WILEY CIA EXAM REVIEW

Focus Notes

Internal Audit Activity's Role in Governance, Risk, and Control

VOLUME 1

S. RAO VALLABHANENI

• *outlines* • *concepts* • *tools and techniques* • *standards*

WILEY CIA EXAM REVIEW

Focus Notes

Internal Audit Activity's Role in Governance, Risk, and Control

VOLUME 1

S. Rao Vallabhaneni

• *Outlines* • *Concepts* • *Tools and Techniques* • *Standards*

JOHN WILEY & SONS, INC.

WILEY CIA EXAM REVIEW

Focus Notes

Internal Audit Activity's Role in Governance, Risk, and Control

VOLUME 1

WILEY CIA EXAM REVIEW

Focus Notes

Internal Audit Activity's Role in Governance, Risk, and Control

VOLUME 1

S. Rao Vallabhaneni

• *Outlines* • *Concepts* • *Tools and Techniques* • *Standards*

JOHN WILEY & SONS, INC.

This book is printed on acid-free paper. ♾

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

ISBN 10: 0470277068 (Volume 1)
ISBN 13: 9780470277065
ISBN: 978-0-470-27710-2 (Set)

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

Contents

Preface

The Wiley CIA Exam Review Focus Notes are developed for each of the four parts of the Certified Internal Auditor (CIA) exam sponsored by the Institute of Internal Auditors (IIA). The purpose of the Focus Notes is to digest and assimilate the vast amounts of knowledge, skills, and abilities (KSAs) tested on the CIA exam in a clear, concise, easy-to-read, and -use format anywhere and any time to achieve success in the exam.

Each of the Focus Notes book topics is organized in the same way as the Wiley CIA Exam Review book topics, that is, one Focus Notes book for each of the four-volume review books. This clear linkage makes the exam study time more efficient and long-lasting, and provides the ability to recall important concepts, tools, and techniques, and the IIA Standards tested on the CIA exams. The Focus Notes are written in an outline format. However, they can be used with any study materials that you have determined works best for you to prepare for the CIA Exam. The Focus Notes provide a quick and easy refresher to the material that you are studying.

The Focus Notes books will be especially useful to auditors who are traveling on an audit assignment, as well as others who are not traveling, due to their small and compact size, giving portability. The simplified outlines included in this material will help you learn the essential KSAs as well as help you retain them for years to come.

The Focus Notes book can also be used as a desk reference on a post-exam basis, similar to a dictionary. With no bias intended and for the sake of simplicity, the pronoun “he” has been used throughout the book rather than “he/she” or “she.” Good luck on the exam!

S. Rao Vallabhaneni
September 2008

About the Author

S. Rao Vallabhaneni is an educator, author, publisher, and practitioner in the business management field with more than 30 years of management and teaching experience in internal auditing, accounting, manufacturing, finance, and information technology consulting in the public and private sectors and the academia. The 2004 Joseph Wasserman Memorial Award recipient, he is the author of more than 50 books, including monographs, audit guides, exam study guides, and articles. He has 24 professional certifications in management, accounting, auditing, finance, information technology, manufacturing, supply chain, quality, and human resources. He is the author of Wiley CIA Exam Review Books and CD Software. His CIA Exam Review books were translated into Chinese and his CISA Exam Review book was translated into Japanese. His recent book, entitled *Corporate Management, Governance, and Ethics Best Practices,* was published by John Wiley & Sons, Inc. (January 2008).

MANAGING AN INTERNAL AUDIT FUNCTION

The internal audit director needs to comply with the IIA's **Attribute Standards,** which say that the chief audit executive (CAE) is responsible for properly managing the department so that: (1) audit work fulfills the general purposes and responsibilities approved by senior management and accepted by the board, (2) resources of the internal auditing (IA) department are efficiently and effectively employed, and (3) audit work conforms to the **Standards.**

Internal Audit Charter

- Basic policy statement under which the internal auditing (IA) department operates.
- Establishes the IA department's position in the organization's hierarchy.
- IA department operates independently of all other departments in the organization.
- Describes the organizational status that the director of internal auditing should report to the chief executive officer (CEO) but have access to the board of directors. A dual reporting relationship exists here: reporting administratively to the president or CEO, and reporting functionally to the audit committee of the board of directors.
- Describes the purpose, authority, and responsibility of the IA department.

Mission or Purpose of the IA Department

- Review organization's activities to determine whether it is efficiently and effectively carrying out its function of controlling in accordance with management's instructions, policies, and procedures.
- Determine the adequacy and effectiveness of the system of internal controls in all areas of activity.
- Review the reliability and integrity of financial information and the means used to identify, measure, classify, and report such information.
- Review the means of safeguarding assets and, as appropriate, verify the existence of such assets.
- Appraise the economy and efficiency with which resources are employed, identify opportunities to improve operating performance, and recommend solutions to problems where appropriate.
- Review operations and plans to ascertain whether results are consistent with established objectives and goals, and whether the operations and plans are being carried out as intended.
- Coordinate audit efforts, where appropriate, with those of the external auditors.

Mission or Purpose of the IA Department (continued)

- Review the planning, design, development, implementation, and operation of relevant computer-based systems to determine whether (a) adequate controls are incorporated in the systems; (b) thorough system testing is performed at appropriate stages; (c) system documentation is complete and accurate; and (d) needs of the users are met.
- Conduct periodic audits of computer centers and make postinstallation evaluations of relevant data processing systems to determine whether those systems meet their intended purposes and objectives.
- Participate in the planning and performance of audits of acquisitions. Follow up to ensure the proper accomplishment of the audit objective.
- Report to those members of management who should be informed, or who should take corrective action, the results of audit examinations, the audit opinions formed, and the recommendations made.
- Evaluate the plans or actions taken to correct reported conditions for satisfactory disposition of audit findings. If corrective action is considered unsatisfactory, hold further discussions to achieve acceptable disposition.
- Provide adequate follow-up to ensure that proper corrective action is taken and that it is effective.

Authority

- The IA department will have full, free, and unrestricted access to records, personnel, and physical properties relevant to the performance of an audit.
- Internal auditors have neither authority over nor responsibility for the activities they audit.
- Audit director should have direct access to the audit committee since it tends to enhance IA's independence and objectivity.

Responsibility

The IA department accomplishes its purpose of assisting management by reviewing, examining, and evaluating activities, furnishing analyses and appraisals, and reporting findings and recommendations. This audit responsibility cannot relieve any operating manager of the requirement for ensuring proper control within his or her area of concern.

The IA department also has the responsibility to perform audit work with due professional care and with appropriate education, experience, certification, professional image and attitude, and personal integrity.

Planning

The director of internal auditing should establish plans to carry out the responsibilities of the internal auditing department. These plans should be consistent with the charter and with the goals for the organization. The planning process involves establishing goals, audit work schedules, staffing plans and financial budgets, and activity reports.

During audit planning, internal auditors should review all relevant information such as risk models/risk analysis, audit plans, audit assignments, and activity reports.

Risk Models/Risk Analysis

- Used in conjunction with development of long-range audit schedules.
- Judgment of the internal auditor and the results of quantitative risk assessment are the basis for audit planning work.
- Factors to be considered during risk analysis include:
  - Financial exposure
  - Potential loss of assets
  - Results of prior audits
  - Major operating changes
  - Damage to assets
  - Failure to comply with laws and regulations
- Skills available on the audit staff are not a risk factor since missing skills can be obtained elsewhere.
- The CAE should allocate the audit work schedule to managers based on risk analysis performed by auditors and skill analysis of the audit managers.

Audit Plan

The *audit plan* should include: a detailed schedule of areas to be audited during the coming year; an estimate of the time required for each audit, risk, exposure, and potential loss to the organization; and the approximate starting date for each audit.

Audit Assignment

Documentation needed to plan an audit assignment should include evidence that resources needed to complete the audit were considered. When the audit director makes audit assignments for inclusion in the work schedule, those assignments should be based on the relative risk of the auditable areas.

Criteria should be established when the audit resources are limited and a decision has to be made to choose between two operating departments for scheduling an audit. The most important criteria are: major changes in operations in one of the departments, more opportunities to achieve operating benefits in one of the departments than in the other, and when potential loss is significantly greater in one department than the other. Least important criteria are whether the audit staff has recently added an individual with experience in one of the auditable areas.

Activity Reports

Activity reports submitted periodically by the audit director to management and to the board should compare performance with audit work schedules. This requires comparing audits completed with audits planned.

Policies and Procedures

The CAE should provide written policies and procedures to guide the audit staff. An audit policies and procedures manual is most essential for guiding the audit staff in maintaining daily compliance with the department's standards of performance, and least important to audit quality control reviews, auditor position/job descriptions, and auditor performance appraisals.

Audit Manual

The need to issue formal manuals will largely depend on the size of the department. Any department with five or more staff members, or whose auditors work alone, should probably have one. The manual should address such things as administrative matters (e.g., progress reports, time and attendance, travel), adherence to the department's guidelines, relationships with auditees, auditing techniques, reporting audit results, and working paper standards (whether paper media, electronic media, or a combination).

Staff Meetings

- Staff meetings are conducted periodically to improve communications.
- Audit staff are afforded a venue where problems are discussed and receive updates regarding departmental policies.
- The CAE can address rumors affecting the audit department and the company.

Audit Reports

A report issued by an internal auditor should contain an expression of opinion when an opinion will improve communications with the reader of the report. Due professional care requires that the auditor's opinions be based on sufficient factual evidence that warrants the expression of the opinions. Due care does not require the performance of extensive audit examination. It calls for reasonable work.

The type of audit report (final, interim, or combination), the form of communication (oral, written, or combination), the type of audience to receive the audit report (internal management, external auditors, or combination), and the type of participants (by job title in the audit and the auditee department) to attend the entrance conference and the exit audit conference should be spelled out in the audit department policies and procedures manual.

An audit policy should require that final audit reports not be issued without a management response. However, when an audit with significant findings is complete except for management's response, the best alternative is to issue an *interim* report regarding the important issues noted. This is because time is of the essence here.

The final audit report should be reviewed, approved, and signed by the director of internal auditing or his designee. When illegal acts are being performed by several of the highest-ranking officers of the company, the audit report should be addressed to the audit committee of the board of directors.

Follow-up

The CAE should ensure follow-up of prior audit findings and recommendations to determine whether corrective action was taken and is achieving the desired results. If the auditor finds that no corrective action has been taken on a prior audit finding that is still valid, the auditor should determine whether management or the board has assumed the risk of not taking corrective action.

Personnel Management and Development

The CAE should establish a program for selecting and developing the human resources of the internal auditing department. A well-developed set of selection criteria is a key factor in the success of an audit department's human resource program.

Hiring

The audit staff should include members proficient in applying internal auditing standards, procedures, and techniques. When hiring an entry-level audit staff, the most likely predictors of an applicant's success as an auditor would be the ability to organize and express thoughts well; the least likely predictors would be: grade point average on college accounting courses; ability to fit well socially into a group; and the level of detail of knowledge of the company. When hiring an auditor, reasonable assurance should be obtained as to each prospective auditor's qualifications and proficiency. It should include obtaining college transcript(s), checking an applicant's references, and determining previous job experience.

Selection Criteria

The CAE should establish the evaluation criteria for the selection of new internal audit staff members. Criteria would be an appreciation of the fundamentals of accounting, an understanding of management principles, and the ability to recognize deviations from good business practices. Criteria would not include proficiency in computerized operations and the use of computers in auditing.

Performance Criteria

The CAE should establish guidelines for evaluating the performance of audit staff members: the evaluator should justify very high and very low evaluations because of their impact on the employee; evaluations should be made annually or more frequently to provide the employee with feedback about competence; and the first evaluation should be made shortly after commencing work to serve as an early guide to the new employee. But the evaluator should not use standard evaluation comments, because there are so many employees whose performance is completely satisfactory. The performance appraisal system for evaluating an auditor should include specific accomplishments directly related to the performance of the audit program.

Continuing Education

The CAE is responsible for establishing continuing education and training opportunities to develop the human resources of the audit department. The main purpose of audit department training is to achieve both individual and departmental goals in training.

External Auditors

The CAE should coordinate internal and external audit efforts to minimize duplication of audit work and to increase the effectiveness of audit work.

Quality Assurance

The CAE should establish and maintain a quality assurance program to evaluate the operations of the internal auditing department. The standard calls for three elements for the quality assurance program: supervision, internal reviews, and external reviews. The audit department should have periodic quality assurance reviews. Accomplishing the intended results and demonstrating consistent quality are also part of the quality assurance task.

Postaudit Quality Review

The postaudit quality review provides top managers with an independent assessment of the extent to which the audit organization complies with professional standards and its own policies and procedures.

Reviewing individual assignments provides valuable feedback to managers on how well-selected auditable units consistently achieve the expected quality. The number and type of assignments selected for testing should provide a reasonable basis for making this assessment.

INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING (STANDARDS)

Internal audit activities are performed in diverse legal and cultural environments; within organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization. While differences may affect the practice of internal auditing in each environment, compliance with the *International Standards for the Professional Practice of Internal Auditing* is essential if the responsibilities of internal auditors are to be met. If internal auditors are prohibited by laws or regulations from complying with certain parts of the *Standards*, they should comply with all other parts of the *Standards* and make appropriate disclosures.

The four purposes of the *Standards* are to:

1. Delineate basic principles that represent the practice of internal auditing as it should be.
2. Provide a framework for performing and promoting a broad range of value-added internal audit activities.
3. Establish the basis for the *evaluation* of internal audit performance.
4. Foster improved organizational processes and operations.

INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING (STANDARDS) (continued)

The *Standards* consist of *Attribute Standards, Performance Standards,* and *Implementation Standards.* The *Attribute Standards* address the characteristics of organizations and parties performing internal audit activities. The *Performance Standards* describe the nature of internal audit activities and provide quality criteria against which the performance of these services can be evaluated. While the *Attribute and Performance Standards* apply to all internal audit services, the *Implementation Standards* apply to specific types of engagements.

There is one set of *Attribute and Performance Standards*; however, there are multiple sets of *Implementation Standards*: a set for each of the major types of internal audit activity. The *Implementation Standards* have been established for assurance (A) and consulting (C) activities.

The *Standards* are part of the Professional Practices Framework. The Professional Practices Framework includes the Definition of Internal Auditing, the Code of Ethics, the *Standards*, and other guidance. Guidance regarding how the *Standards* might be applied is included in Practice Advisories that are issued by the Professional Issues Committee.

IIA'S ATTRIBUTE STANDARDS

Purpose, Authority, and Responsibility

- Formally defined in a charter, consistent with the *Standards,* and approved by the board (IIA Standard 1000).
- The nature of assurance services provided to the organization should be defined in the audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances should also be defined in the charter (IIA Standard 1000.A1).
- The nature of consulting services should be defined in the audit charter (IIA Standard 1000.C1).

Independence and Objectivity

Organizational Independence

- The CAE should report to a level within the organization that allows the internal audit activity to fulfill its responsibilities (IIA Standard 1110).
- The internal audit activity should be free from interference in determining the scope of internal auditing, performing work, and communicating results (IIA Standard 1110.A1).

Individual Objectivity

- Internal auditors should have an impartial, unbiased attitude and avoid conflicts of interest (IIA Standard 1120).

Impairments to Independence or Objectivity

- If independence or objectivity is impaired in fact or appearance, the details of the impairment should be disclosed to appropriate parties. The nature of the disclosure will depend on the impairment (IIA Standard 1130).
- Internal auditors should refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an ***internal*** auditor provides assurance services for an activity for which the ***internal*** auditor had responsibility within the previous year (IIA Standard 1130.A1).
- Assurance engagements for functions over which the CAE has responsibility should be overseen by a party outside the internal audit activity (IIA Standard 1130.A2).
- Internal auditors may provide consulting services relating to operations for which they had previous responsibilities (IIA Standard 1130.C1).
- If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure should be made to the engagement client prior to accepting the engagement (IIA Standard 1130.C2).

Proficiency and Due Professional Care

Proficiency

Internal auditors should possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities (IIA Standard 1210).

The CAE should obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement (IIA Standard 1210.A1).

The internal auditor should have sufficient knowledge to identify the indicators of fraud but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud (IIA Standard 1210.A2).

Internal auditors should have knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing (IIA Standard 1210.A3).

The CAE should decline the consulting engagement or obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement (IIA Standard 1210.C1).

Due Professional Care

Internal auditors should apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility (IIA Standard 1220).

The internal auditor should exercise due professional care (IIA Standard 1220.A1) by considering the

- Extent of work needed to achieve the engagement's objectives
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied
- Adequacy and effectiveness of risk management, control, and governance processes
- Probability of significant errors, irregularities, or noncompliance
- Cost of assurance in relation to potential benefits

In exercising due professional care, the internal auditor should consider the use of computer-assisted audit tools and other data analysis techniques (IIA Standard 1220.A2).

The internal auditor should be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified (IIA Standard 1220.A3).

Due Professional Care (continued)

The internal auditor should exercise due professional care during a consulting engagement (IIA Standard 1220.C1) by considering the

- Needs and expectations of clients, including the nature, timing, and communication of engagement results
- Relative complexity and extent of work needed to achieve the engagement's objectives
- Cost of the consulting engagement in relation to potential benefits

Continuing Professional Development

Internal auditors should enhance their knowledge, skills, and other competencies through continuing professional development (IIA Standard 1230).

Quality Assurance and Improvement Program

The CAE should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity and continuously monitors its effectiveness. *Each part of the program* should be designed to help the internal auditing activity add value and improve the organization's operations and to provide assurance that the internal audit activity is in conformity with the *Standards* and the Code of Ethics:

- Quality Program Assessments (IIA Standard 1310)
- Internal Assessments (IIA Standard 1311)
- External Assessments (IIA Standard 1312)
- Reporting on the Quality Program (IIA Standard 1320)
- Use of "Conducted in Accordance with the Standards" (IIA Standard 1330)
- Disclosure of Noncompliance (IIA Standard 1340)

IIA'S CODE OF ETHICS

The IIA's Code of Ethics promotes an ethical culture in the profession of internal auditing.

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The IIA's Code of Ethics extends beyond the definition of internal auditing to include two essential components: (1) Principles, and (2) Rules of Conduct.

The Code of Ethics together with the IIA's Professional Practices Framework and other relevant Institute pronouncements provide guidance to internal auditors serving others. "Internal auditors" refers to Institute members, recipients of or candidates for IIA professional certifications, and those who provide internal auditing services within the definition of internal auditing.

Applicability and Enforcement

This Code of Ethics applies to both individuals and entities that provide internal auditing services. For Institute members and recipients of or candidates for IIA professional certifications, breaches of the Code of Ethics will be evaluated and administered according to the Institute's Bylaws and Administrative Guidelines. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate engaging in such conduct can be liable for disciplinary action.

Principles and Rules of Conduct

- Integrity
- Objectivity
- Confidentiality
- Competency

MANAGING THE INTERNAL AUDIT ACTIVITY

The CAE is responsible for properly managing the internal audit activity so that

- Audit work fulfills the general purposes and responsibilities described in the charter and approved by the board and senior management as appropriate.
- Resources of the internal audit activity are efficiently and effectively employed.
- Audit work conforms to the *International Standards for the Professional Practice of Internal Auditing (Standards)*.

PLANNING

The CAE should establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals (IIA Standard 2010).

The internal audit activity's plan of engagements should be based on a risk assessment, undertaken at least annually. The input of senior management and the board should be considered in this process (IIA Standard 2010.A1).

The CAE should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Those engagements that have been accepted should be included in the plan (IIA Standard 2010.C1).

Linking the Audit Plan to Risk and Exposures

- Any organization faces a number of uncertainties and risks that can both negatively and positively affect the organization.
- The internal audit activity's audit plan should be designed based on an assessment of risk and exposures that may affect the organization.
- The audit universe can include components from the organization's strategic plan.
- Changes in management direction, objectives, emphasis, and focus should be reflected in updates to the audit universe and related audit plan.
- Audit work schedules should be based on, among other factors, an assessment of risk priority and exposure.
- Management reporting and communication should convey risk management conclusions and recommendations to reduce exposures. For management to fully understand the degree of exposure, it is critical that audit reporting identify the criticality and consequence of the risk exposure to achieving objectives.

COMMUNICATION AND APPROVAL

- The CAE should submit annually to the board for approval, and to senior management as appropriate, a summary of the internal audit activity's work schedule, staffing plan, and financial budget. The CAE should also submit all significant interim changes for approval and information. Engagement work schedules, staffing plans, and financial budgets should inform senior management and the board of the scope of internal auditing work and of any limitations placed on that scope.
- The approved engagement work schedule, staffing plan, and financial budget, along with all significant interim changes, should contain sufficient information to enable the board to ascertain whether the internal audit activity's objectives and plans support those of the organization and the board.

RESOURCE MANAGEMENT

- Staffing plans and financial budgets, including the number of auditors and the knowledge, skills, and other competencies required to perform their work, should be determined from engagement work schedules, administrative activities, education and training requirements, and audit research and development efforts.
- The CAE should establish a program for selecting and developing the human resources of the internal audit activity.
- The CAE should consider using persons from cosourcing arrangements, other consultants, or company employees from other departments to provide specialized or additional skills where needed.

POLICIES AND PROCEDURES

The form and content of written policies and procedures should be appropriate to the size and structure of the internal audit activity and the complexity of its work. Formal administrative and technical audit manuals may not be needed by all internal auditing entities. A small internal audit activity may be managed informally. Its audit staff may be directed and controlled through daily, close supervision and written memoranda. In a large internal audit activity, more formal and comprehensive policies and procedures are essential to guide the audit staff in the consistent compliance with the internal audit activity's standards of performance.

COORDINATION

- Internal and external auditing work should be coordinated to ensure adequate audit coverage and to minimize duplicate efforts.
- Oversight of the work of external auditors, including coordination with the internal audit activity, is the responsibility of the board. Actual coordination should be the responsibility of the CAE.
- In coordinating the work of internal auditors with the work of external auditors, the CAE should ensure that work to be performed by internal auditors in fulfillment of Section 2100 of the *Standards* does not duplicate the work of external auditors, which can be relied on for purposes of internal auditing coverage.
- The CAE may agree to perform work for external auditors in connection with their annual audit of the financial statements. Work performed by internal auditors to assist external auditors in fulfilling their responsibility is subject to all relevant provisions of the *Standards*.
- The CAE should make regular evaluations of the coordination between internal and external auditors.
- In exercising its oversight role, the board may request the CAE to assess the performance of external auditors.

Audit Coverage

Planned audit activities of internal and external auditors should be discussed to ensure that audit coverage is coordinated and duplicate efforts are minimized. Sufficient meetings should be scheduled during the audit process to ensure coordination of audit work and efficient and timely completion of audit activities and to determine whether observations and recommendations from work performed to date require that the scope of planned work be adjusted.

Access to Each Other's Audit Programs and Working Papers

Access to the external auditors' programs and working papers may be important in order for internal auditors to be satisfied as to the acceptability for internal audit purposes of relying on the external auditors' work. Such access carries with it the responsibility for internal auditors to respect the confidentiality of those programs and working papers. Similarly, access to the internal auditors' programs and working papers should be given to external auditors in order for external auditors to be satisfied as to the acceptability, for external audit purposes, of relying on the internal auditors' work.

Exchange of Audit Reports and Management Letters

Internal audit final communications, management's responses to those communications, and subsequent internal audit activity follow-up reviews should be made available to external auditors. These communications assist external auditors in determining and adjusting the scope of work. In addition, the internal auditors need access to the external auditors' management letters. Matters discussed in management letters assist internal auditors in planning the areas to emphasize in future internal audit work.

Common Understanding of Audit Techniques, Methods, and Terminology

- The CAE should understand the scope of work planned by external auditors and should be satisfied that the external auditors' planned work, in conjunction with the internal auditors' planned work, satisfies the requirements of Section 2100 of the *Standards*.
- The CAE should ensure that the external auditors' techniques, methods, and terminology are sufficiently understood by internal auditors. The CAE should also ensure that the reverse situation is taking place.

Acquisition of External Audit Services

- The internal auditor's participation in the selection, evaluation, and retention of the organization's external auditors may vary from no role in the process, to advising management or the audit committee, assistance or participation in the process, management of the process, or auditing the process. Since the IIA *Standards* require internal auditors to "share information and coordinate activities with other internal and external providers of relevant assurance and consulting services," it is advisable for internal auditors to have some role or involvement in the selection or retention of the external auditors and in the definition of scope of work.
- A board- or audit committee–approved policy can facilitate the periodic request for external audit services and position such exercises as normal business activities so that the current service providers do not view a decision to request proposals as a signal that the organization is dissatisfied with current services.

REPORTING TO THE BOARD AND SENIOR MANAGEMENT

Internal auditors should consider the following suggestions when reporting to the board and senior management:

- Significant engagement observations may include conditions dealing with irregularities, illegal acts, errors, inefficiency, waste, ineffectiveness, conflicts of interest, and control weaknesses.
- Management's responsibility is to make decisions on the appropriate action to be taken regarding significant engagement observations and recommendations. The CAE should consider whether it is appropriate to inform the board regarding previously reported significant observations and recommendations in those instances where senior management and the board assumed the risk of not correcting the reported condition. This may be particularly necessary where there have been changes in organization, board, senior management, or other changes.
- Activity reports should also compare (a) actual performance with the internal audit activity's goals and audit work schedules, and (b) expenditures with financial budgets. Reports should explain the reason for major variances and indicate any action taken or needed.

Relationship with the Audit Committee

Three areas of activities are key to an effective relationship between the audit committee and the internal audit function, mainly through the CAE:

1. Assisting the audit committee to ensure that its charter, activities, and processes are appropriate to fulfill its responsibilities
2. Ensuring that the charter, role, and activities of internal audit are clearly understood and responsive to the needs of the audit committee and the board
3. Maintaining open and effective communications with the audit committee and the chairperson

Internal Audit Activity's Role

The CAE's relationship to the audit committee should revolve around a core role of the CAE ensuring that the audit committee understands, supports, and receives all assistance needed from the internal audit function. The IIA supports the concept that sound governance is dependent on the synergy generated among the four principal components of effective corporate governance systems: boards of directors, management, internal auditors, and external auditors. In that structure, internal auditors and audit committees are mutually supportive.

Communications with the Audit Committee

Audit committees should:

- Meet privately with the CAE on a regular basis to discuss sensitive issues.
- Provide an annual summary report or assessment on the results of the audit activities relating to the defined mission and scope of audit work.
- Issue periodic reports to the audit committee and management summarizing results of audit activities.
- Keep the audit committee informed of emerging trends and successful practices in internal auditing.
- Discuss with the external auditor and the CAE about fulfillment of committees' information needs.
- Review information submitted to the audit committee for completeness and accuracy.
- Confirm there is effective and efficient work coordination of activities between internal and external auditors. It also should determine whether there is any duplication between the work of the internal and external auditors and give the reasons for such duplication.

NATURE OF WORK

- The scope of internal auditing work encompasses a systematic, disciplined approach to evaluating and improving the *adequacy* and *effectiveness* of risk management, control, and governance processes and the quality of performance in carrying out assigned responsibilities.
- *Adequacy* of risk management, control, and governance processes is present if management has planned and designed processes in a manner that provides reasonable assurance that the organization's objectives and goals will be achieved efficiently and economically.
- *Effectiveness* of risk management, control, and governance processes is present if management directs processes in such a manner as to provide reasonable assurance that the organization's objectives and goals will be achieved.
- The primary objectives of the overall management process are to achieve: relevant, reliable, and credible financial and operating information; effective and efficient use of the organization's resources; safeguarding of the organization's assets; compliance with laws, regulations, ethical and business norms, and contracts; identification of risk exposures and use of effective strategies to control them; established objectives and goals for operations or programs.

NATURE OF WORK (continued)

- *Control* is any action taken by management to enhance the likelihood that established objectives and goals will be achieved.
- All business systems, processes, operations, functions, and activities within the organization are subject to the internal auditors' evaluations. The comprehensive scope of work of internal auditing should provide reasonable assurance that management's risk management system is effective; system of internal control is adequate, effective, and efficient; and governance process is effective by establishing and preserving values, setting goals, monitoring activities and performance, and defining the measures of accountability.

RISK MANAGEMENT

The internal audit activity should:

- Assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems (IIA Standard 2110). Monitor and evaluate the effectiveness of the organization's risk management system (IIA Standard 2110.A1).
- Evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the (IIA Standard 2110.A2) reliability and integrity of financial and operational information; effectiveness and efficiency of operations; safeguarding of assets; compliance with laws, regulations, and contracts.
- During consulting engagements, internal auditors should address risk consistent with the engagement's objectives and be alert to the existence of other significant risks (IIA Standard 2110.C1).
- Internal auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization (IIA Standard 2110.C2).

Assessing the Adequacy of Risk Management Processes

Internal auditors may be charged with the responsibility for providing assurance to management and the audit committee on the adequacy of the organization's risk management processes. This responsibility would require the auditor to formulate an opinion on whether the organization's risk management process is sufficient to protect the assets, reputation, and ongoing operations of the organization.

- Risk management is a key responsibility of management. However, internal auditors acting in a consulting role can assist the organization in identifying, evaluating, and implementing risk management methodologies and controls to address those risks.
- Developing assessments and reports on the organization's risk management processes is normally a high audit priority.
- Each organization may choose a particular methodology to implement its risk management process. The five key objectives of a risk management process are:
  1. Risks arising from business strategies and activities are identified and prioritized.
  2. Management and the board have determined the level of risks acceptable to the organization, including the acceptance of risks designed to accomplish the organization's strategic plans.
  3. Risk mitigation activities are designed and implemented to reduce, or otherwise manage, risk at levels that were determined to be acceptable to management and the board.

Assessing the Adequacy of Risk Management Processes (continued)

4. Ongoing monitoring activities are conducted to periodically reassess risk and the effectiveness of controls to manage risk.
5. The board and management receive periodic reports of the results of the risk management processes. The corporate governance processes of the organization should provide periodic communication of risks, risk strategies, and controls to stakeholders.

- Internal auditors should recognize that there could be significant variations in the techniques used by various organizations for their risk management practices. Risk management processes should be designed for the nature of an organization's activities. Depending on the size and complexity of the organization's business activities, risk management processes can be:
  - Formal or informal
  - Quantitative or subjective
  - Embedded in the business units or centralized at a corporate level
  - Internal auditors should obtain sufficient evidence to satisfy themselves that the five key objectives of the risk management processes are being met in order to form an opinion on the adequacy of risk management processes.

Auditor's Role in Identifying and Reporting Environmental Risks

Internal auditors should be alert to the potential risks that may result from the organizational placement and reporting relationships of environmental auditors. The risks related to environmental noncompliance, fines and penalties, and other mismanagement may result in significant losses for the organization.

Potential Risks

- The CAE should include the environmental, health, and safety (EH&S) risks in any entity-wide risk management assessment and assess the activities in a balanced manner relative to other types of risk associated with an entity's operations.
- Where the CAE finds that the management of the EH&S risks largely depends on an environmental audit function, the CAE needs to consider the implications of that organizational structure and its effects on operations and the reporting mechanisms. If the CAE finds that the exposures are not adequately managed and residual risks exist, that conclusion would normally result in changes to the internal audit activity's plan of engagements and further investigations.
- The majority of environmental audit functions report to their organization's environmental component or general counsel, not to the CAE.

CONTROL

The internal audit activity should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement (IIA Standard 2120).

- Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization's governance, operations, and information systems (IIA Standard 2120.A1).
- Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization (IIA Standard 2120.A2).
- Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended (IIA Standard 2120.A3).
- Adequate criteria are needed to evaluate controls. Internal auditors should ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors should use such criteria in their evaluation. If inadequate, internal auditors should work with management to develop appropriate evaluation criteria (IIA Standard 2120.A4).

CONTROL (continued)

- During consulting engagements, internal auditors should address controls consistent with the engagement's objectives and be alert to the existence of any significant control weaknesses (IIA Standard 2120.C1).
- Internal auditors should incorporate knowledge of controls gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization (IIA Standard 2120.C2).

Assessing and Reporting on Control Processes

- One of the tasks of a board of directors is to establish and maintain the organization's governance processes and obtain assurances concerning the effectiveness of the risk management and control processes. Senior management's role is to oversee the establishment, administration, and assessment of that system of risk management and control processes.
- Among the responsibilities of the organization's managers is the assessment of the control processes in their respective areas. Internal and external auditors provide varying degrees of assurance about the state of effectiveness of the risk management and control processes in select activities and functions of the organization.
- Senior management and the board normally expect that the CAE will perform sufficient audit work and gather other available information during the year so as to form a judgment about the adequacy and effectiveness of the risk management and control processes.
- The CAE should develop a proposed audit plan normally for the coming year that ensures sufficient evidence will be obtained to evaluate the effectiveness of the risk management and control processes.
- In determining the proposed audit plan, the CAE should consider relevant work that will be performed by others in order to minimize duplication and inefficiencies.

Assessing and Reporting on Control Processes (continued)

- The CAE should evaluate the coverage of the proposed plan from two viewpoints: adequacy across organizational entities and inclusion of a variety of transaction and business-process types.
- The challenge for internal audit is to evaluate the effectiveness of the organization's system of risk management and controls based on the aggregation of many individual assessments. Those assessments are largely gained from internal audit engagements, management's self-assessments, and external auditors' work.
- Three key considerations in reaching an evaluation of the overall effectiveness of the organization's risk management and control processes are: (1) Were significant discrepancies or weaknesses discovered from the audit work performed and other assessment information gathered?; (2) If so, were corrections or improvements made after the discoveries?; and (3) Do the discoveries and their consequences lead to the conclusion that a pervasive condition exists resulting in an unacceptable level of business risk?
- The CAE's report on the state of the organization's risk management and control processes should be presented, usually once a year, to senior management and the board.
- Ample evidence exists of an "expectation gap" surrounding the internal audit activity's work in evaluating and providing assurance about the state of risk management and control processes.

Using Control Self-Assessment for Assessing the Adequacy of Control Processes

- Senior management is charged with overseeing the establishment, administration, and evaluation of the processes of risk management and control. Operating managers' responsibilities include assessment of the risks and controls in their units. Internal and external auditors provide varying degrees of assurance about the state of effectiveness of the risk management and control processes of the organization.
- A methodology encompassing self-assessment surveys and facilitated workshops called *control self-assessment* (CSA) is a useful and efficient approach for managers and internal auditors to collaborate in assessing and evaluating control procedures. In its purest form, CSA integrates business objectives and risks with control processes. Control self-assessment is also referred to as *control/risk self-assessment* (CRSA).
- Outcomes that may be derived from self-assessment methodologies are: People are trained and experienced; informal, "soft" controls are more easily identified and evaluated; people are motivated to take ownership of the control processes in their units, and corrective actions taken by the work teams are often more effective and timely; the entire organization is subject to greater monitoring and continuous improvement; internal auditors become involved in and knowledgeable about the self-assessment process; internal audit activity acquires more information about the control processes within the organization; managers will be less tempted to abdicate those activities to specialists; primary role of the internal audit activity will continue

Using Control Self-Assessment for Assessing the Adequacy of Control Processes (continued)

to include the validation of the evaluation process by performing tests and the expression of its professional judgment on the adequacy and effectiveness of the whole risk management and control systems.

- The wide variety of approaches used for CSA processes in organizations reflects the differences in industry, geography, structure, organizational culture, degree of employee empowerment, dominant management style, and the manner of formulating strategies and policies.
- The three primary forms of CSA programs are facilitated team workshops, surveys, and management-produced analysis. Organizations often combine more than one approach.
- Facilitated team workshops gather information from work teams representing different levels in the business unit or function. The format of the workshop may be based on objectives, risks, controls, or processes. A report is created during the deliberations session and the team reviews the report before the end of the final session.
- The survey form of CSA utilizes a questionnaire that tends to ask mostly simple "Yes–No" or "Have–Have Not" questions.
- The management-produced analysis form of CSA covers most other approaches by management groups to produce information about selected business processes, risk management activities, and control procedures.

Using Control Self-Assessment for Assessing the Adequacy of Control Processes (continued)

- All self-assessment programs are based on managers and members of the work teams possessing an understanding of risks and controls concepts and using those concepts in communications.
- Internal audit's investment in some CSA programs is fairly significant. It may sponsor, design, implement, and, in effect, own the process, conducting the training, supplying the facilitators, scribes, and reporters, and orchestrating the participation of management and work teams. In other CSA programs, internal audit's involvement is minimal, serving as interested party and consultant of the whole process and as ultimate verifier of the evaluations produced by the teams. In most programs, internal audit's investment in the organization's CSA efforts is somewhere between the two extremes just described.
- A CSA program augments the traditional role of internal audit activity by assisting management in fulfilling its responsibilities to establish and maintain risk management and control processes and to evaluate the adequacy of that system.
- Although providing staff support for the CSA program as facilitator, scriber, reporter, trainer, and specialist, the internal audit activity often finds that it may reduce the effort spent in gathering information about control procedures and eliminate some testing.

Auditor's Role in Quarterly Financial Reporting, Disclosures, and Management Certifications

Internal auditors should consider the following guidance regarding quarterly financial reports, disclosures, and management certifications related to requirements of the Securities and Exchange Commission (SEC) applicable to both U.S. registrants and foreign registrants.

- The strength of all financial markets depends on investor confidence. Events involving allegations of misdeeds by corporate executives, independent auditors, and other market participants have undermined that confidence. In response to this threat, U.S. legislative bodies and regulatory agencies in other countries passed legislation and regulations affecting corporate disclosures and financial reporting (e.g., in the United States, the Sarbanes-Oxley Act of 2002 required additional disclosures and certifications of financial statements by principal executive and financial officers).
- The new law challenges companies to devise processes that will permit senior officers to acquire the necessary assurances on which to base their personal certification. A key component of the certification process is the management of risk and internal controls over the recording and summarizing of financial information.

New Statutory Requirements

Section 302 of the Sarbanes-Oxley Act outlines the corporate responsibility for financial reports, and the Securities and Exchange Commission (SEC) has issued guidance to implement the Act. As adopted, SEC Rules 13a-14 and 15d-14 require an issuer's principal executive officer(s) and the principal financial officer(s), or persons performing similar functions, to certify in each quarterly and annual report, including transition reports, filed or submitted by the issuer under Section 13(a) or 15(d) of the Exchange Act, that they have complied with the Act.

Recommended Actions

- The internal auditor's role in such processes may range from initial designer of the process, participant on a disclosure committee, or coordinator or liaison between management and its auditors, to independent assessor of the process.
- All internal auditors involved in quarterly reporting and disclosure processes should have a clearly defined role and evaluate responsibilities with appropriate IIA *Consulting and Assurance Standards* and with guidance contained in related Practice Advisories.
- Internal auditors should ensure that organizations have a formal policy and documented procedures to govern processes for quarterly financial reports, related disclosures, and regulatory reporting requirements.
- Internal auditors should encourage organizations to establish a "disclosure committee" to coordinate the process and provide oversight to participants. Representatives from key areas of the organization should be represented on the committee.
- Internal auditors should periodically review and evaluate quarterly reporting and disclosure processes, disclosure committee activities, and related documentation, and provide management and the audit committee with an assessment of the process and assurance concerning overall operations and compliance with policies and procedures.

Recommended Actions (continued)

- Internal auditors should recommend appropriate improvements to the policies, procedures, and process for quarterly reporting and related disclosures based on the results of an assessment of related activities.
- Internal auditors should compare processes for complying with Section 302 of the Sarbanes-Oxley Act (quarterly financial reporting and disclosures) to procedures developed to comply with Section 404 concerning management's annual assessment and public report on internal controls. Processes designed to be similar or compatible will contribute to operational efficiencies and reduce the likelihood or risk for problems and errors to occur or go undetected.

Auditing the Financial Reporting Process

- Executive management is the owner of the control environment and financial information, including the notes accompanying the financial statements and the accompanying disclosures in the financial report.
- The external auditor assures the financial report user that the reported information fairly presents the financial condition and result of operations of the organization in accordance with generally accepted accounting principles.
- The internal auditor performs procedures to provide a level of assurance to senior management and the audit or other committee of the governing board that controls surrounding the processes supporting the development of financial reports are effective.

Reporting on Internal Control

- An organization's audit or other board committee and internal auditing activity have interlocking goals. The core role of the CAE is to ensure that the audit committee receives the support and assurance services it needs and requests.
- Internal audit activity's work plans and specific assurance engagements begin with a careful identification of the exposures facing the organization, and internal audit's work plan is based on the risks and the assessment of the risk management and controls processes maintained by management to mitigate those risks.

A Framework for Internal Control

- Several widely accepted control models exist to assess the internal control system of an organization (e.g., COSO and CoCo). Any other recognized and credible model is appropriate to use.
- The COSO model states:
  - Internal control is not limited to accounting controls and is not narrowly restricted to financial reporting.
  - While accounting and financial reports are important issues, there are other important factors such as resource protection, operational efficiency and effectiveness, and compliance with rules, regulations, and organization policies that impact the financial reporting.
  - Internal control is management's responsibility and requires the participation of all persons within an organization, if it is to be effective.
  - The control framework is tied to the business objectives and is flexible enough to be adaptable.

Reporting on the Effectiveness of Internal Control

- The CAE should provide to the audit committee the internal audit's assessment of the effectiveness of the organization's system of controls, including its judgment on the adequacy of the control model or design. A governing board must rely on management to maintain an adequate and effective internal control system. It will reinforce that reliance with independent oversight.
- Internal controls cannot ensure success. Bad decisions, poor managers, or environmental factors can negate controls. Also, dishonest management may override controls and ignore or stifle communications from subordinates.

Roles for the Internal Auditor

- The CAE needs to review internal audit's risk assessment and audit plans for the year, if adequate resources have not been committed to helping senior management, the audit committee, and the external auditor with their responsibilities in the upcoming year's financial reporting regimentation.
- The CAE should allocate the internal audit's resources to the financial reporting, governance, and control processes consistent with the organization's risk assessment. The CAE should perform procedures that provide a level of assurance to senior management and the audit committee that controls surrounding the processes supporting the development of financial reports are adequately designed and effectively executed.
- Topics that the CAE may consider in supporting the organization's governance process and the oversight responsibilities of the governing board and its audit committee (or other designated committee) to ensure the reliability and integrity of financial reports should include financial reporting, corporate governance, and corporate control.

Control Criteria

- Before controls can be evaluated, management should determine the level of risk they want to take in the area to be reviewed. Internal auditors should identify what that level of risk is.
- If management has not identified the key risks and the level of risk they want to take, the internal audit may be able to help them through the facilitation of risk identification workshops or other techniques used by the organization.
- Once the risk level is determined, the controls currently in place can be assessed to determine how successful they are expected to be in reducing the risk to the desired level.

GOVERNANCE

The internal audit activity should assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives (IIA Standard 2130):

- Promoting appropriate ethics and values within the organization
- Ensuring effective organizational performance management and accountability
- Effectively communicating risk and control information to appropriate areas of the organization
- Effectively coordinating the activities of and communicating information among the board, external and internal auditors, and management

The internal audit activity should evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities (IIA Standard 2130.A1).

Consulting engagement objectives should be consistent with the overall values and goals of the organization (IIA Standard 2130.C1).

Role of the Internal Audit Activity and Internal Auditor in the Ethical Culture of an Organization

Governance and Organizational Culture

The way in which an organization chooses to conduct its affairs to meet the following four responsibilities: (1) Complies with society's legal and regulatory rules, (2) Satisfies the generally accepted business norms, ethical precepts, and social expectations of society, (3) Provides overall benefit to society and enhances the interests of the specific stakeholders in both the long term and the short term, and (4) Reports fully and truthfully to its owners, regulators, other stakeholders, and general public to ensure accountability for its decisions, actions, conduct, and performance is commonly referred to as its *governance process*. The organization's governing body and its senior management are accountable for the effectiveness of the governance process.

Shared Responsibility for the Organization's Ethical Culture

All people associated with the organization share some responsibility for the state of its ethical culture. Because of the complexity and dispersion of decision-making processes in most enterprises, each individual should be encouraged to be an ethics advocate, whether the role is delegated officially or merely conveyed informally. Codes of conduct and statements of vision and policy are important declarations of the organization's values and goals, the behavior expected of its people, and the strategies for maintaining a culture that aligns with its legal, ethical, and societal responsibilities.

Internal Audit Activity as Ethics Advocate

- Internal auditors and the internal audit activity should take an active role in support of the organization's ethical culture.
- The internal audit activity may assume one of several different roles as an ethics advocate. Those roles include chief ethics officer (ombudsman, compliance officer, management ethics counselor, or ethics expert), member of an internal ethics council, or assessor of the organization's ethical climate. In some circumstances, the role of chief ethics officer may conflict with the independence attribute of the internal audit activity.

Assessment of the Organization's Ethical Climate

At a minimum, the internal audit activity should periodically assess the state of the ethical climate of the organization and the effectiveness of its strategies, tactics, communications, and other processes in achieving the desired level of legal and ethical compliance.

ETHICS/COMPLIANCE

Role of Corporate Code of Ethics

Ethics is knowing what is right or wrong, proper or improper. Ethics forms basic ground rules for individuals to follow.

Conflict of Interest

The conflict-of-interest policy often is considered a part of the overall ethics policies. Conflict-of-interest concerns sometimes constitute the main part of ethics standards.

Options for Facilitating Ethical Behavior

- Distributing the code in a training program with top management attendance
- Transmitting the code with the chief executive officer's personal letter (tone-from-the-top)
- Showing ethics examples in a workshop (role-playing)
- Showing videotapes with top management supportive comments

Monitoring Compliance with the Code of Conduct

Compliance with the code of conduct is an ongoing responsibility of each employee and is primarily based on the honor system. Employees should be asked to certify or sign a form asserting that they have complied with the code or to list exceptions to such compliance.

Fraud in Financial Reporting

The Treadway Commission in 1987 made specific recommendations on the Code of Corporate Conduct, as follows: The public company should develop and enforce written codes of corporate conduct. Codes of conduct should foster a strong ethical climate and open channels of communication to help protect against fraudulent financial reporting. As a part of its ongoing oversight of the effectiveness of internal controls, a company's audit committee should annually review the program that management establishes to monitor compliance with the code.

EXAMPLE OF THE CONTENT OF A CODE OF CONDUCT

Although each organization is different in some respects, certain types of employee behavior can be expected in all organizations. The contents of a code of conduct are divided into three groups: (1) mandatory (those items that should always appear in a code-of-conduct document), (2) strongly suggested, and (3) desirable. Factors that determine what is appropriate for each specific code are based on a complete understanding of the business and corporate culture.

IIA'S PERFORMANCE STANDARDS

Nature of Work

The internal audit activity ***should*** evaluate and contribute to the improvement of risk management, control, and governance processes using a systematic and disciplined approach (IIA Standard 2100).

Risk Management

- The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems (IIA Standard 2110).
- The internal audit activity should monitor and evaluate the effectiveness of the organization's risk management system (IIA Standard 2110.A1).
- The internal audit activity should evaluate risk exposures relating to the organization's governance, operations, and information systems (IIA Standard 2110.A2).
- During consulting engagements, internal auditors should address risk consistent with the engagement's objectives and be alert to the existence of other significant risks (IIA Standard 2110.C1).
- Internal auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization (IIA Standard 2110.C2).

CORPORATE GOVERNANCE PRINCIPLES

Definition

Corporate governance refers to the method by which a firm is being governed, directed, administered, or controlled and to the goals for which it is being governed. It is concerned with the relative roles, rights, and accountability of such stakeholder groups as owners, boards of directors, managers, employees, and others who assert to be stakeholders.

Corporate Governance Principles and Issues

- Components of corporate governance.
- Roles of four major groups.
- Separation of ownership from control.
- Role of the board of directors.
- Need for board independence.
- Issues surrounding compensation. Major issues include CEO compensation and outside director compensation.
- Consequences of merger, acquisition, and takeover wave.
- Insider trading scandals.
- Board member liability.
- Improving corporate governance: (1) changes in boards of directors, and (2) increased role of shareholders.

ALTERNATIVE CONTROL FRAMEWORKS OR MODELS

Committee of Sponsoring Organizations (COSO)—United States

Definition of Internal Control

Internal controls have objectives, concepts, and components. *Internal control* is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.

Internal Control Components

Internal control consists of five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring.

Tiered Approach to Audits

When there is a conflict between the choices, the COSO-based approach should not override the risk-based approach to audits. Self-assessment questionnaires, which are soft controls, can be applied at any organizational level (first tier). The second tier is the activity level (e.g., process, subprocess, function, or department). Hard controls, such as documenting and testing control activities, are evaluated during the second tier. The best approach is analytical, starting from objectives, and then identifying risks and controls, evaluating the design of the controls, and testing control effectiveness.

Relationship of Internal Control Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and the components, which represent what is needed to achieve the objectives. Information is needed for all three objective categories—to effectively manage business operations, to prepare financial statements reliably, and to determine compliance. All five components are applicable and important to achievement of operations objectives. Each component cuts across and applies to all three objectives categories.

Responsibility for Internal Control

Who is responsible for establishing and ensuring an adequate and effective internal control environment within the organization? It is the management, the audit committee, and the board of directors—not the auditors. Auditors are responsible for ensuring an adequate and effective system of internal control in the organization.

According to the COSO study, everyone in an organization has responsibility for internal control: management, board of directors, internal auditors, and other personnel.

COSO's Internal Control Standards Summary

Standard 1: Control Environment

1.1 Integrity and ethical values

1.2 Commitment to competence

1.3 Management's philosophy and operating style

1.4 Organizational structure

1.5 Assignment of authority and responsibility

1.6 Human resources policies and practices

1.7 Oversight groups

Standard 2: Risk Assessment

2.1 Risk identification

2.2 Risk analysis

2.3 Managing risk during change

COSO's Internal Control Standards Summary (continued)

Standard 3: Control Activities

3.1 Types of control activities

3.2 Integration with risk assessment

3.3 Control over information systems

3.4 Entity-specific control activities

Standard 4: Information and Communication

4.1 Information

4.2 Communications

4.3 Means of communicating

Standard 5: Monitoring

5.1 Ongoing monitoring activities

5.2 Separate evaluations

5.3 Internal reporting of deficiencies

Limitations of Internal Control

- Internal control—even effective internal control—operates at different levels with respect to different objectives. For objectives related to the effectiveness and efficiency of an entity's operations—achievement of its basic mission, profitability goals, and the like—internal control can help to ensure that management is aware of the entity's progress, or lack of it. But it cannot provide even reasonable assurance that the objectives themselves will be achieved. The first set of limitations acknowledges that certain events or conditions are simply outside management's control.
- Internal control cannot provide absolute assurance with respect to any of the three objectives categories. The second set of limitations has to do with the reality that no system will always do what it is intended to do. The best that can be expected in any internal control system is that reasonable assurance is obtained.

Criteria of Control (CoCo)—Canada

The Canadian Institute of Chartered Accountants (CICA) has issued 20 “criteria of control” (CoCo) as a framework for making judgments about control. The term “control” has a broader meaning than internal control over financial reporting. CoCo defines control as “those elements of an organization (including its resources, systems, processes, culture, structure, and tasks) that, taken together, support people in the achievement of the organization’s objectives.” It defines three categories of objectives: effectiveness and efficiency of operations; reliability of internal and external reporting; and compliance with applicable laws, regulations, and internal policies.

CoCo Defines Four Types of Criteria: Purpose, Commitment, Capability, and Monitoring and Learning

The *purpose* type groups criteria that provide a sense of the organization's direction and address objectives (including mission, vision, and strategy); risks (and opportunities); policies; planning; and performance targets and indicators. The *commitment* type groups criteria that provide a sense of the organization's identity and values and address ethical values, including integrity, human resource policies, authority, responsibility, accountability, and mutual trust. The *capability* type groups criteria that provide a sense of the organization's competence and address knowledge, skills, and tools; communication processes; information; coordination; and control activities. The *monitoring and learning* type groups criteria that provide a sense of the organization's evolution and address monitoring internal and external environment, monitoring performance, challenging assumptions, reassessing information needs and information systems, follow-up procedures, and assessing the effectiveness of controls.

Control Self-Assessment (CSA)—United States

CSA deals with evaluating the system of internal control in any organization. CSA is a shared responsibility among all employees in the organization, not just internal auditing or senior management.

Elements of CSA

- Up-front planning and preliminary audit work
- Gathering of process owners with a meeting facilitator
- Structured agenda to examine the process's risks and controls
- Note-taker and electronic voting technology to input comments and opinions
- Reporting the results and the development of corrective action plans

Scope of CSA

CSA can be done either as a standalone project or as a supplement to traditional audit work. CSA is not suitable to situations such as finding fraud or compliance reviews (e.g., regulatory audits), or when participants have conflicting objectives, as in third-party contracts. CSA can be applied to numerous situations, business issues, and industries, regardless of size. It is a management tool that has equal application to horizontal (organization-wide), vertical (single department), or diagonal (process inquiries) issues.

Effect on Auditors

CSA can be used to assess business and financial statement risks, control activities, ethical values, and control effectiveness; the controls that mitigate those risks; and overall compliance with policies and procedures.

Interrelationships between CSA, CoCo, and COSO

CSA can be an effective tool for accomplishing the objectives of both CoCo and COSO. CSA acts as a link to the CoCo and COSO.

Cadbury Report—United Kingdom

The Cadbury Report of the committee on the financial aspects of corporate governance consists of internal controls, fraud, audit (internal and external), financial reporting practices, audit committees, shareholders, corporate governance, the board of directors, and the code of best practice.

The external auditors' role is to report whether the financial statements give a true and fair view, and the audit is designed to provide a reasonable assurance that the financial statements are free of material misstatements. The auditors' role is not (to cite a few of the misunderstandings) to prepare the financial statements, or to provide absolute assurance that the figures in the financial statements are correct, or to provide a guarantee that the company will continue to exist.

Turnbull Model—United Kingdom

The London Stock Exchange has developed a Combined Code for corporate governance that requires company directors to (at least annually) conduct a review of the effectiveness of the system of internal control and report to shareholders that they have reviewed the effectiveness of all three types of controls, including financial, operational, and compliance control.

King Model—South Africa

The Institute of Directors in South Africa has established the King Committee on Corporate Governance. The committee has developed a Code of Corporate Practices and Conduct, and compliance with the code is a requirement to be listed in the Johannesburg stock exchange Securities Exchange in South Africa.

KonTraG Model—Germany

The KonTraG model affects control and transparency in business, as part of reforming the corporate governance. Specifically, it impacts the board of directors, supervisory board, corporate capitalization principles, authorization of no-par-value shares, small nonlisted stock corporations, banks investing in industrial companies, and the acceptance of internationally recognized accounting standards.

ENTERPRISE RISK MANAGEMENT VOCABULARY, CONCEPTS, AND TECHNIQUES

Definition

Enterprise risk management (ERM) is defined as a rigorous and coordinated approach to assessing and responding to all risks that affect the achievement of an organization's strategic and financial objectives. This includes both upside and downside risks.

ERM risks are classified as follows: financial risk; hazard risk; strategic risk; operational risk.

ERM Vocabulary

Hazard is a condition that creates or increases the probability of a loss. Three types of hazards exist: physical hazard, moral hazard, and morale hazard.

Hedging is taking a position opposite to the exposure or risk.

Insurance is an economic device whereby an individual or a corporation substitutes a small certain cost (the premium) for a large uncertain financial loss (the claim, or contingency insured against) that would exist if it were not for the insurance policy (contract).

Insurable interest is an interest that might be damaged if the peril insured against occurs; the possibility of a financial loss to an individual or a corporation that can be protected against through insurance.

Natural hedges are created from the relationship between revenues and costs of a business unit or a subsidiary.

Peril is the cause of possible loss, the event insured against. “Open peril” is a term used to describe a broad form of property insurance in which coverage applies to loss arising from any fortuitous cause other than those perils or causes specifically excluded.

Portfolio effect considers risk and return of a firm when it is investing in acquisition or expansion projects.

Risk is a possibility of loss.

ERM Vocabulary (continued)

Pure risk is a condition in which there is the possibility of loss or no loss.

Speculative risk exists when there is uncertainty about an event that could produce either a profit or a loss.

Static risks, which can be either pure or speculative, stem from an unchanging society that is in stable equilibrium. Examples of pure static risk include the uncertainties due to such random events as lightning, windstorms, and death. In contrast, **dynamic risks** are produced because of changes in society. Dynamic risks also can be either pure or speculative. Examples of sources of dynamic risk include urban unrest, increasingly complex technology, and changing attitude of legislatures and courts about a variety of issues.

Subjective risk refers to the mental state of an individual who experiences doubt or worry as to the outcome of a given event. In addition to being subjective, a particular risk may be either pure or speculative and either static or dynamic.

Objective risk differs from subjective risk primarily in the sense that it is more precisely observable and therefore measurable. In general, objective risk is the probable variation of actual from expected experience.

Risk assessment (risk analysis) is the process of identifying the risks and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. It includes risk measurement and prioritization.

ERM Vocabulary (continued)

Risk financing includes internal funding for risks (self-insurance and residual risk) and external transfer of risks, such as insurance and hedging.

Risk management is the total process of identifying, controlling, and mitigating risks as it deals with uncertainty.

Risk mitigation includes designing and implementing controls and control-related procedures to minimize risks.

Risk monitoring includes internal and external reporting and feedback into risk assessment, continuing the loop.

Risk transfer involves payment by one party (the transferor) to another party (the transferee, or risk bearer). Five forms of risk transfer are: (1) hold-harmless agreements, (2) incorporation, (3) diversification, (4) hedging, and (5) insurance.

Self-insurance is a risk-retention program that incorporates elements of the insurance mechanism where the self-insured organization pays the claims rather than an insurance company.

Approaches to ERM

An ERM approach can be viewed in three dimensions:

1. The range of organization operations. This includes business units or locations, starting small as pilot projects and eventually rolling out to the entire enterprise (i.e., institutionalization).
2. The sources of risk (hazard, financial, operational, and strategic). This may include property catastrophe risk and currency risk.
3. The types of risk management activities or processes (risk identification, risk measurement, risk mitigation, and risk monitoring).

Alternative Risk-Transfer Tools

Five alternative risk-transfer tools, other than traditional insurance, include: (1) captives, (2) financial insurance, (3) multiline/multiyear insurance, (4) multiple-trigger policies, and (5) securitization. Multiple-trigger policies and securitization tools are more commonly used.

Implementation of ERM

Senior management support and commitment is needed to properly implement the ERM program in the organization. A dedicated group of cross-functional staff is needed to push it through the organization. Most organizations are implementing the ERM program incrementally. Some are beginning by layering additional sources of risk, one at a time, into their exiting processes for risk assessment and risk mitigation. Some are embracing all sources of risk at the outset, but are tackling the processes one at a time, with most starting with risk assessment. Others are taking on all risk sources and all processes, but on a small, manageable subset of their operations as a pilot project.

Internal Auditing in ERM Implementation

The CAE is an ERM champion and should use risk-based audit plans that are consistent with the organization's goals. Internal auditing is the implementation arm of an ERM program. Internal auditors act as facilitators in cross-functional risk assessment workshops conducted in the business units.

RISK/CONTROL IMPLICATIONS OF DIFFERENT ORGANIZATIONAL STRUCTURES

Organization Defined

An organization is “a system of consciously coordinated activities or forces of two or more persons.” In other words, when people gather together and formally agree to combine their efforts for a common purpose or goal, an organization is the result.

Organizations share four characteristics: (1) coordination of effort, (2) common goal or purpose, (3) division of labor, and (4) hierarchy of authority.

Classifying Organizations

Four categories of organizations exist, although some large and complex organizations have overlapping categories: (1) business organizations, (2) nonprofit service organizations, (3) mutual-benefit organizations, and (4) commonwealth organizations.

Theories of Organization

Two theories exist: the traditional view and the modern view. The traditional view has closed-system thinking, while the modern view incorporates open-system thinking.

Theories of Organizing

Several theories of organizing exist: bureaucracy, administrative theory, scientific management theory, human relations theory, and contingency design theory.

Types of Departmentalization

Two common forms of integration are through the hierarchical chain of command and departmentalization. Some integration is needed to offset the negative effects of differentiation. It is through departmentalization that related jobs, activities, or processes are grouped into major organizational subunits such as departments, divisions, groups, or units. Four basic types of departmentalization include: (1) functional departments, (2) product-service departments, (3) geographic location departments, and (4) customer classification departments.

RISK/CONTROL IMPLICATIONS OF DIFFERENT LEADERSHIP STYLES

The control environment has a pervasive influence on the way business activities are structured, objectives are established, and risks are assessed. It also influences control activities, information and communication systems, and monitoring activities.

Control Environment Factors

- Integrity and ethical values
- Commitment to competence
- Board of directors or audit committee
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices

Agents of Change

Organizations must change to survive in a competitive environment. This requires everyone in the organization believing in and accepting the change. Ideally, managers need to be architects or agents of change rather than the victims of change. When managers are acting as agents of change, their company will be much more responsive, flexible, and competitive. In addition to managers, internal auditors can act as change agents due to the nature of their work. Auditors facilitate change through their recommendations to management. Each recommendation auditors make requires some change in the existing policies, procedures, and practices or the creation of new ones.

How to Change

A corporation can change by reengineering business policies, processes, jobs, and procedures; outsourcing nonstrategic activities; partnering with major suppliers and customers; implementing total quality management programs; redesigning the organizational structure to fit the business strategy; renovating physical plants and facilities; installing computer-based systems and technologies; understanding one's own products, services, markets, and customers as well as those of competitors; and installing performance measurement methods and reward systems.

Types of Organizational Change

- Anticipatory change
- Reactive change
- Incremental change
- Strategic change

Resistance to Change

Organizational change comes in all forms, sizes, and shapes, and with varying degrees of impact and consequences for employees. Among the most common reasons for resistance to change are: surprise, inertia, misunderstanding, emotional side effects, lack of trust, fear of failure, personality conflicts, lack of tact, threat to job status or security, and breakup of work groups. *Management faces the challenge of foreseeing and neutralizing resistance to change, as the resistance is both rational and irrational.*

Factors in the Change Process

Internal auditors should consider the following factors of change process during their audit work: paradigm shift, motivating stakeholders, grapevine, employee empowerment, barriers to change, departmental border-crossing, performance measurement system, and cultural differences at workplace.

Organizational Development

Organizational development (OD) is a systematic approach to planned change programs intended to help employees and organizations function more effectively. OD combines the knowledge from various disciplines, such as behavioral science, psychology, sociology, education, and management. OD is a process of fundamental change in an organization's culture. For OD programs to be effective, not only must they be tailored to unique situations, but they also must meet the seven common objectives in order to develop trust:

1. Deepen the sense of organizational purpose and align individuals with that purpose.
2. Strengthen interpersonal trust, communication, cooperation, and support.
3. Encourage a problem-solving rather than a problem-avoiding approach to organizational problems.
4. Develop a satisfying work experience capable of building enthusiasm.
5. Supplement formal authority with authority based on personal knowledge and skill.
6. Increase personal responsibility for planning and implementing.
7. Encourage personal willingness to change.

CONFLICT MANAGEMENT

Conflict management involves accepting or even encouraging constructive conflict as necessary. The key point is to minimize the destructive form of conflict.

Personal Conflict Prevention and Control Methods

Although it is impossible to totally eradicate conflict, personal conflict prevention and control can avert much needless strife (unrealistic conflict). Both individuals and institutions need to develop prevention and control methods.

Group or Organizational Conflict Prevention and Control Methods

Individual actions alone are not enough. Group and/or organizational actions are needed to prevent and control the conflict that occurs in the workplace. The way an organization is structured has a bearing on the amount of conflict generated in it. The potential for conflict tends to be greater in centralized, bureaucratic organizations than in decentralized organizations. The more rigid institutions have less effective communication and are less adept at managing conflict constructively than are the organizations at the other end of the continuum.

MANAGEMENT CONTROL TECHNIQUES

Management controls, in the broadest sense, include the plan of organization, methods, and procedures adopted by management to ensure that its goals and objectives are met. Management controls, also known as *internal controls*, include accounting and administrative controls.

Traditional Management Controls

Management controls include the process for planning, organizing, directing, and controlling the entity's operations. They include the management control systems for measuring, reporting, and monitoring operations. Managerial control can be divided into feedforward and feedback controls. A feedforward control is a proactive control such as defect prevention, inspection, training, and budgeting. A feedback control is used to evaluate past activity to improve future performance. It measures actual performance against a standard to ensure that a defined result is achieved.

Contemporary Management Controls

Many new management controls have evolved over the years, including economic-value-added (EVA), market-value-added (MVA), activity-based costing (ABC), open-book management, and the balanced scorecard system.

TYPES OF CONTROL

Control Characteristics

Control is any positive and negative action taken by management that would result in accomplishment of the organization's goals, objectives, and mission. Controls should not lead to compulsion or become a constraint on employees. Controls should be natural and should be embedded in the organizational functions and operations. More so, controls should be accepted by the employees using or affected by them. Use and implementation of controls should be inviting, not inhibiting. Controls should be seen as beneficial from the employee's personal and professional viewpoints.

Control Requirements

The auditor needs to understand the control requirements of an application system or a business operation before assessing control strengths and weaknesses. In other words, there should be a basis or baseline in place (i.e., standards, guidelines, and benchmarks) prior to control measurement and assessment. In the absence of a baseline of standards, auditor's findings, conclusions, and recommendations will be questioned and will not be accepted by the auditee.

Combination, Complementary, and Compensating Controls

Combination Controls

Rarely would a single control suffice to meet control objectives. Rather, a combination of controls or complementary controls are needed to make up a whole and to provide a synergistic effect.

Complementary Controls

Complementary controls (hand-in-hand controls) have an important place in both the manual and the automated control environment. Complementary controls are different from compensating controls in that, in the latter category, weak controls in one area or function are balanced by strong controls in other areas or functions, and vice versa. A function or an area need not be weak to use complementary controls. Complementary controls can enhance the effectiveness of two or more controls when applied to a function, program, or operation.

Compensating Controls

Normally the auditor will find more control-related problems if it is a first-time audit of an area. Generally the more frequently an area is audited, the lower the probability of many control weaknesses. Therefore, determining the nature of efficient and effective operations needs both audit instinct and business judgment. During the control evaluation process, the auditor should consider the possibility of availability of compensating controls as a way to mitigate or minimize the impact of inadequate or incomplete controls. In essence, the concept of compensating controls deals with the balancing of weak internal controls in one area with strong internal controls in other areas of the organization. Here the word “area” can include a section within a user or IS department.

Control Assessment

During an assessment of control strengths and weaknesses, the auditor might run into situations where a business function, system, or manual/automated procedure is overcontrolled or undercontrolled. This means that there may be too many controls in one area and not enough controls in other areas. Also, there may be duplication or overlapping of controls between two or more areas. Under these conditions, the auditor should recommend to eliminate either some user controls, some IS controls, some manual controls, some automated controls, or a combination of them.

Cost-Benefit Analysis

A cost-benefit analysis is advised during the process of designing each type of control into an application system during its development and maintenance as well as during its operation. Ideally, costs should never exceed the benefits to be derived from installing controls. However, costs should not always be the sole determining factor, because it may be difficult or impractical to quantify benefits such as timeliness, improved quality and relevance of data and information, and improved customer service and system response time.

Costs versus Controls versus Convenience

Costs of controls vary with their implementation time and the complexity of the system or operation. Control implementation time is important to realize benefits from installing appropriate controls. There are **tradeoffs** among costs, controls, and convenience factors. The same is true among system usability, maintainability, auditability, controllability, and securability attributes of systems.

Control by Dimension

Control can be viewed through three different dimensions of timing: precontrol, concurrent control, and postcontrol. Control can also be viewed through two different dimensions of action: feedback control and feedforward control.

Specific Types of Controls

Controls prevent the adverse effects of risks. Specific types of controls include controls by function and controls by objectives. Controls by function include directive controls, preventive controls, detective controls, corrective controls, manual controls, computer controls, and management controls. Controls by objectives include data completeness, data timeliness, data accuracy, data authorization, and data consistency.

Controls in Business Application Systems

The scope of business application system controls includes controls over data origination, preparation, and data input; data processing; system-related file maintenance; data output; application system documentation; spreadsheet work; data integrity; and user satisfaction assessment.

Inventory of Controls in Business Application Systems

Application controls are designed to control computerized application systems, helping to ensure the completeness and accuracy of transaction processing, authorization, and validity. The following lists provide the nature of each control (preventive, detective, and corrective); the type of control (completeness, accuracy, continuity, authorization, consistency, and security) is indicated where necessary.

Preventive Controls

Brevity codes. This is an accuracy control.

Data attribute checks. This is an accuracy control.

Validity checks. This accuracy control is both a preventive control and a detective control.

Compatibility tests. This is a security control.

Processing parameters. This is a continuity control.

Prenumbered forms. This is a completeness control.

System-assigned numbers. This is an accuracy control.

Precoded forms/screens. This is an accuracy control.

Turnaround documents. This is an accuracy control.

Reference values or codes kept outside the program. This is a continuity control.

Transaction cancellation. This is a completeness control.

Management approvals. This is an authorization control.

Preventive Controls (continued)

Concurrent access controls. This is a security control.

Two-person controls. This is an accuracy control.

Overrides. This is both a security control and an authorization control.

Detective Controls

Summary integrity check. This is both an accuracy control and a completeness control, and similar to a batch-control technique.

Batch totals. This is both an accuracy control and a completeness control.

Hash totals. This is an accuracy control.

Limit check. This is an accuracy control.

Reasonableness test. This is an accuracy control.

Check digit. This is an accuracy control.

Overflow check. This is an accuracy control.

Format checks. This is an accuracy control.

Date checks. This is both an accuracy control and a continuity control.

Label check. This is a continuity control.

Completeness test. This is a completeness control.

Detective Controls (continued)

Range test. This is an accuracy control.

Range check. This is an accuracy control.

Discrete value check. This is a consistency control.

Record count. This is both an accuracy control and a continuity control.

Sign test. This is an accuracy control.

Size test. This is a completeness control.

Sequence check. This is a completeness control.

Duplicate checks. This is a completeness control.

Cross-field editing. This is a consistency control.

Cross-record editing. This is a consistency control.

System matching. This is a completeness control.

Detective Controls (continued)

Field combination tests. This is an accuracy control.

Run-to-run totals. This is both an accuracy control and a continuity control.

Suspense file. This is a completeness control.

Header and trailer record verification. This is an accuracy control.

Balance controls. This is an accuracy control.

System logging of transactions. This is a security control.

Comparison controls. This is a consistency control.

Computation controls. This is an accuracy control.

Ratio test. This is a consistency control.

Rounding technique. This is an accuracy control.

Relationship test. This is a consistency control.

Detective Controls (continued)

Descriptive read-back. This is an accuracy control.

Data checks. This is an accuracy control.

Key verification. This is an accuracy control.

One-for-one checking. This is both an accuracy control and a completeness control.

Cross footing. This is an accuracy control.

Corrective Controls

Program comments. This is a consistency control.

Job control comments. This is a consistency control.

Automatic error correction. This is a continuity control.

Overrides by supervisors. This is both a continuity control and an authorization control.

Audit trail report. This is an accuracy control.

Control report. This is an accuracy control.

Exception report. This is an accuracy control.

Error report. This is an accuracy control.

Before/after image record reporting for file maintenance. This is an accuracy control.

Clear and complete error messages. This is a continuity control.

Error total. This is an accuracy control.

Documentation. This is a continuity control.

Corrective Controls (continued)

Automatic backup and recovery. This is a continuity control.

Journaling. This is a continuity control.

Checkpoint control. This is a continuity control.

Transaction back-out. This is a continuity control.

Recovery logging. This is a continuity control.

Fallback procedure. This is a continuity control.

AUDIT PROCESS

Conducting an audit is a process with a series of activities to be reviewed and a series of procedures to be followed. A structured methodology, consisting of audit phases or stages, can be used during the audit process to ensure quality and to ensure that all required activities are accomplished—starting from the beginning of an audit to the completion of the audit. Each phase has defined tasks to be completed. Five such phases include (1) the preliminary survey, (2) the audit program, (3) fieldwork, (4) reporting, and (5) monitoring and follow-up. The audit report is the end product of the audit process.

AUDIT PLANNING

Two kinds of audit plans exist: (1) staff plans, and (2) audit plans.

Staff Plans

Staff planning should include assigning staff with the appropriate skills and knowledge for the job, assigning an adequate number of experienced staff and supervisors to the audit (consultants should be used when necessary), and providing for on-the-job training of staff.

Audit Plans

A written audit plan should be prepared for each audit and is essential to conducting audits efficiently and effectively. The form and content of the written audit plan will vary among audits. The plan generally should include an audit program and a memorandum or other appropriate documentation of key decisions about the objectives, scope, and methodology of the audit and of the auditors' basis for those decisions.

ANALYTICAL REVIEWS

As a part of fieldwork, the internal auditor should perform analytical reviews to understand the relationships between various data. The focus is on determining the reasonableness of data. Techniques such as regression analysis, simple ratio analysis, and trend analysis can be used to provide insights into the financial and operational data. The outcome of the review is to provide a "red flag" to the auditor so that he or she can adjust the audit scope and the audit procedures accordingly.

PLANNING MATERIALITY

Material errors, irregularities, and illegal acts will have a direct and material effect on financial statement amounts. *Materiality* is defined as the magnitude of a misstatement that would influence the judgment of a reasonable user of financial statements. Audit procedures must be designed to provide reasonable assurance of detecting material financial statement misstatements (i.e., material errors and irregularities). Thus, materiality refers to the level of precision (or accuracy) of the financial statements; the lower the materiality, the greater the precision and vice versa. From an internal audit viewpoint, materiality refers not only to the financial statements but also to the business operations and computer systems.

Types of Errors

Three types of errors can exist: (1) known errors (detected errors), (2) likely errors (estimated errors), and (3) possible errors (errors implicit in sampling work). Errors are defined as financial statement misstatements that are either intentional or unintentional.

Who Should Set the Materiality Level?

The auditor and the auditee should arrive at an understanding about the levels of materiality and the assurance level to be applied in an audit. This understanding should be based on cost-benefit considerations.

What Is Material and Immaterial?

Due professional care requires that the auditor consider the relative materiality or significance of matters to which audit procedures are applied. Various studies suggest that the magnitude of an error as a percentage of income is the most important factor in determining its materiality; items that have a more than 10% effect on income would normally be considered material, while items constituting less than 5% of income would normally be considered immaterial.

Qualitative versus Quantitative Materiality

Sometimes the nature of disclosure (sensitive or not) and the evidence of a desire to mislead (accidental or deliberate) are more important than quantitative factors. The auditor should weigh more toward human behavior. Quantitative materiality is applicable during the planning stage of an audit. Qualitative materiality is applicable during the evaluation stage of an audit since it is not practical to plan the audit to detect qualitative misstatements.

How to Compute Materiality

Materiality is computed by taking a base and multiplying that by a percentage. The base, in declining order of importance, includes total revenues, total expenditures, total assets, retained earnings, and income. The percentage used can be a flat percentage or one obtained from a sliding scale. A flat percentage is based on the notion that materiality is completely relative; a sliding scale is based on the notion that some amounts are large enough to be always material.

DETAILED RISK ASSESSMENT

Audit resources are limited and expensive, and hence they should be properly allocated and scheduled for maximum utilization. Risk models or risk analysis is often used in conjunction with development of long-range audit schedules. Performing risk analysis and risk assessment is a major step in audit planning work. A **risk** is defined as the probability that an unfavorable event occurs that could lead to a financial or other form of loss. The potential occurrence of such an event is called **exposure.** Risks are caused by exposures. Controls can reduce or eliminate risks and exposures.

Audit Risk Factors

High-risk areas should receive high priority while low-risk areas should be given low priority. A systematic risk assessment approach is better than a haphazard, trial-and-error approach. Potentially important audit risk factors include:

- Quality of internal control system (most important factor)
- Competence of management
- Integrity of management
- Size of unit
- Recent change in accounting system
- Complexity of operations
- Liquidity of assets
- Recent change in key personnel
- Economic condition of unit

Audit Risk Factors (continued)

- Rapid growth
- Extent of computerized data processing
- Time since last audit
- Pressure on management to meet objectives
- Extent of government regulation
- Level of employee morale
- Audit plans of independent auditors
- Political exposure
- Need to maintain appearance of independence by internal auditor
- Distance of unit from home office (least important factor)

Approaches to Risk Assessment

The purposes of risk analysis and assessment are to identify risks and exposures, calculate the damage or loss, and make cost-effective control recommendations. Several risk assessment techniques and approaches are available to quantify risks. Some of them, used in combination, are judgment and intuition, scoring approach, Delphi technique, and quantitative methods.

DETERMINING AUDIT OBJECTIVES AND SCOPE

Audit Objectives

Audit objectives are what the audit project is going to accomplish. Clearly defining the audit assignment objective(s) is a must at the beginning of each audit since it guides the extensiveness of internal control assessment, as well as the scope and methodology of the audit work. Audit assignments with broad objectives are generally more difficult to accomplish and require more staff resources and time than do assignments with specific objectives. Therefore, to the extent possible, audit objective(s) should be defined as precisely as possible to preclude unnecessary work, while concomitantly meeting the assignment's purpose.

Audit Scope

The *scope* of an internal audit is initially defined by the audit objectives. Preliminary survey, audit programs, audit project scheduling, and time estimates are driven by audit objectives. An example of an audit objective is evaluating whether cash receipts are adequately safeguarded. Scope is the boundary of the audit. Determining the scope of the audit is part of audit planning. It addresses such things as the period and number of locations to be covered. The audit scope should include financial, operational, and compliance audits.

Considerations for Audit Scope

Determining the audit scope normally involves matters such as the number of locations to be visited, time frames to be covered, and the type and depth of work needed to ensure that assignment objectives are accomplished and that all applicable audit standards are met.

Audit Scope Impairments

During the audit engagement, auditors may find scope impairments. When factors external to the audit organization and the auditor restrict the audit scope or interfere with the auditor's ability to form objective opinions and conclusions, the auditor should attempt to remove the limitation or, failing that, report the limitation.

AUDIT WORK PROGRAM

Preparing an **audit program** is the next step after completing the preliminary survey work. An audit program serves as a roadmap for the auditor. The audit program provides the auditor the necessary guidance to proceed with the detailed audit work in terms of audit procedures to be conducted and required audit evidence to be collected during the audit. The audit program should focus on major activities and key controls within and around such activities. Two types of audit programs exist: (1) standard audit program, and (2) customized audit program.

PLANNING THE AUDIT WORK

Planning and managing an audit assignment starts from developing work plans to completing the audit engagement. The majority of the audit work takes place in the fieldwork phase. In planning, auditors define the audit's objectives, scope, and methodology. Planning continues throughout the audit, and auditors should document their plan and changes to it. The most important task is to make sure that sufficient staff and other resources are available to do the audit work. The audit work can be done either at the headquarters (home office) and/or at the field offices.

Engagement Planning

- Internal auditors should develop and record a plan for each engagement, including the scope, objectives, timing, and resource allocations (IIA Standard 2200).
- Internal auditors should consider the objectives of the activity being reviewed and the means by which the activity controls its performance (IIA Standard 2201).
- Internal auditors should consider the significant risks to the activity, its objectives, resources, and operations, and the means by which the potential impact of risk is kept to an acceptable level (IIA Standard 2201).
- Internal auditors should consider the adequacy and effectiveness of the activity's risk management and control systems compared to a relevant control framework or model (IIA Standard 2201).
- Internal auditors should consider the opportunities for making significant improvements to the activity's risk management and control systems (IIA Standard 2201).

Engagement Planning (continued)

- When planning an engagement for parties outside the organization, internal auditors should establish a written understanding with them about objectives, scope, respective responsibilities, and other expectations, including restrictions on distribution of the results of the engagement and access to engagement records (IIA Standard 2201.A1).
- Internal auditors should establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding should be documented (IIA Standard 2201.C1).

Engagement Objectives and Scope

Engagement Objectives

- Audit objectives should be established for each engagement (IIA Standard 2210).
- Internal auditors should conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives should reflect the results of this assessment (IIA Standard 2210.A1).
- The internal auditor should consider the probability of significant errors, irregularities, noncompliance, and other exposures when developing the engagement objectives (IIA Standard 2210.A2).
- Consulting engagement objectives should address risks, controls, and governance processes to the extent agreed on with the client (IIA Standard 2210.C1).

Engagement Scope

- The established scope should be sufficient to satisfy the objectives of the engagement (IIA Standard 2220).
- The scope of the engagement should include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties (IIA Standard 2220.A1).
- If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards (IIA Standard 2220.A2).
- In performing consulting engagements, internal auditors should ensure that the scope of the engagement is sufficient to address the agreed-on objectives. If internal auditors develop reservations about the scope during the engagement, these reservations should be discussed with the client to determine whether to continue with the engagement (IIA Standard 2220.C1).

Engagement Resource Allocation

Internal auditors should determine appropriate resources to achieve engagement objectives. Staffing should be based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources (IIA Standard 2230).

Engagement Work Program

- Internal auditors should develop work programs that achieve the engagement objectives. These work programs should be recorded (IIA Standard 2240).
- Work programs should establish the procedures for identifying, analyzing, evaluating, and recording information during the engagement. The work program should be approved *prior to its implementation,* and any adjustments should be approved promptly (IIA Standard 2240.A1).
- Work programs for consulting engagements may vary in form and content depending on the nature of the engagement (IIA Standard 2240.C1).

Appendix: Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (SOX) contains provisions affecting the corporate governance, auditing, and financial reporting of public companies, including provisions intended to deter and punish corporate accounting fraud and corruption. The SOX act generally applies to those companies required to file reports with the SEC under the Securities Act of 1933 and the Securities Exchange Act of 1934.

Title 1—Public Company Accounting Oversight Board (PCAOB)

- Section 101: PCAOB establishment
- Section 102: Registration with the PCAOB
- Section 103: Auditing, quality control, and independence standards and rules
- Section 104: Inspections of registered public accounting firms
- Section 105: Investigations and disciplinary proceedings

Index

C

D

E

F

G

I