework

For risks that relate directly to business ethics and the ethics of individual senior executives a framework that has been developed by the Open Compliance & Ethics Group is particularly relevant. It provides considerable detail on tangible methods companies can use to mitigate specific ethics and legal compliance risks. Considerable work and input has gone in to the development of this framework and it has undergone a very rigorous exposure and comment process. This framework is particularly relevant to the type of risks that caused SOX to be enacted in the U.S.

Identify, Assess & Report On Residual Risk Status

Once the assurance contexts to be assessed have been decided on, relevant risks identified, prioritized and evaluated, and the mitigating controls for those risks identified and documented, the last step is determining the current “Residual Risk Status”. **This sequence can also be reversed wherein a company monitors the residual risk status for a given assurance context and only completes a formal risk and control assessment to determine the cause when the residual risk status information indicates a problem.** The option of monitoring key performance indicators and key risk indicators prior to completing full assessments is not available to U.S. listed companies that must comply with the current SOX regulations for sections 302 and 404.

Residual risk is defined in AS/NZ 4360 Risk Management standard as “the risk remaining after implementation of risk treatment”. For ICoFR this is the risk that remains financial statement line items and/or notes are, or could potentially be materially wrong in whole or part.

Residual risk status is a collection of information that helps management and audit committees decide whether the residual risk related to the goal of reliable financial disclosures is, or is not, acceptable.

Types of Residual Risk Status Information

Concerns – (also known as issues or review findings) these are real or potential situations that have been identified where the current controls in place do not, or might not, mitigate one or more risks in whole or part. Management must then decide whether the situation represents a Concern-acceptable or a Concern-unacceptable. In many companies concerns explicitly or implicitly deemed acceptable are often not documented. An example is an accounting balance that involves estimates that requires a high level of judgment and experience. A risk is inexperienced staff making the estimates make serious mistakes. The current employee that is making the judgments is new to the industry and the position and lacks knowledge and experience. This creates a residual risk concern. In the absence of adding other compensating controls this produces a residual risk concern that is either

acceptable or unacceptable to senior management. We encourage companies to document residual risk concerns that they elect to accept at a point in time because new information may emerge and a concern that was acceptable at a point in time may not be down the road because of differences in circumstances and/or risk tolerance. It is very important that external auditors are made aware of situations where the controls may not mitigate one or more risks that threaten the reliability of one or more accounts or notes. In some percentage of these situations they can elect to increase the substantive testing work they do to confirm the reliability of the accounts in question with the end result that the goal of reliable auditors certified financial statements is still achieved. In other situations, it may not be possible or be very expensive to reduce the risk of financial statement error. An example of this type of situation is when accounting program change controls or data access controls are unreliable and the impacted account balances are not amenable to reliable external auditor confirmation (e.g. whether a program functioned consistently and correctly throughout an entire accounting period without unauthorized changes). Auditors are placed in a very difficult situation when general IT controls are seriously deficient because audit theory dictates that extensive work must be done to achieve a high level of audit assurance.

Indicator Data – this is information about how well a given assurance context is being met. (NOTE: This is not whether controls were performed as described but rather the degree to which the controls are actually mitigating risks to the assurance context being assessed.) An ICoFR example is a company discloses in their 10K that they have a profit before tax of \$100 million. Their auditor has given a clean opinion on the financial statements and an opinion that ICoFR is effective in accordance with COSO. It is subsequently determined that \$30 million of inventory shown on the balance sheet does not exist and the financial statements for the period must be restated. The assurance context is that inventory balances are reliable. The new information that has surfaced helps illustrate how well the controls worked to mitigate one or more risks. For an individual account balance indicator data could be a material error discovered by the external auditor after management has signed off on the financial statements, or information that emerges in a subsequent accounting period and management is now aware that statements filed with the SEC contained some level of material error. Other less obvious examples might be an abnormal number of credit notes that must be issued in the first quarter of the year because the customers deny that they actually ordered the goods that were included in the prior period's sales. This is indicator data that the assurance contexts of reliable accounts receivable and sales were not met in part for that year-end.

Impact Data – this is information that helps decision makers understand the consequences that will or could flow from specific errors in the company's financial statements. Errors that impact only on classifications within similar balance sheet or income statement classifications are generally not as serious as balance sheet errors that impact on the income reported. Errors in some balance sheet accounts or notes to the financial statements however could have an impact on debt covenants triggering a loan repayment, credit rating review or other major consequences. An example would be errors in a note disclosure that is used extensively by security analysts that track a particular industry. The likely impact of financial statement errors is an area that is complex with few hard and fast rules. Investors sometimes appear to have fairly high tolerance to certain types of accounting errors but react drastically to others. A related area that is currently being debated on a global level is what type and/or size of error should result in a restatement of prior period financial statements.

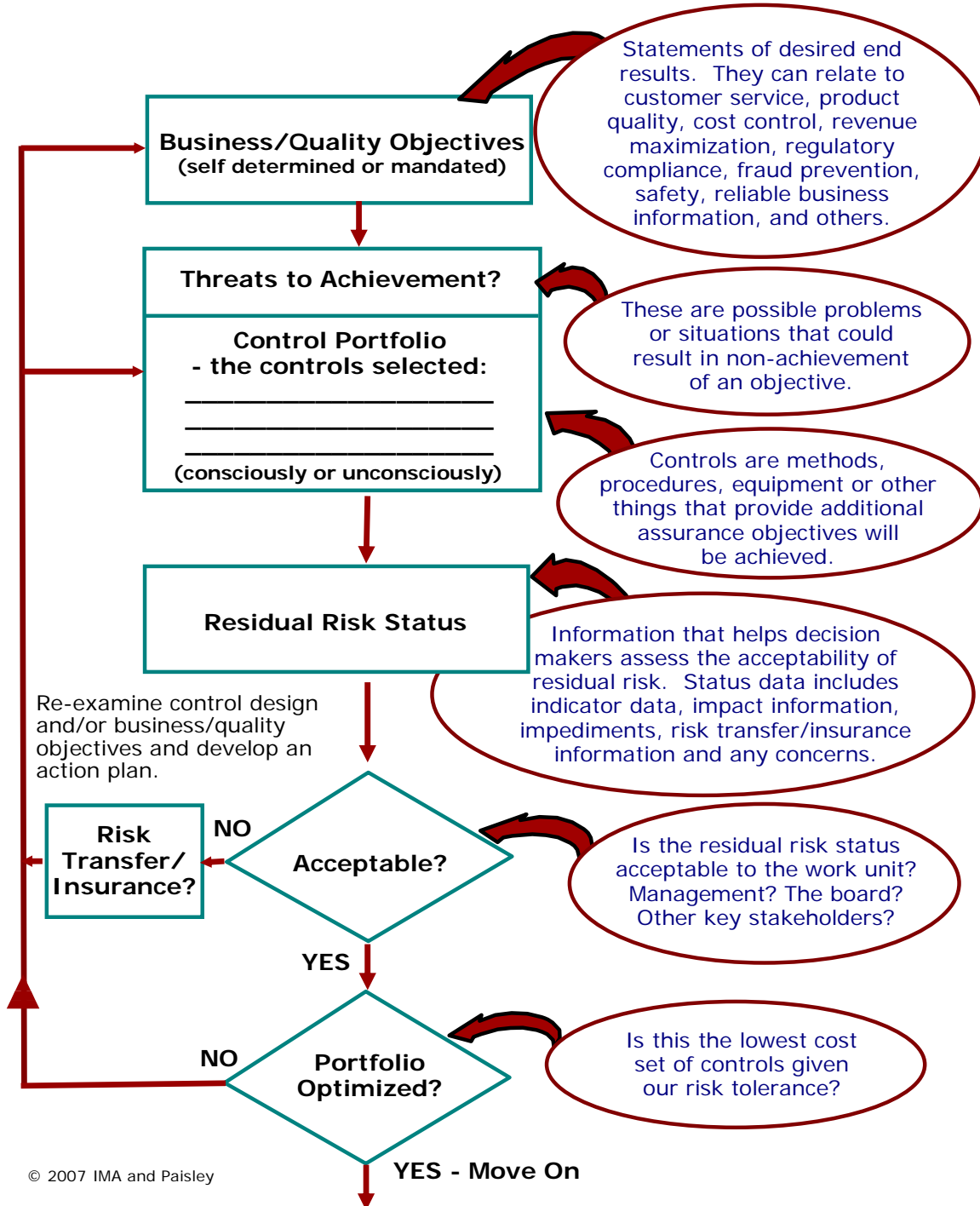
Impediment Data – in some situations there may be risks that threaten the reliability of accounting disclosures that are very difficult, expensive or even impossible to mitigate to a tolerable level because of one or more circumstances. An example might be a company that is developing new products or services that have not existed previously anywhere in the

world. Since there is no historical/corporate memory or awareness of these risks it can cause material accounting errors. Another example of an impediment would be a legal decision handed down or an out of court settlement reached late in an accounting period in a case a company in the same industry is involved in that has the potential of materially impacting a company's valuation of one or more accounts. It may not be possible or practical to access this information on a timely basis. A very simple example may be a situation where a majority shareholder has dictated that an unqualified individual that lacks the necessary knowledge or skills fill key accounting positions like CFO or Controller. The only viable mitigation for the type of risks that would flow from this situation is the skill of the external auditor finding and correcting errors and/or highly competent personnel in the controllership department.

Transfer/Risk Sharing Information – this is information about situations where some or all of the responsibility to mitigate risks has been shared or contractually transferred to another party. For ICoFR an example is outsourcing all responsibility for the company's pension fund management including the design and operation of controls to ensure accounting balances are reliable. Under current U.S. rules this may require that the organization that is doing the accounting have a "SAS 70 review" of their controls. Determining that one has been done may, or may not be enough to discharge a company's responsibility to ensure their own financial statements are reliable.

CONCLUDING REMARKS

This chapter has outlined an approach that meets globally accepted risk management standards. The SEC and PCAOB will be issuing new revised guidance to SEC registrants on how to assess and report on ICFR in May/June of 2007. It is not clear at the time of writing that the new SEC/PCAOB regulatory expectations will allow registrants to use the type of risk-based approach described in this paper. Interested readers should visit the Institute of Management Accountants website, www.imanet.org, for the IMA's comments on the new 2007 guidance. The IMA comment paper will specifically address whether the new, revised SEC/PCAOB ICFR guidance allows registrants to use globally accepted risk management principles in this area.



© 2007 IMA and Paisley

CARD[®]model



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 support them?

2. Commitment: Are the people that are important to the achievement of specific objectives committed to the achievement of those objectives?

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?

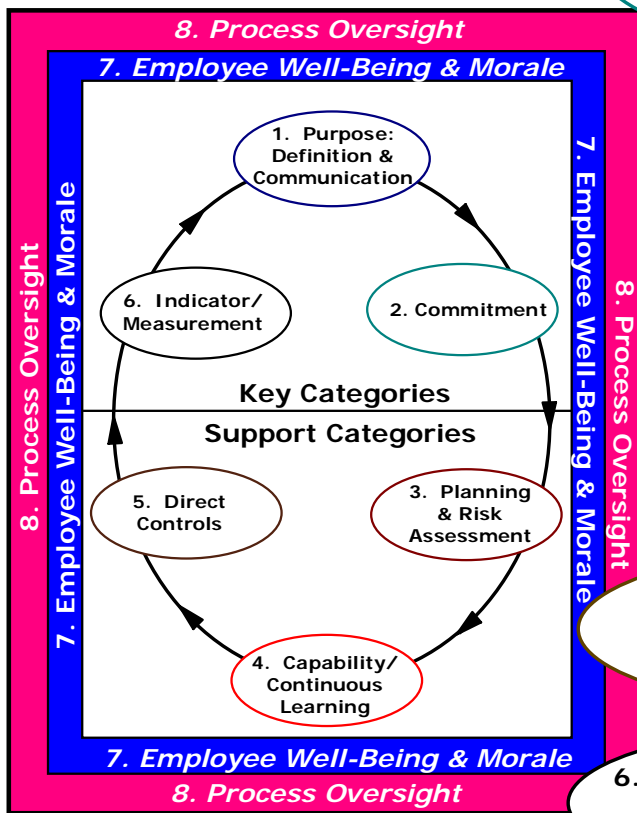
4. Capability/Continuous Learning: Do we have the necessary knowledge and skills to achieve specified objectives?

5. Direct Controls: What specific methods, procedures or devices help directly assure the achievement of objectives?

6. Indicator/Measurement: Do we know how well we are, or are not, achieving specific objectives?

7. Employee Well-Being & Morale: Is employee well-being and morale negatively or positively impacting on the achievement of objectives?

8. Process Oversight: Are there people or processes in place to check that the other controls selected are resulting in an acceptable level of residual risk? (i.e. risk of not achieving the objective.)



© 2007 IMA and Paisley

CARDMENU DETAILED LISTING OF ELEMENTS

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