Comprehensive Update on Generally Accepted Auditing Standards (GAAS)

Presented by
Charles W. Hester
CPA, CFF, FCPA, CGFM, CFE, CFS
Course Objectives

- Participants will gain a greater understanding of:
  - Applying GAAS (SAS, SSAE, GAGAS, and IIA) and recent changes in these auditing standards.
  - Developing confidence in performing audits or being the recipient of an audit.
  - Reviewing practical implementation issues for government and non-government operations.
  - Considering the impact of International Auditing Standards.
  - Learning where standards are headed.

Who are the players?

- American Institute of CPAs (AICPA), Statements on Auditing Standards (SAS), Standards for Attestation Engagements (SSAE), and Quality Control Standards (SQCS)
  - www.aicpa.org
- International Federation of Accountants (IFAC), International Auditing and Assurance Standards Board (IAASB)
  - www.ifac.org
- Public Company Accounting Oversight Board (PCAOB)
  - www.pcaobus.org
- Government Accountability Office (GAO), Government Auditing Standards (GAGAS)
  - www.gao.gov
- The Institute of Internal Auditors (IIA), International Professional Practices Framework (IPPF)
  - www.theiia.org
AICPA Standards

- Generally Accepted Auditing Standards (AU)
- Attestation Standards (AT)
- Standards for Accounting and Review Services (AR)
- Standards for Consulting Services (CS)
- Standards for Valuation Services (VS)
- Quality Control Standards (QC)
- Ethics Standards (ET)

AICPA’s GAAS

- 10 Generally Accepted Auditing Standards consisting of:
  - 3 General Standards, 3 Standards of Fieldwork, and 4 Standards of Reporting
- Hierarchy of Authority:
  - Category 1 – Standards
  - Category 2 – Interpretive Publications
  - Category 3 – Other Auditing Publications
What’s new in the SASs

• SAS Number 70 – Service Organizations
• SAS Number 113 – Omnibus 2006
• SAS Number 114 – The Auditor’s Communication With Those Charged With Governance
• SAS Number 115 – Communicating Internal Control Related Matters Identified in an Audit
• SAS Number 116 – Interim Financial Information

SAS No. 70 – Service Organizations

• Issued – April 2010
• Effective – periods after June 15, 2011
• Significant provisions:
  – As part of ASB’s efforts to converge U.S. and International Standards, this SAS was replaced by 2 new Standards (SAS 70 & SSAE 16)
  • New SAS 70 based on the IAASB’s International Standard on Auditing No. 402

SAS No. 113 – Omnibus 2006

• Issued – November 2006
• Significant provisions:
  – Amends SASs 1, 57, 59, 85 95, 99, & 101
  • Revises the terminology used in the 10 standards in SAS 95 to reflect the terminology used in SAS 102, Defining Professional Requirements in Statements on Auditing Standards
  • Adds a footnote to SAS 99 to provide a clear link between the auditor’s consideration of fraud and the auditor’s assessment of risk and the auditor’s procedures in response to those assessed risks
  • Replaces, throughout the SASs, the term “completion of fieldwork” with the term “date of the auditor’s report”
SAS No. 114 – The Auditor’s Communication With Those Charged With Governance

• Issued – December 2006 – Supersede SAS 61
• Effective – periods after Dec. 15, 2006
• Significant provisions:
  – Auditor MUST communicate with those charged with governance significant audit matters relevant to the responsibilities of overseeing the financial reporting process
  – Those charged with governance = those responsible for overseeing the strategic direction of the entity and obligations related to the accountability of the entity
  – Management = Those responsible for achieving the objectives of the entity who have the appropriate authority
  – Management is responsible for the financial statements, including designing, implementing, and maintaining effective internal control over financial reporting

SAS No. 114 – Continued

• Additional Significant provisions:
  – Document the form, timing and expected content of communications
  – Communicate significant findings in writing if oral communication would not be adequate
  – Requirement to evaluate the two-way communication between the auditor and those charge with governance
  – Document significant matters communicated
  – Communicate conditions that indicate that there could be substantial doubt about the entity’s ability to continue as a going concern

SAS No. 115 – Communicating Internal Control Related Matters Identified in an Audit

• Issued – December 2008 – Supersede SAS 112
• Effective – periods after Dec. 15, 2009
• Significant provisions:
  – Defines the terms deficiency in internal control, significant deficiency, and material weakness
  – Provides guidance on evaluating the severity of deficiencies in internal control identified in an audit of financial statements
  – Requires the auditor to communicate, in writing, significant deficiencies and material weaknesses identified in an audit
SAS No. 116 – Interim Financial Information

• Issued – January 2009 – Supersedes SAS 71
• Effective – periods after Dec. 15, 2009
• Significant provisions:
  – Provides guidance on the nature, timing, and extent of the procedures to be performed by an independent accountant when conducting a review of interim financial information

What’s else is new in the SASs

• SAS Number 117 – Compliance Audits
• SAS Number 118 – Other Information in Documents Containing Audited Financial Statements
• SAS Number 119 – Supplementary Information in Relation to the Financial Statements as a Whole
• SAS Number 120 – Required Supplementary Information

SAS No. 117 – Compliance Audits

• Issued – December 2009 – Supersedes SAS 74, primarily developed to respond 2007 Single Audit Project
• Effective – periods after June 15, 2010
• Significant provisions:
  – Establishes standards and provides guidance on performing and reporting on an audit of an entity’s compliance with applicable government grant and/or contract
  – Reflects changes in the government audit environment and incorporates the risk assessment standards
  – Requires the auditor to adapt and apply the AICPA’s Professional Standards to a compliance audit and provides guidance on how to do so
Communication with Those Charged with Governance

- Amends AU 801 to require the auditor to communicate the following:
  - The auditor’s responsibility under GAGAS, as well as SAS Nos. 99, 114, and 115
  - An overview of the planned scope and timing of the compliance audit
  - Significant findings from the compliance audit
  - Significant deficiencies and material weaknesses in internal control over compliance

Determine Programs and Compliance Requirements to Test

- Consult the OMB Circular A-133 Compliance Supplement
- Read laws, regulations, rules and provisions of contracts or great agreements
- Make inquiries of management and other knowledgeable individuals
- Read minutes of governing board meetings
- Read documentation of applicable compliance requirements from previous audits

Perform Risk Assessment Procedures

- Inquire of management about reports by others with findings
- Obtain an understanding of management’s response to findings
- Use the information obtained to assess risk and determine the nature, timing, and extent of compliance audit procedures
Factors Influencing the Nature and Extent of Risk Assessment Procedures

- Nature and complexity of applicable compliance requirements
- Length of time the requirements have existed
- Auditor’s knowledge of the entity’s internal control over compliance
- Services provided and how external factors affect the services
- Amount of oversight by the grantor
- Ways management addresses findings

Assess Risks of Material Non-compliance

- Complexity of the requirements, their susceptibility to non-compliance and the length of time the entity has been subject to them – for example
  - Does the entity have financial difficulties that present an increased risk of grant/contract funds being used for unauthorized purposes, or
  - Does the entity have poor record-keeping for government programs

Tests of Details and Transactions

- Tests of controls and perform substantive analytical procedures of:
  - Grant disbursements or expenditures
  - Eligibility files
  - Cost allocation plans
  - Periodic reports filed with grantor agencies
  - Compliance Supplement requirements
Obtain Management Representations

- It is responsible for understanding and complying with requirements
- For establishing and maintaining controls that provide reasonable assurance of compliance
- Has identified and disclosed all government programs and related activities
- Has made available all contracts and grant agreements
- Has disclosed all known non-compliance
- Has disclosed any communications from grantors regarding possible non-compliance
- Is responsible for taking corrective action on all findings

Address Subsequent Events

- Relevant reports issued by internal auditors
- Reports issues by other auditors indentifying non-compliance
- Reports on non-compliance issued by grantor and pass-through entities
- Information about non-compliance obtained through other engagements performed for the entity
OMB Guidance

• OMB Circular A-133 = Audits of States, Local Governments and Non-Profit Organizations, dated June 26, 2007
• OMB Circular A-133 Compliance Supplement, dated June 2010

AICPA’s Audit Risk Alert

• Government Auditing and Circular A-133 Developments 2010
  – Audit Risk – Audits in Accordance with A-133
  – Understanding the Entity and Its Environment and Assessing the Risk of Material Non-Compliance
  – Legislative and Regulatory Developments
  – Audit and Attestation Issues and Developments
  – Internal Control Issues and Developments
  – Other Recently Issued Audit Guidance

SAS No. 118 – Other Information in Documents Containing Audited Financial Statements

• Issued – February 2010
• Effective – periods after Dec. 15, 2010
• Significant provisions:
  – Eliminates the distinction between other information included in an auditor-submitted document and that in a client-prepared document
  – Establish presumptive mandatory requirements that the auditor
    • Make appropriate arrangements to obtain the other information prior to the report release date
    • Communicate the auditor’s responsibility with respect to the other information
    • Identifies a material inconsistency or misstatement of fact prior to the report release date, the auditor communicate that matter to those charged with governance
SAS No. 119 – Supplementary Information in Relation to the Financial Statements as a Whole

- Issued – February 2010
- Effective – periods after Dec. 15, 2010
- Significant provisions:
  - Establishes a presumptively mandatory requirement that:
    - In order to opine on whether supplementary information is fairly stated the auditor determine that specific conditions are met
    - The auditor obtain the agreement of management that it acknowledges and understands its responsibility
    - In order to opine that auditor performs specific procedures using the same materiality level used in the audit of the financial statements

SAS No. 120 – Required Supplementary Information

- Issued – February 2010
- Effective – periods after Dec. 15, 2010
- Significant provisions:
  - Defines required supplementary information
  - Defines designated accounting standard setter
  - Establishes a presumptively mandatory requirement that:
    - The auditor apply specific procedures to required supplementary information
    - If the auditor is unable to apply the specific procedures, the auditor consider whether management contributed to the inability to complete the procedures, the auditor inform those charged with governance
    - The Auditor include an explanatory paragraph in the report on the financial statements to refer to the required supplementary information

Proposed SASs

- ASB Clarity Project – redrafting all sections of the Codification of SASs
  - Significant provisions:
    - Link ASB Standards with International Standards
      - Had been occurring informally over the past several years
    - New SASs will use the related ISA as the base standard
      - ASB would modify the SAS only where modifications are deemed necessary to better service the needs of U.S. users of audited financial statements or non-issuers, or
      - Where modifications are appropriate for U.S. legal or regulatory reasons
What’s new in the SSAEs

- SSAE Number 16 – Reporting on Controls at a Service Organization
  - Issued – April 2010
  - Effective – periods after June 15, 2011
  - Significant provisions
    - Auditor is required to obtain a written assertion from management about the subject matter of the engagement
    - Suitable criteria are used to measure, present and evaluate the subject matter
    - Auditor may not use evidence obtained in prior engagements
    - Auditor is required to identify in tests of controls any tests performed by internal auditors
    - Auditor’s examination report must contain identified elements

What’s new in the SQCSs

- SQCS Number 7 – A Firm’s System of Quality Control
  - Effective – periods after Jan. 1, 2009
  - Significant provisions
    - Two types of Peer Review: System Reviews focus on a firm’s system of quality control, while Engagement Review focus on work performed on selected non-audit engagements
    - Three types of Peer Review Reports: Pass, Pass with Deficiencies, and Fail

Results of AICPA Peer Review

1. Failure to document observation and inspection procedures.
2. Failure to document risk assessment procedures.
3. Failure to link risk assessments to actual procedures performed.
4. Failure to properly use electronic third-party practice aids.
Proposed SSAEs & SQCSs

- DRAFT SSAE – Reporting on Compiled Prospective Financial Statements When the Practitioner’s Independence Is Impaired, dated June 3, 2010
- DRAFT SQCS – A Firm’s System of Quality Control (Redrafted), dated June 1, 2009
The International Auditing and Assurance Standards Board (IAASB)

- New structure for International Standards on Auditing (ISAs) and International Standards on Quality Control (ISQCs)
  - Part I = Scope of Handbook and How it is Arranged
  - Part II = Framework
    - 1000-1100 = International Auditing Practice Statements (IAPSs)
    - 2000-2699 = International Standards on Review Engagements (ISREs)
    - 3000-3699 = International Standards on Assurance Engagements (ISAEs)

The Sarbanes-Oxley Act of 2002 (P.L. 107-204)

- New public company accounting oversight board (PCAOB)
- New roles for audit committees and auditors
- Criminal penalties and whistleblower protection
- Financial reporting and additions to the audit process
**New Public Company Accounting Oversight Board**

- Majority of board are non-CPAs
- Funded by mandatory fees on registered firms
- Board will set standards for the CPAs
- Board can investigate and discipline registered firms
- Board also responsible for foreign firms auditing US-traded public companies

**New roles for audit committees and auditors**

- Report to audit committee, not management
- Audit committee must approve all services
- CPA must provide certain information to committee
- Auditor cannot offer specified non-audit services
- Lead audit/review partner rotated at least every 5 years
- Employment limitations on CPA firm

**Criminal penalties and whistleblower protection**

- Failure to maintain working papers is now a felony!
- Destroying documents in federal or bankruptcy investigation is a felony!
- Increased criminal penalties for securities fraud
- Statute of limitations for fraud has been extended
- Many other significant provisions
Financial reporting and additions to the audit process

- Second partner review and approval of audit reports
- Management must assess and make representations about the effectiveness of internal control processes
- Audit reports must contain a description of the testing of internal controls

PCAOB Standards

- Auditing
- Attestation
- Ethics and Independence
- Quality Control
- Guidance Related to Standards

PCAOB Auditing Standards

- AS No. 1 – References in Auditors’ Reports to the Standards of PCAOB
- AS No. 3 – Audit Documentation
- AS No. 4 – Reporting on Whether a Previously Reported Material Weakness Continues to Exist
- AS No. 5 – An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements
- AS No. 6 – Evaluating Consistency of Financial Statements
- AS No. 7 – Engagement Quality Review
PCAOB Attestation (Interim) Standards

- AT 101 – Attest Engagements
- AT 201 – Agreed-Upon Procedures Engagements
- AT 301 – Financial Forecasts and Projections
- AT 401 – Reporting on Pro-Forma Financial Information
- AT 601 – Compliance Attestation
- AT 701 – Management’s Discussion and Analysis

PCAOB Ethics & Independence Rules

- 3501 – Definition of Terms Employed in Section 3, Part 5 of Rules
- 3502 – Responsibility Not to Knowingly or Recklessly Contribute to Violations
- 3520 – Auditor Independence
- 3521 – Contingent Fee
- 3522 – Tax Transactions

PCAOB Ethics & Independence Rules - Continued

- 3523 – Tax Services for Persons in Financial Reporting Oversight Roles
- 3524 – Audit Committee Pre-approval of Certain Tax Services
- 3525 – Audit Committee Pre-approval of Non-audit Services Related to Internal Control Over Financial Reporting
- 3526 – Communication with Audit Committee Concerning Independence
Interim Ethics & Independence

• Adopted AICPA’s Code of Professional Conduct:
  – ET 101 – Independence
  – ET 102 – Integrity and Objectivity
  – ET 191 – Ethics Rulings on Independence, Integrity, and Objectivity
• Adopted the AICPA’s Independence Standards Board:
  – ISB No. 2 – Certain Independence Implications of Audits of Mutual Funds and Related Entities
  – ISB No. 3 – Employment with Audit Clients
  – ISB Interpretation 99-1 – Impact on Auditor Independence of Assisting Clients in the Implementation of FAS 133 (Derivatives)

Quality Control

• Adopted AICPA’s Quality Control Standards:
  – QC 20 – System of Quality Control for a CPA Firm’s Accounting and Auditing Practice
  – QC 30 – Monitoring a CPA Firm’s Accounting and Auditing Practices
  – QC 40 – The Personnel Management Element of a Firm’s System of Quality Control – Competencies Required by a Practitioner-in-Charge of an Attest Engagement

Supreme Court Questions
PCAOB’s Constitutionality

• Actual questions before the Court:
  1. Whether SOX violates the Constitution’s separation of powers doctrine.
  2. Whether, under the appointments clause, PCAOC member are “inferior officers.”
  3. If PCAOB members are inferior officers, whether the Act’s provisions for their appointment by the SEC violates the appointments clause.
Supreme Court Ruling on June 28, 2010

• PCAOB technically lost in a 5 to 4 decision that is 113 pages long.
  – The Court rules that the tenure of PCAOB members is unconstitutional, but held that “Board’s existence does not violate the separation of powers.”

Now when will the next shoe fall?

• OMB Circular No. A-123, Management Accountability and Control
• OMB Circular No. A-127, Financial Management Systems
• OMB Circular No. A-130, Management of Federal Information Resources
OMB Circular A-123, Management Accountability and Control

- Revised December 21, 2004 (Effective beginning with Fiscal Year 2006)
- Applies to Federal managers
  - But has useful ideas and may be coming to State & Locals soon
- Changed emphasis from prior version

OMB Circular A-123 - Continued

- Purpose of Management Controls
  - Programs achieve intended results
  - Resources used consistent with mission
  - Programs and resources protected from fraud, waste, and mismanagement
  - Laws and regulations are followed
  - Reliable and timely information obtained, maintained, reported, and used to make decisions

OMB Circular A-123 - Continued

- Cites Government Performance and Results Act (GPRA) of 1993 and Sarbanes-Oxley Act (SOX) of 2002
  - Agencies must:
    • Develop strategic plans
    • Set performance goals
    • Compare actual performance to goals
OMB Circular A-123 - Continued
• Controls are an integral part of the Management Process
  – Controls are not an isolated management tool
  – Integrate GPRA & SOX activities with other improvement efforts
  – Management controls are part of cycle of planning, budgeting, management, accounting and auditing

OMB Circular A-123 - Continued
• Consider overall impact
  – Balance of controls
  – Too many can cause inefficiency
  – Managers should benefit from controls, not be encumbered by them

OMB Circular A-123 - Continued
• Federal managers must evaluate controls
  – Reporting reflects commitment to improvement (supportive attitude)
  – Failing to report a known deficiency would reflect adversely on the agency
OMB Circular A-127, Financial Management Systems

- Revised July 23, 1993
- Transmittal Memorandum No. 2,
  - issued June 10, 1999
- Transmittal Memorandum No. 3,
  - Issued December 1, 2004
- Revised January 9, 2009
- Applies to Federal managers
  - But has useful ideas
- Changed emphasis from prior version

OMB Circular A-127 - Continued

- Prescribes policies and standards for developing, operating, evaluating and reporting on financial management systems
  - Collecting, processing, maintaining, transmitting, and reporting data about financial events
  - Supporting financial planning or budgeting activities
  - Accumulating and reporting cost information
  - Supporting the preparation of financial statements

OMB Circular A-127 - Continued

- Financial Management System Requirements
  - Agency-Wide Financial Information Classification Structure
  - Integrated Financial Management System
    - Common Data Elements
    - Common Transaction Processing
    - Consistent Internal Controls
    - Efficient Transaction Entry
OMB Circular A-127 -
Continued

• Financial Management System
  Requirements – Continued
  – Application of the U. S. Government Standard
    General Ledger (SGL) at the Transaction
    Level
    • Data in Financial Reports Consistent with the
      SGL
    • Transaction Recorded Consistent with SGL
      Rules
    • Supporting Transaction Detail for SGL Accounts
      Readily Available

OMB Circular A-127 -
Continued

• Financial Management System
  Requirements - Continued
  – Federal Accounting Standards (FASAB)
  – Financial Reporting
    • Agency Financial Management Reporting
    • Performance Measures
  – Budget Reporting
  – Functional Requirements

OMB Circular A-130, Management
of Federal Information Resources

• Revised November 28, 2000
• Provides uniform government-wide
  information resources management
  policies
• Includes procedural and analytical
  guidelines for implementing specific
  aspects of the policies
Generally Accepted Government Auditing Standards (GAGAS)

- Where are they now?
- Where are they going?

History of GAO Auditing Standards

- Initially Issued 1972
- Amendment No. 1, dated May 1999
- Amendment No. 2, dated July 1999
- Amendment No. 3, dated January 2002
- 2003 Revision (2005 Amendments)
- January 2007 Revisions
- July 2007 Revisions
- August 2010 Exposure Draft
Initial Standards, Issued 1972

- General Standards (4)
- Examination and Evaluation Standards (5)
- Reporting Standards (4)
  - Audit Standards Supplement Series (Number 1 through Number 14)
  - Illustrative only, not authoritative
- Additional GAO Publications
  - Guidelines for Financial and Compliance Audits of Federally Assisted Programs
  - Lessons Learned During Performance of GAO Audit Assignments

1981 Revisions to GAGAS

- Chapter 1 – Introduction
- Chapter 2 – Summary of Standards
- Chapter 3 – Scope of Audit Work
- Chapter 4 – General Standards
- Chapter 5 – Examination and Evaluation (Field Work) and Reporting Standards - Financial and Compliance Audits
- Chapter 6 – Examination and Evaluation Standards - Economy and Efficiency Audits and Program Results Audits
- Chapter 7 – Reporting Standards - Economy and Efficiency Audits and Program Results Audits
- Appendix – Auditing Computer-Based Systems: Auditor's Role During System Design and Development

1988 Revisions to GAGAS

- Chapter 1 – Introduction
- Chapter 2 – Types of Government Audits
- Chapter 3 – General Standards
- Chapter 4 – Field Work Standards for Financial Audits
- Chapter 5 – Reporting Standards for Financial Audits
- Chapter 6 – Field Work Standards for Performance Audits
- Chapter 7 – Reporting Standards for Performance Audits
1994 Revisions to GAGAS

- Same Chapter order – 1 through 7
- Emphasized auditor’s responsibility
  1. The audit is conducted by personnel who collectively have the necessary skills,
  2. Independence is maintained,
  3. Applicable standards are followed in planning and conducting audits and reporting the results,
  4. The organization has an appropriate internal quality control system in place, and
  5. The organization undergoes and external quality control review.

GAGAS Amendment Number 1

- Documentation Requirements When Assessing Control Risk at Maximum for Controls Significantly Dependent Upon Computerized Information Systems
  - Issued May 1999
  - Effective for Financial Statement audits of periods ending September 30, 1999
  - GAO’s Assessing the Reliability of Computer-Processed Data, dated October 2002

GAGAS Amendment Number 2

- Auditor Communication
  - Issued July 1999
  - Effective for Financial Statement audits of periods ending January 1, 2000
GAGAS Amendment
Number 3

• Independence
  – Issued January 2002
  – Effective for all audits of periods on or after October 1, 2002
  • GAO’s Answers to Independence Standard Questions, dated July 2002
    – July 2007 paragraph reference update to July 2007 GAGAS

2003 Revisions to GAGAS

• Pre-2003
  – Chapter 1, Introduction
  – Chapter 2, Types of Government Audits
  – Chapter 3, General Standards
  – Chapter 4, Field Work Standards for Financial Audits
  – Chapter 5, Reporting Standards for Financial Audits
  – Chapter 6, Field Work Standards for Performance Audits
  – Chapter 7, Reporting Standards for Performance Audits

• 2003 Revision
  – Chapter 1, Introduction
  – Chapter 2, Types of Government Audits and Attestation Engagements
  – Chapter 3, General Standards
  – Chapter 4, Field Work Standards for Financial Audits
  – Chapter 5, Reporting Standards for Financial Audits
  – Chapter 6, General, Field Work and Reporting Standards for Attestation Engagements
  – Chapter 7, Field Work Standards for Performance Audits
  – Chapter 8, Reporting Standards for Performance Audits

Major Changes Between 1994 and 2003 GAGAS

• Defined the types of audits and attestation engagements and the applicable Standards
• Consistent application of GAGAS where applicable
• Additions to strengthen Standards and clarify language
### GAO’s Guidance on GAGAS

#### Requirements for Continuing Professional Education

- Issued April 2005
  - Who is subject to CPE requirements?
  - How should compliance with CPE requirements be measured?
  - What qualifies as acceptable CPE?
  - Measuring CPE hours?
  - How are CPE requirements to be administered?

### January 2007 Revisions to GAGAS

- Issued January 31, 2007
- Superseded the 2003 Revisions – and prior revisions and amendments
- Contained final 2006 Proposed Revisions except for quality control and peer review sections
  - At same time issued exposure draft requesting comments on re-drafted sections on quality control and peer review

### July 2007 Revisions to GAGAS

- Supersedes the January 2007 Revision and prior revisions and amendments
- Finalizes the quality control and peer review sections
- Issued technical changes from the January 2007 revision to address posed questions and for consistency regarding the use of terms to define auditor requirements
- Issued a summary of Major Changes from the 2003 Standards
Government Auditing Standards: Implementation Tool

• Professional Requirements Tool for Use in Implementing Requirements Identified by “Must” and “Should” in July 2007 Revision of Government Auditing Standards
  – General Requirements for Audit Organizations
  – Specific Requirements for Financial Audits
  – Specific Requirements for Attestation Engagements
  – Specific Requirements for Performance Audits
    • Issued December 2007

Need to stay up-to-date!

• Professional Standards Update No. 50, dated September 2008
• Interim Guidance on Reporting Deficiencies in Internal Control for GAGAS Financial Audits and Attestation Engagements, dated November 2008
• Minutes of the Advisory Council on Government Auditing Standards

Yellow Book Essentials — Part 1

• We will cover:
  – Basic information about the Yellow Book
  – The major changes to the current Yellow Book
    • Chapter 1 – Use and Application of GAGAS
    • Chapter 2 – Ethical Principles in Government Auditing
    • Chapter 3 – General Standards
The Yellow Book is available online

You can access the Yellow Book online

http://www.gao.gov/new.items/d07731g.pdf

Basic information about the Yellow Book

- It is mandatory in most circumstances
- It covers
  - Financial audits
  - Attestations engagements
  - Performance audits
- For financial audits and attestations
  - It incorporates all AICPA standards
  - It has additional requirements

Major changes in the July 2007 issuance

- Terminology made consistent with AICPA and PCAOB guidance
- Greater emphasis placed on auditors’ ethical responsibilities
- Clarification of the independence standard regarding non-audit services
- Enhanced standards for performance audits
- Internal control terminology consistent with new SASs and SSAEs
GAGAS terminology has changed

- Mandatory requirements use “must” or “is required”
- Presumptively mandatory requirements use “should”
- Explanatory material uses “may,” “might” or “could”
- This terminology conforms to AICPA and PCAOB standards

Chapter 1: Use and Application

- Some basic concepts
  - Auditing is essential for government accountability
  - GAGAS helps to ensure high quality work
  - Government audits are intended to provide “an independent, objective, non-partisan assessment”
  - Government officials are accountable to legislatures, public and others
  - Auditors must consider entire text of GAGAS when conducting audits

Auditors should explain the extent of their compliance with GAGAS

- Unmodified: audit conformed to GAGAS
- Modified: audit conformed to GAGAS except for …
  - Should explain reason for not following some standards
  - Disclose impact on report of missed requirements
Auditors can use GAGAS in conjunction with other standards

- AICPA’s SASs for financial audits
- AICPA’s SSAEs for attestation engagements
- PCAOB standards for publicly traded companies
- International Auditing and Assurance Standards Board for international audits
- IIA’s International Standards for the Professional Practice of Internal Auditing
- Others

Other Standards Available

- Quality Standards for Federal Offices of Inspector General, issued by the P.C.I.E. in October 2003
- Quality Standards for Inspections, issued by the P.C.I.E. in January 2005
- Quality Standards for Investigations, issued by the P.C.I.E. in December 2003

Financial Audits

- New standards applicable to audits of periods starting after Dec. 31, 2007
- Primary purpose is to express opinion on fairness of financial statements
- Can be segments of financial statement or special reports
- Include compliance audit work included in OMB Circular A-133 audits
Attestation Engagements

• Applicable to attestations of periods starting after Dec. 31, 2007
• Covers a subject matter or management assertion
• Can cover broad range of financial and non-financial objectives
• Three Levels of attestation engagements

Three Levels of Attestation Engagements

• Examination Level
  – Sufficient testing to express an opinion
  – With the Yellow Book requirements, it is essentially the same as an audit
• Review Level
  – Sufficient testing to conclude whether any information came to the auditor’s attention that the subject matter or assertion was not fairly presented
• Agreed-Upon Procedures
  – Auditors report results of specific procedures performed on subject matter

Performance Audits

• Applicable to audits starting after Dec. 31, 2007
• Evaluation against stated criteria
• Synonymous with:
  – Program or performance evaluations
  – Economy and efficiency audits
  – Operational audits
  – Compliance audits
  – Management audits
Audit organizations can provide non-audit services

- Non-audit services are not covered by GAGAS
- Therefore must not cite GAGAS
- Need to consider whether non-audit services impact auditor’s independence

Chapter 2: Ethical Principles

- Government audits are essential for accountability
- Top audit management must set the right tone
- Ethics are also a personal responsibility
- Important to maintaining independence

Ethical concepts consider

- Public interest
- Integrity
- Objectivity
- Proper use of government information, resources and position
- Professional behavior
Definition of Ethics

“Professionally right or befitting; conforming to professional standards of conduct.”

Public Interest

• “Collective well-being” of the community of people and entities the audit organization serves.

Integrity

• Includes auditors conducting their work with an attitude that is objective, fact-based, non-partisan, and non-ideological with regard to the auditee and the users of the audit report.
  – Also includes being honest, candid and constructive
Objectivity

- Being independent if fact and appearance when providing audit and attestation services, maintaining an attitude of impartiality, having intellectual honesty and being free of conflict of interest.

Use of Information, Resources and Position

- Proper use of Government information, resources and position – not inappropriately for the auditor’s personal gain or in a manner contrary to law or detrimental to the legitimate interests of the auditee or the audit organization.
  – Includes proper handling of sensitive or classified information or resources.

Professional Behavior

- Compliance with laws and regulations and avoidance of any conduct that might bring discredit to the auditor’s work.
  – Also putting forth an honest effort in performance of their duties and services in accordance with relevant technical and professional standards.
Definition of Integrity

“Uncompromising adherence to ethical principles.”

Chapter 3: General Standards

• Covers all governmental audits and attestation engagements
  – Independence
  – Professional judgment
  – Competence
  – Quality control systems and peer reviews
• In addition to field work and reporting standards

Independence (Standard No. 1)

• Applies to audit organization and auditors
• Must be free of personal, external and organizational impairments
• Independent in fact and appearance
• If there is an impairment
  – Preferably, decline assignment
  – If cannot decline, disclose in GAGAS compliance scope section
Auditors should consider independence of specialists

- Specialists should be able to work and report impartially
- Should not employ specialists who are not independent

Examples of personal impairments

- Immediate family or close family member is key person in auditee
- Direct financial interest or significant indirect financial interest
- Management or decision-making responsibility for auditee
- Auditor maintained organization’s records
- Preconceived ideas or biases
- Seeking employment with the auditee

Personal impairments

- Organization should have system to
  - Establish procedures to identify and resolve personal impairments
  - Communicate policy to all auditors
  - Establish procedures to monitor compliance
  - Establish a disciplinary mechanism to promote compliance
  - Stress importance of independence
  - Document steps taken
Examples of external impairments

- Pressure to inappropriately reduce scope or extent of work
- Unreasonable restrictions on time allowed or access to records
- Interference on assignment, appointment and promotion of audit personnel
- Authority to determine report content
- Threat to replace auditor for inappropriate reasons

Organizational impairments

- Independence can be impacted by:
  - Audit organization’s place in entity
  - Non-audit services provided

No assumed organizational impairments for external reports if

- Audit organization is external to auditee
  - Assigned to different level of government (For example, Federal vs. state)
  - Assigned to difference branch of government
- Or audit organization’s head is
  - Directly elected
  - Appointed by, removable by and reports to legislative body
  - Appointment is confirmed by legislature
  - Accountable to independent body
OK for external audits with all the following **statutory** protections

- Preventing abolishment of audit agency
- Preventing arbitrary firing the audit head
- Preventing auditee from interfering in conduct or reporting of audit
- Requiring regular reports to legislature or other independent body
- Allowing audit organization sole authority to hire, fire and promote
- Ensuring audit organization has access to auditee records

OK for internal audits if the audit head meets **all** following criteria

- Accountable to head/deputy of government body
- Reports directly to head/deputy
- Organizationally located outside the staff or line management function of the auditee
- Has access to those charged with governance

Other provisions for internal reporting

- Sufficiently removed from political pressure
- Reports regularly to independent audit committee or oversight body
- Documents conditions that allow it to be considered independent
Organizational independence when performing non-audit services

- Audit organization must evaluate whether non-audit services create independence impairment in fact or in appearance
- Should consider past non-audit services
- Should set policies to avoid impairments to independence

Two overarching principles

- Auditors must not perform management functions or make management decisions
- Auditors must not audit their own work or provide non-audit services in situations where the amounts or services involved are significant/material to the subject matter of the audit

Three possibilities for non-audit services

- Do not impair auditor independence
- Do not impair independence if supplemental safeguards are in place
- Do impair independence
Non-audit services that do not impair independence

- Participating in committees, task forces, etc. in a advisory capacity
- Provide tools, methodologies, guidance to management
- Providing routine advice on accounting, internal control, etc.

Non-audit services that do impair independence

- Maintaining, preparing basic accounting records, including posting transactions
- Determining account balances or capitalization criteria
- Designing or installing accounting or IT system
- Providing payroll services that are material to audit and/or involve making management decisions

Other non-audit services that impair independence

- Providing appraisals, valuations
- Recommending individuals for hire
- Developing performance measurement system that is material to audit
- Developing internal control system or performing the organization’s self-assessment
- Developing policies, procedures, controls
- Conducting internal audit functions
### Services not impairing independence – with supplemental safeguards

- Preparing draft financial statements based on entity’s data
- Providing limited payroll services if not material to audit
- Reviewing work of specialists in appraisals, evaluations
- Preparing indirect cost proposals (but OMB has separate restrictions)

### Other non-audit services requiring supplemental safeguards

- Providing advisory services on information technology
- Sitting on employment panels
- Preparing routine tax filings
- Maintaining depreciation schedules, so long as management makes decisions on method and rate of depreciation, etc.

### Supplemental safeguards – all necessary

- Document consideration of impact of non-audit services
- Persons who provided services cannot work on the audit
- Do not reduce scope or extent of work below the level that would be appropriate if unrelated party had performed non-audit services
Additional supplemental safeguard

• The audit organization should have a clear understanding with auditee that auditee management is responsible for
  – Subject matter of non-audit services
  – Substantive outcomes of non-audit work
  – Making any management decisions regarding non-audit work
• Should document that understanding in writing with management

Professional Judgment
(Standard No. 2)

• Applies to all auditors in an organization
• Use professional judgment in planning and performing the audit
• Exercise professional skepticism
  – Have a questioning mind and critically assess the evidence
  – Do not assume that management is either honest or dishonest
  – Require persuasive evidence

Use professional judgment in all aspects of audit responsibilities

• Professional judgment and competence are interrelated
• Consider risk level of each assignment, including the risk that the auditor may come to an improper conclusion
Professional judgment does not imply unlimited responsibility

- Auditor and audit organization are not expected to be infallible
- Absolute assurance is not obtainable because of nature of evidence and fraud characteristics
- Auditors try to minimize, mitigate and explain possible limitations or weaknesses associated with a specific audit

Competence (Standard No. 3)

- Responsibility of the audit organization
- Staff in total has adequate professional proficiency
- Audit organizations should have a constant process to develop staff
- May employ specialists to assist in complex or subjective issues

Staff members must collectively possess

- Knowledge of GAGAS applicable to audit
- General knowledge of entity’s environment
- Skills to communicate clearly
- Appropriate needed skills, such as statistical sampling or IT
Additional qualifications for financial audits and attestation engagements

- Understand appropriate GAAP
- For financial audits, should know GAAS and SASs, and be able to apply them
- For attestation engagements should know SSAEs and be able to apply them

Continuing professional education

- Applies to all auditors performing under GAGAS
- At least 80 hours each 2-year period “that directly enhance” professional competency
- At least 20 hours each year
- 24 of 80 hours should be in government-related training
- Internal specialists should meet the CPE requirements

Other CPE issues

- Auditors have primary responsibility for meeting CPE requirements
- Audit organization should have quality controls to ensure and document that auditors meet CPE requirements
- GAO provides guidance on CPE
- Auditors who use specialists should assess and document their qualifications
- Outside specialists don’t have to meet the GAGAS CPE requirements
Quality Control and Assurance (Standard No. 4)

• Audit organizations must:
  – Establish a system of quality control
  – Have an external peer review at least once every three years

Quality Control and Assurance

• GAO clarified that an audit organization's
  – Non-compliance with peer review results in a modified GAGAS
  – Non-compliance with the requirements for a system of quality control does not impact the GAGAS statement, but is monitored through peer review
  – System of quality control also provides reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements

System of quality control policies and procedures should address

• Leadership for quality of audit work
• Independence, legal and ethical requirements
• Initiation, acceptance and continuation of audit work
• Human resources to ensure competent staff
• Documentation and reporting
• Monitoring of audit quality
External peer review

- Obtain a peer review at least once every three years
- The peer review should cover
  - Quality Control Policies and Procedures
  - Adequacy and results of monitoring procedures
  - Review of selected audits
  - Review of other documents and interviews with audit staff

Peer review report

- Describes scope of review
- Cites the standards to which agency is being held
- Gives an opinion on the system of quality control
- Explains modified or adverse opinions
- References any separate letter of comment

Other peer review requirements

- GAGAS has standards for review team
- External auditors should make the peer review report publicly available
  - Does not include letter of comment
- Internal auditors should provide a copy to those responsible for management
- Government auditors should notify oversight bodies
- Firms bidding on jobs should make report and comment letter available
Bottom line!

- Required to modify GAGAS compliance statement if:
  - Do not have an external peer review performed by independent reviewers at least once every 3 years
  - The review must meet all the requirements of GAGAS §3.55 through §3.60 which covers
    - Scope of the peer review
    - Risk assessment to select engagements
    - Communications of results of review
    - Criteria peer review team must meet

---

Yellow Book Essentials — Part 2

- Yellow Book Essentials — Part 1 covered:
  - The major changes to the Yellow Book
  - The general standards
- This session will cover the Yellow Book fieldwork and reporting requirements for:
  - Financial audits
  - Attestations

---

Chapter 4: Field Work Standards for Financial Audits

- GAGAS includes AICPA’s three field work standards
  - Plan and supervise
  - Understand entity and its environment, including internal controls in order to assess risk
  - Obtain sufficient, appropriate evidence
GAGAS has extra requirements

- Auditor communication
- Considering the results of previous audits and attestation engagements
- Detecting material misstatements resulting from violations of compliance requirements or abuse
- Developing elements of a finding
- Audit documentation

Auditor communication

- GAAS requires auditors to communicate in writing with clients
- Under GAGAS, auditors must also communicate with oversight bodies and third-parties requesting audit
- Explain nature of audit work and level of assurance
- Any potential restrictions on reports to prevent risk of misinterpretation

Consider results of prior audits and attestation engagements

- Ask management to identify previous audits, attestation engagements, or other relevant studies
- Ask management about corrective actions to address significant findings
- Use this information to assess risk and determine extent of audit work
Look for compliance violations

• The auditor should design the audit to provide reasonable assurance of detecting material misstatements caused by violations of grant or contract terms

Auditors should follow up on indications of abuse

• Abuse is behavior that a prudent person would consider deficient or improper, including misuse of authority
• Abuse may not involve non-compliance
• Determine whether it occurred and its effect on financial data
• Consider it quantitatively and qualitatively
• As abuse is subjective, auditors are not expected to provide reasonable assurance of detecting it

Develop the elements of a finding

• Condition – What is!
• Criteria – What should be!
• Cause – Why did it occur?
• Effect – So what?
• GAO considers recommendations as separate from findings
• Need for the various elements depends on the audit objectives
GAAS and GAGAS have the same audit documentation requirements

- Prepare audit documentation to enable an experienced auditor who has had no previous connection with the audit to understand
  - The nature, timing and extent of audit testing
  - The results and the evidence obtained
  - The conclusions reached
  - That the accounting records agree or reconcile with the audited financial statements

Under GAGAS, audit documentation should contain

- Evidence of supervisory review before the audit is issued
- Determination that some standards don’t apply or were not followed, with an explanation of the reason and the impact on the audit

Data can be retained in many forms

- Can be on paper, electronic or other media
- Should be retrievable and safeguarded
- GAGAS anticipates that auditors will cooperate with others to prevent duplication of effort
- Audit organizations should develop policies to deal with requests for audits and audit documentation
GAGAS provides additional considerations for financial audits
• May need to set lower materiality levels
• Design audit to have reasonable assurance of detecting material misstatements resulting from error or fraud
• If illegal act is likely:
  – Determine the potential financial effect
  – Consider any other implications
• Avoid interfering with investigations

SAS 99 – Consideration of Fraud in a Financial Statement Audit
• Issued – October 2002
• Supersedes SAS 82 and Amends SAS 1 (Codification of Auditing Standards and Procedures) and SAS 85 (Management Representations)
  – Effective for audits of financial statements for periods beginning on or after December 15, 2002

The Fraud Triangle

- Incentive/Pressure
- Opportunity
- Attitude/Rationalization
SAS 99 guidance for detecting fraud

- Maintain professional skepticism
- Consider the fraud triangle
- Staff must discuss fraud during the audit
- Obtain information to identify and assess the risks of fraud
- Make inquiries of management and others
- Document the steps taken

Auditors must exercise professional skepticism

- Auditors must always consider that fraud could be present
- Do not assume that management is honest or dishonest — require persuasive evidence
- Incorporate an element of unpredictability in the audit procedures

Incentives/pressures

- Financial instability or operating conditions may threaten organization
- Third parties may pressure with requirements or expectations
- Oversight body and/or management may have personal financial impacts
- Oversight body may establish unrealistic goals
Opportunities

- Poor internal controls
- Oversight body does not monitor management effectively
- Complex or unstable organizational structure

Reasons for ability to rationalize fraud

- Absence of a strong ethical structure
- Poor communication or enforcement of organization’s values
- Known history of problems
- Failure to correct known problems

Audit staff regularly communicates about fraud

- Hold a brainstorming session before starting the audit
- Communicate with each other throughout the engagement
- Signer of report ensures there was appropriate communication
- Document the brainstorming session, other activities related to fraud detection and the communications
Identify and assess the risks of fraud

• Consider the results of analytical procedures
• Consider the fraud risk factors
  – Where is the entity most susceptible to fraud?
  – What kind of fraud is most likely?
  – How would it be concealed?

Make inquiries of management and others

• About management’s awareness and understanding of fraud
• Also make inquiries of:
  – Audit committee
  – Internal auditors
  – Operating personnel
  – In-house counsel
  – Others who may have information

Your reputation can be impacted

• You can miss fraud and still meet standards
• But the media usually don’t understand
  – “How could you have missed …?”
• Therefore, be sure you document all the steps you take to look for fraud
Chapter 5: Reporting Standards for Financial Audits

- GAGAS includes GAAS reporting standards for financial audits
  - State whether financial statements are presented in accordance with GAAP
  - Identify any inconsistencies with prior period
  - Ensure that disclosures are reasonably adequate
  - Express an opinion or explain why not

GAGAS has extra requirements

- State that audit conformed with GAGAS
- Report on internal control and compliance
- Report deficiencies in internal control and “FINA”
- Communicate significant matters
- Report restatements
- Obtain response from auditee
- Confidential or sensitive information
- Report issuance and distribution

Compliance with GAGAS

- Report should state it was performed in accordance with GAGAS
- OK to cite GAAS
- OK to issue separate GAAS-only reports
Report work on internal controls and compliance

- Describe scope of testing of internal controls over financial reporting and compliance, or refer to other reports with that information
- Separate report should be considered integral part of the audit
- State whether auditor can express opinion on effectiveness of internal controls over financial reporting and compliance

Report deficiencies in internal controls and “FINA”

- Report
  - Significant deficiencies or material weaknesses in internal control
  - All instances of fraud and illegal acts unless “inconsequential”
  - Significant compliance violations and abuse

Definitions of internal control deficiencies

- **Significant deficiency** adversely affects ability to record, process, or report financial data reliably
  - More than remote chance of a misstatement that is “more than inconsequential”
- **Material weakness** is a significant deficiency or combinations of deficiencies so that there is more than remote chance of material misstatement
Reporting Internal Control Deficiencies

<table>
<thead>
<tr>
<th>Old Definitions</th>
<th>New Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Material Weakness ('03 GAGAS §5.14 and SAS 60, §15)</td>
<td>Material Weakness (AU 325.06 and '07 GAGAS §5.11b)</td>
</tr>
<tr>
<td>Reportable Condition ('03 GAGAS §5.13 and SAS 60, §02)</td>
<td>Significant Deficiency (AU 325.06 and '07 GAGAS §5.11a)</td>
</tr>
<tr>
<td>Management Letter comments ('03 GAGAS §5.16)</td>
<td>Other matters related to internal control ('07 GAGAS §5.14)</td>
</tr>
</tbody>
</table>

May have to report to outsiders

- Law or regulations may require it (e.g., to an Inspector General or Attorney General)
- Auditor should also report if:
  - Auditee is required to report, but does not
  - Auditee delays in making report
  - Management does not take timely and appropriate corrective action
- Auditors may have to report even if they have withdrawn or are fired from the audit

When reporting instances of “FINA”

- Place findings in perspective
  - Relate to universe or sample
  - Quantify amounts, if appropriate
- Try to develop elements of a finding
May communicate significant matters in the audit report

- Use professional judgment to determine what to emphasize, such as:
  - Uncertainties that could significantly impact financial condition
  - Government may not be able to meet commitments
  - Going concern issues
  - Uncertainties regarding estimates
- May be in separate section of report
- May include information not disclosed in F/S

Reporting on restatements

- Under GAAS auditors should notify management if previous financial statements were materially misstated
- GAGAS also requires auditors to:
  - Evaluate the timeliness and adequacy of management’s disclosures
  - Report on restated financials
  - Report directly to appropriate officials if management does not

Obtain and report views of responsible officials

- Effective technique to ensure audit is fair, complete and objective
- Request comments in writing, but oral comments are acceptable
- Include comments in the report
- Auditors should report any disagreement with management comments – in a fair and objective manner
- Modify report if appropriate
**Confidential or sensitive information**

- If certain information is prohibited from general disclosure or is confidential or sensitive:
  - State nature of information omitted
  - Why it was omitted
- May be prohibited from disclosure by law or regulation
- May need to consult with legal counsel
- Judgment whether to omit data should consider broad public interest

**Report distribution**

- Governmental auditors
  - Auditee
  - Organizations arranging for audits
  - Other oversight officials
  - Most government agencies require reports to be public
- Internal auditors may follow ISPPIA
- Non-governmental auditors follow agreements

**Federal Report on the National Single Audit Sampling Project**

- Report issued by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency
- Summarizes results of a 2+ year effort to:
  - Assess the quality of single audits & establish a statistically based measure of audit quality
  - Recommend changes in single audit requirements, standards and procedures to improve the quality of single audits
Background

- The scope was limited to assessing audit work and reporting related to Federal awards (i.e., it did not assess audit work and reporting related to general-purpose financial statements).
- A statistical sample of 208 audits were randomly selected and reviewed from the 38,523 audits submitted and accepted for the period April 2003 through March 2004.
- The sample was split into two strata:
  - **Stratum One** included audits of entities that expended $50 million or more of Federal awards.
  - **Stratum Two** included audits of entities that expended at least $500,000 of Federal awards, but less than $50 million.

Report’s Breakdown of the Sample

<table>
<thead>
<tr>
<th>Description</th>
<th>Stratum One</th>
<th>Stratum Two</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of audits submitted and accepted for the period 4/03 – 3/04</td>
<td>852</td>
<td>37,671</td>
<td>38,523</td>
</tr>
<tr>
<td>Number of audits selected for the National Single Audit Project</td>
<td>96</td>
<td>112</td>
<td>208</td>
</tr>
</tbody>
</table>

Stratum One Results

<table>
<thead>
<tr>
<th>Description</th>
<th>Number of Audits</th>
<th>Percent of Audits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audits were acceptable and thus could be relied upon</td>
<td>61</td>
<td>63.5%</td>
</tr>
<tr>
<td>Audits had significant deficiencies and thus were of limited reliability</td>
<td>12</td>
<td>12.5%</td>
</tr>
<tr>
<td>Audits were unacceptable and could not be relied upon</td>
<td>23</td>
<td>24.0%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>96</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
### Stratum Two Results

<table>
<thead>
<tr>
<th>Description</th>
<th>Number of Audits</th>
<th>Percent of Audits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audits were acceptable and thus could be relied upon</td>
<td>54</td>
<td>48%</td>
</tr>
<tr>
<td>Audits had significant deficiencies and thus were of limited reliability</td>
<td>18</td>
<td>16%</td>
</tr>
<tr>
<td>Audits were unacceptable and could not be relied upon</td>
<td>40</td>
<td>36%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>112</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

### National Single Audit Sampling Project, June 2007

<table>
<thead>
<tr>
<th>Description</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable</td>
<td>39</td>
<td>19</td>
</tr>
<tr>
<td>Acceptable with Deficiencies</td>
<td>76</td>
<td>37</td>
</tr>
<tr>
<td>Significant Deficiencies</td>
<td>30</td>
<td>14</td>
</tr>
<tr>
<td>Material Reporting Errors</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Substandard</td>
<td>54</td>
<td>26</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>208</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

### Types of Deficiencies Noted

- Misreporting of audit coverage of major Federal programs
- Unreported audit findings
- Compliance testing not documented as performed or not applicable
- Deficiencies in understanding and testing of internal control over compliance
- Deficiencies in risk assessments as part of major program determination
Deficiencies Noted - Continued

- Missing audit finding information
- Deficiencies in presentation and auditing of Schedules of Expenditures of Federal Awards (SEFA)
- Management representations related to Federal awards missing or misdated
- Consideration of audit materiality at the major Federal program level not documented
- Other miscellaneous kinds of deficiencies

Report Recommendations

- The report recommends a three-pronged approach to improve audit quality:
  - Revise and improve single audit criteria, standards and guidance to address deficiencies identified in the Project;
  - Establish minimum requirements for completing comprehensive training on performing single audit as a prerequisite for conducting single audits and require single audit update training for continued performance of single audits; and
  - Review and enhance processes to address unacceptable audits and not meeting established training and continuing professional education requirements.

AICPA Ethics Investigations Resulting from Government Agency Referrals

<table>
<thead>
<tr>
<th>Violations</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Standards</td>
<td>75</td>
<td>6%</td>
</tr>
<tr>
<td>Auditing Standards</td>
<td>602</td>
<td>52%</td>
</tr>
<tr>
<td>Act Discreditable</td>
<td>487</td>
<td>42%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1,164</td>
<td>100%</td>
</tr>
</tbody>
</table>
Resources Auditees and Auditors should have and use

- President’s Council on Integrity & Efficiency - UNIFORM GUIDE FOR INITIAL REVIEW OF A-133 AUDIT REPORTS
- President’s Council on Integrity & Efficiency – UNIFORM QUALITY CONTROL REIVERW GUIDE FOR A-133 AUDITS

Chapter 6: Attestation engagements

- Attestation engagements include
  - Examination: sufficient testing to express an opinion whether subject matter meets criteria in all material respects
  - Review: sufficient testing to express conclusion whether information came to auditor’s attention that subject matter does not meet criteria in all material respects
  - Agreed-upon procedures: report on findings based on specific procedures performed on subject matter

AICPA’s Statements on Standards for Attestation Engagements

- SSAE No. 10 – Attestation Standards: Revision and Re-codification, January 2001
- SSAE No. 11 – Attest Documentation, January 2002
- SSAE No. 12 – Amendment to SSAE No. 10: Revision and Re-codification, September 2002
- SSAE No. 13 – Defining Professional Requirements in SSAEs, December 2005
- SSAE No. 14 – SSAE Hierarchy, November 2006
- SSAE No. 15 – Examination of an Entity’s Internal Control Over Financial Reporting That is Integrated With an Audit of Its Financial Statements, October 2008
GAGAS incorporates AICPA general standard

“The practitioner [auditor] must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users.”

GAGAS incorporates AICPA field work standards

• Must adequately plan the work and must properly supervise any assistants
• Must obtain sufficient evidence to provide a reasonable basis for conclusion that is expressed in the report

GAGAS has additional field work standards

• Auditor communication
• Considering the results of previous audits and attestation engagements
• Internal control
• Detecting “FINA”
• Developing elements of a finding
• Attest documentation (essentially the same as the audit documentation standards)
Auditor communication

- GAAS requires communication with clients
- GAGAS also requires auditors communicate with
  - Third-parties requesting engagement
  - Oversight bodies
- Explain reasons for early termination

Information to be communicated

- Nature, timing, and extent of planned testing and reporting
- Level of assurance the auditor will provide
- Any potential restrictions on the auditor’s reports

Consider results of prior audits and attestation engagements

- Ask management to identify previous audits, attestation engagements, or other relevant studies
- Ask management to identify corrective actions to address significant findings
- Evaluate whether entity has taken appropriate corrective actions
- Use this information in assessing risk and determining attestation work
Internal control
(in examination-level engagements)

- Obtain sufficient understanding of internal control that is germane to subject under review
- Deficiency in design
  - Control is missing
  - Not properly designed
- Deficiency in operation
  - Does not operate as designed
  - Person performing control does not have necessary authority or qualifications

Detecting “FINA”

- For examination-level
  - Reasonable assurance of detecting material “FIN”
  - Document assessment of risk
- For review level and agreed-upon procedures, follow up on indications of "FIN" that could be material
- For all levels, follow up on indications of abuse

Develop the elements of a finding

- Condition – What is!
- Criteria – What should be!
- Cause – This occurred because?
- Effect – So what?
- GAO considers recommendations as separate from findings
Attest documentation

• “Experienced auditor” standard again
• Document
  – Objectives, scope and methodology
  – Work performed that supports judgments and conclusions
  – Evidence of supervisory review before issuance
  – Alternatives if not evaluating IT systems
• Same other requirements as for audits

Additional considerations for attestations

• May need to use lower levels of materiality for government programs
• Avoid interfering with investigations
  – May need to work with investigators
  – May need to withdraw from engagement
  – May need to defer from work

GAAS reporting standards for attestation engagements

• GAGAS adopts four AICPA mandatory requirements
  – Identify subject matter and nature of engagement
  – State auditor’s conclusion
  – State any auditor’s significant reservations about engagement
  – Report sets forth any report restrictions
GAGAS has extra requirements

- Reporting compliance with GAGAS
- Reporting deficiencies in internal control and "FINA"
- Reporting views of responsible officials
- Reporting confidential or sensitive information
- Report distribution

Reporting compliance with GAGAS

- State attestation engagement was conducted in accordance with GAGAS, including underlying SSAEs
- May cite the SSAEs as well
- May also issue separate SSAE report

Reporting deficiencies in internal control and "FINA"

- Report all significant internal control deficiencies, including material weaknesses
- All fraud and illegal acts unless inconsequential
- non-compliance or abuse that is material to subject matter
- Should place findings in perspective
- May have to report "FINA" directly to external parties
Reporting views of responsible officials
• If the report discloses deficiencies in internal control or "FINA", obtain views of responsible officials
• Report those views
• Report planned corrective actions
• Auditors may need to
  – Modify audit report
  – Explain why they disagree with response

Reporting confidential or sensitive information
• If pertinent information is prohibited from general disclosure, state:
  – Nature of the information omitted
  – Why it was omitted
• Consider broad public interest in deciding whether to report
• Use the same reporting rules as for audits

Report issuance and distribution
• Same reporting rules as audits
• AICPA limitations on attestation report issuance does not necessarily limit report distribution in government environment
Yellow Book Essentials – Part 3

• Yellow Book Essentials — Part 1 and 2 covered:
  – The major changes to the Yellow Book Chapters 1 through 6
• This session will cover the Yellow Book fieldwork and reporting requirements for Performance Audits

Chapter 7: Field Work Standards for Performance Audits

• Planning
• Supervision
• Evidence
• Audit documentation

Need to consider reasonable assurance, significance and audit risk throughout the audit

Need reasonable assurance that:

• Evidence is sufficient and appropriate to support audit findings and conclusions
• Need for evidence varies according to objectives, findings and conclusions
Significance

- Relative importance of a matter in the entire context
- Includes quantitative and qualitative factors
- Impacts type and extent of audit work
- Affects development of findings and conclusions

Audit risk

- Possibility that findings, conclusions, recommendations or assurance is improper or incomplete
- Includes quantitative and qualitative factors
- Can be reduced by increasing audit scope, adding experts or other resources, changing methodology, etc.

Planning (Standard No. 1)

“Auditors must adequately plan and document the planning of the work necessary to address the audit objectives”

“Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to provide reasonable assurance that the evidence is sufficient and appropriate to support the auditors’ findings and conclusions.”
Auditors must gain an understanding of:

- Nature of programs and needs of potential report users
- Relevant internal controls
- Information systems controls in order to assess risk
- Legal, regulatory, contact and grant provisions, potential fraud or abuse
- Results of relevant previous reviews

Considering nature of program

- Visibility, sensitivity and relevant risks
- Age of program, any recent changes
- Size of program
- Level and extent of other reviews
- Program’s strategic plan and objectives
- External factors that could impact it

Auditors need to consider:

- Laws, regulations and contractual requirements
- Purpose and goals
- Internal controls
- Efforts
- Program operations
- Outputs
- Outcomes
Internal control
- Should understand relevant internal controls
- Assess whether it has been properly designed and implemented
- Plan to obtain evidence to support assessment of effectiveness of controls
- Consider whether it is necessary to evaluate IT controls
- Internal auditing is an important part of internal control

Definition of Internal Controls

“The plan of organization and methods and procedures adopted by management to ensure that resource use is consistent with laws, regulations, and policies; that resources are safeguarded against waste, loss, and misuse; and that reliable data are obtained, maintained, and fairly disclosed in reports.”
Single Audit Requirement

“...each audit shall determine and report in writing whether the government, department, agency, or establishment undergoing the audit has internal control systems to provide reasonable assurance that it is managing federal financial assistance programs in compliance with applicable laws and regulations.”

Information systems controls are important when

- IT is used extensively throughout the program under audit
- Fundamental business processes related to audit objectives rely on them
- If they are significant to the audit objectives, auditors should assess their effectiveness
Types of IT System Controls

- General controls
  - Create environment for proper operation of application controls
  - Include security management, segregation of duties, contingency planning
- Application controls
  - Help ensure validity, completeness, accuracy and confidentiality of transactions
  - Include control over input, processing, output, master data, application and management system

Legal and other requirements

- Determine laws, regulations, and grant/contract provisions that are significant to audit objectives
- Design and perform procedures to provide reasonable assurance of detecting material "FIN"
- Because abuse is subjective, auditors are not required to provide reasonable assurance of detection

Consider the risk of fraud and abuse

- For fraud, GAGAS has essentially the same audit requirements as SAS 99
- Follow up on indications of abuse
  - Remember, abuse can be qualitative and quantitative
- Avoid interfering with investigations or legal proceedings
Considering previous reviews

• Ask management to identify previous audits or other reviews that relate to audit objectives
• Ask whether recommendations have been implemented
• Use this info to assess risk and determine audit steps, including corrective actions

Planning should include

• Potential criteria
• Sources of evidence and amount and type of evidence needed
• Whether to use work of other auditors/experts
• Assigning sufficient staff
• Communicating with auditee and others
• Preparing an audit plan

GAGAS provides examples of audit criteria

• Purpose or goals of program
• Policies and procedures
• Technically developed standards or norms
• Expert opinions
• Prior period performance
• Defined business practices
• Grant/contract terms
• Best practices of leading organizations
Considering the work of others

• Should determine whether other audits have useful data
• If relying on work of others, must conduct procedures to provide adequate basis for that reliance
• Similar issues when relying on work of non-auditors

Assigning staff and other resources

• Assign staff with sufficient collective knowledge, skills and experience
• Adequate number of staff and supervisors
• Provide on-the-job training for staff
• If engaging specialists, auditor should document
  – Objectives and scope of specialist’s work
  – Intended use of work
  – Specialist’s procedures and findings
  – Assumptions and methods used

Communicating with management and others

• Communicate with head of auditee, audit committee or Board of Directors and CFO
• Also with third-parties requesting audit, such as contracting officers
• Explain audit objectives, time frames, planned reporting, including any restrictions
• Written communication is preferred
• Document early termination
Preparing the audit plan

- Prepare a written plan for each audit
- Opportunity for auditors to consider whether
  - Proposed objective are likely to be useful
  - Plan addresses relevant risks
  - Available evidence will be sufficient
  - Scope and methodology will satisfy objectives
  - Sufficient staff and other resources are available

Supervision
(Standard No. 2)

- Must properly supervise audit staff
- Includes providing guidance, staying informed about significant problems, reviewing work and providing O-J-T
- Required supervision can vary depending on
  - Size of audit organization
  - Significance of the audit
  - Experience of staff

Obtaining Sufficient, Appropriate Evidence (Standard No. 3)

- Obtain sufficient, appropriate evidence to provide reasonable basis for the auditor’s findings and conclusions
  - Appropriateness encompasses relevance, validity and reliability
  - Sufficiency considers whether enough evidence to convince
- Use professional judgment to determine sufficiency and appropriateness
GAGAS provides guidance on evidence

- Good internal controls provide better evidence than weak controls
- Direct evidence is better than indirect
- Originals are more reliable than copies
- Ability to speak freely affects testimonial evidence
- The best testimony is from unbiased person who has direct knowledge
- Evidence from unbiased third party is more reliable than from management

Sources of evidence influences reliability

- Statistical samples vs. non-statistical samples
- Auditors must evaluate reliability of self-reported information
- When auditors must evaluate the reliability of computer-generated data, if they plan to use it

GAGAS provides guidance on sufficiency of evidence

- Higher audit risk requires more quantity and quality of evidence
- Stronger evidence reduces the amount of evidence required
- A large volume of evidence does not overcome problems of relevance, validity and reliability
Overall assessment of evidence

• Sufficiency and appropriateness are interrelated
• Sufficiency and appropriateness are relative concepts
• Should consider the expected significance of the evidence

Audit findings

• Try to develop the components of a finding:
  – Condition – What is!
  – Criteria – What should be!
  – Cause – Why did this occur?
  – Effect – So what?
  – No reference to recommendation (GAO refers to findings and recommendations)

Audit documentation

• Provides principal support for auditors’ report
• Aid auditors in conducting and supervising the audit
• Allow for a review of audit quality
• Circumstances determine the form, content and extent of documentation
• Documentation should be prepared before issuance of the audit report
Basic requirement for audit documentation

• Prepare audit documentation to enable an experienced auditor who has had no previous connection with the audit to understand
  – The nature, timing and extent of audit testing
  – The results of the audit tests
  – Source of evidence obtained
  – How the evidence relates to the conclusions
  – All significant conclusions reached

Auditors should document

• Objectives, scope and methodology
• Work performed to support significant judgments and conclusions, including descriptions of transactions and records examined
• Evidence of supervisory review before the audit is issued
• Any reasons for not following a GAGAS requirement

Data can be retained in many forms

• Can be on paper, electronic or other media
• Must be retrievable and safeguarded
• GAGAS anticipates that auditors will cooperate with others to prevent duplication of effort
• Audit organizations should develop policies to deal with requests for audits and audit documentation
Chapter 8: Reporting Standards for Performance Audits

- Must have reports for all audits
- Reports should be in retrievable form
- Purpose of reports
  - Communicate audit results to all users
  - Reduce misunderstanding
  - Make results available to public
  - Facilitate follow-up

Objectives, scope and methodology

- Objectives should be expressed in clear, specific, neutral terms
- Clearly describe the scope of work
  - Any limitations
  - Any standards not followed
- Explain work performed to achieve objectives
  - Identify any significant assumptions
  - Explain sampling that is significant to results

Findings

- Present sufficient, appropriate evidence to support findings and conclusions
- Clearly developed findings will help convince readers
- Make recommendations if appropriate
- Describe any limitations
- Place findings in perspective
- Provide information for context
Report deficiencies in internal control and “FINA”

- Scope of work on internal control
- Significant deficiencies in internal control
- All instances of fraud and illegal acts
- Significant non-compliance
- Significant abuse

GAGAS may require reporting of “FINA” to outside entities

- Law or regulations may require it (e.g., to an Inspector General or Attorney General)
- Auditor must also report if:
  - Auditee is required to report, but does not
  - Auditee delays in making report
  - Management does not take timely and appropriate corrective action
- Auditors may have to report even if they have withdrawn or are fired from the audit

Report conclusions and recommendations

- Conclusions are logical inferences about the program, not just a summary of findings
- Recommend corrective actions when appropriate
  - Recommendation should address the root cause of the problem
**Other requirements for reporting**

- Work was performed in accordance with GAGAS
  - Unmodified compliance
  - Modified compliance
- Requesting and reporting views of management
- Reporting confidential or sensitive information

  Essentially the same as financial audits

---

**Report distribution**

- Governmental auditors
  - Auditee
  - Organizations arranging for audits
  - Other oversight officials
- Government internal auditors can follow IIA standards
- Non-government auditors follow agreements

---

**Supplemental Guidance**

- Contained in Appendix 1
- Advisory, not mandatory
- First section applies to all audits and engagements
- Subsequent sections apply to specific chapters
Overall guidance

- Examples:
  - Internal control deficiencies
  - Abuse
  - Indicators of fraud risk
- Determining significance of laws, regulations, and grant/contract provisions

Some examples of internal control deficiencies

- Insufficient control consciousness
- Ineffective oversight
- Systems that did not detect material misstatements
- Ineffective internal audit or risk assessment
- Fraud by senior management
- Intentional overrides of controls

Some examples of abuse

- Creating unneeded overtime
- Having staff perform personal errands
- Misusing position for personal gain
- Making extravagant/expensive travel choices
- Procurements contrary to policy or that are extravagant/expensive
Some indicators of fraud risk

- Threats to entity’s financial stability, budget
- Entity’s operations provide opportunities for fraud
- Inadequate management monitoring for compliance
- Lack of communication/support for ethical standards
- Key documentation lacking or nonexistent
- History of impropriety

Determining whether rules are significant to audit objectives

- Express each audit objective in the form of a question
- Identify laws/regulations/provisions that relate to specific aspects of a program
- Determine whether violations of laws/regulations, etc. could significantly impact audit objectives
- May consult with legal counsel, investigators, other auditors, law enforcement authorities

Guidance for Chapter 1

- GAGAS may be required by rules
- Many auditors voluntarily follow GAGAS
- Auditors may need to evaluate who is charged with governance
Entity managers have many responsibilities
- Using resources legally, economically, ethically and effectively
- Complying with laws and regulations
- Designing and implementing control systems
- Reporting to oversight bodies and to the public
- Addressing findings, correcting problems
- Following sound procurement practices

Guidance for Chapter 3: Non-audit services that don’t impair independence
- Providing unaudited data
- Developing standards, methodologies, etc. for use throughout government
- Collaborating with professional associations to improve auditing
- Developing FAQ’s to help others understand technical issues
- Providing training and presentations
- Identifying good business practices for users

Guidance for Chapter 7
- Types of evidence
  - Physical
  - Documentary
  - Testimonial
  - No reference to analytical
- Consider appropriateness of evidence in relation to the audit objectives
  (Verification of data, considering performance of program, benchmarking, etc.)
Guidance for Chapter 8: Report quality elements

• **Accurate** – fact based
• **Objective** – balanced in content and tone
• **Complete** – supported by evidence
• **Convincing** – flows logically from facts
• **Clear** – easy to read and understand
• **Concise** – keep it short and simple (KISS)
• **Timely** – in time for governance to resolve
Overall Proposed Changes

- Chapters 1 and 2 have been realigned
- All financial audit standards are now in Chapter 4
- Terminology has been updated for consistency with other standards
- Consistency of the use of footnotes has been improved
- The guidance provided in *Answers to Independence Standard Questions* will be suspended by this revision.

Revised Chapter 1

- Government Auditing: Foundation and Ethical Principles
  - Two definitions will be incorporated:
    - "Auditor" describes individuals performing work under GAGAS regardless of job title
    - "Audit Organization" refers to organizations that perform audits and attestation engagements using GAGAS
  - Structural location of the audit function relative to the audited entity is addressed
    - External audit organizations report to third parties externally
    - Internal audit organizations are accountable to top management and those charged with governance and do not generally issue reports to third parties externally
    - Government audit organizations that report to both third parties and top management are considered external audit organizations

Revised Chapter 2

- Standards for the Use and Application of GAGAS
  - The role of professional judgment in determining the appropriate type of GAGAS compliance statement is emphasized
  - The requirement that auditors use GAGAS as the prevailing standard if inconsistencies exist between GAGAS and other standards cited will be removed
Revised Chapter 3

• General Standards
  – A conceptual framework for independence is added to provide a means for auditors to assess auditor independence
  • The proposed conceptual framework is designed to achieve harmonization with AICPA and International Standards, with additional considerations for government audits
  – Requirements for CPE are clarified

Revised Chapter 4

• Standards for Financial Audits
  – Certain AICPA standards have been emphasized
  – Deleted certain paragraphs to eliminate redundancy with AICPA standards
  – Discussion of reasonable assurance has been revised
  – Deleted the requirement to document the results of the work to the date of termination and why the audit was terminated.
  – Deleted the requirement to audit organizations develop policies to address request by outside parties to obtain access to audit documentation

Revised Chapter 5

• Standards for Attestation Engagements
  – Early communication of deficiencies has been added
  – Several sections have been removed
  – Review-level and agreed-upon procedures engagements are separately discussed
  • Additional AICPA considerations have been added
    – Establishing an understanding regarding services to be performed
    – Reporting in accordance with AICCPA standards
Revised Chapter 6

- Field Work Standards for Performance Audits
  - Discussion of validity as an aspect of the quality of evidence has been revised
  - Discussion of the sufficiency and appropriateness of computer-process information has been revised
  - The requirement that audit organizations develop policies to address requests for outside parties has been removed

Revised Chapter 7

- Reporting Standards for Performance Audits
  - Fraud reporting requirement is now limited to occurrences that are significant within the context of the audit
  - With a requirement to communicate in writing other instances of fraud to those charged with governance
Purpose of IIA Standards

1. Delineate basic principles that represent the practice of internal auditing as it should be.
   a. The use of the word “should” in the Standards represents a mandatory obligation.
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.

Definition

- The Institute of Internal Auditors’ International Professional Practice Framework (IPPF)
  - Definition of Internal Auditing
  - Code of Ethics
  - International Standards
    • Position Papers
    • Practice Advisories
    • Practice Guides

Definitions - Continued

- Internal Audit Activity = A department, division, team of consultants or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization’s operations.
  - The internal audit activity 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.
Definitions - Continued

• **Assurance Services** = An objective examination of evidence for the purpose of providing an independent assessment on risk management, control or governance processes for the organization.
  – Examples may include financial, performance, compliance, system security and due diligence engagements.

• **Consulting Services** = Advisory and related client service activities, the nature and scope of which are agreed with the client and which are intended to add value and improve an organization's governance, risk management and control processes without the internal auditor assuming management responsibility.
  – Examples include counsel, advice, facilitation and training.

IIA Standards

• **Attribute Standards** address the characteristics of organizations and parties performing internal audit activities.

• **Performance Standards** describe the nature of internal audit activities and provide quality criteria against which the performance of these services can be evaluated.

• **Implementation Standards** apply to specific types of engagements.
  – Implementation Standards have been established for assurance (A) and consulting (C) activities.

IIA Attribute Standards

• Standard 1000 – Purpose, Authority and Responsibility
• Standard 1100 – Independence and Objectivity
• Standard 1200 – Proficiency and Due Professional Care
• Standard 1300 – Quality Assurance and Improvement Program
IIA Attribute Standard 1000 – Purpose, Authority and Responsibility

• Internal Audit activities should be formally defined in a charter and approved by those responsible for governance.
  – Implementation Standard 1000.A1 – Assurance services provided to the organizations and to outside parties should be defined in the audit charter.
  – Implementation Standard 1000.C1 – Consulting services provided should be defined in the audit charter.

Standard 1000 – Endorsed and Strongly Recommended Guidance

• Practice Advisory 1000-1: Internal Audit Charter
• Practice Advisory 1000-C1-1: Principles Guiding the Performance of Consulting Activities of Internal Auditors
• Practice Advisory 1000-C1-2: Additional Considerations for Formal Consulting Engagements

Internal Audit Charter

• A formal written document that defines the internal audit activity’s purpose, authority and responsibility. The Charter should:
  1. Establish the activity’s position within the organization,
  2. Authorize access to records, personnel and physical properties relevant to the performance of engagements, and
  3. Define the scope of internal audit activities.
IIA Attribute Standard 1100 – Independence and Objectivity

- The internal audit activity should be independent, and internal auditors should be objective in performing their work (Practice Advisory 1100-1).
  - Attribute Standard 1110: Organizational Independence
  - Attribute Standard 1120: Individual Objectivity
  - Attribute Standard 1130: Impairments to Independence or Objectivity

Attribute Standard 1110: Organizational Independence

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

Standard 1110 – Endorsed and Strongly Recommended Guidance

- Practice Advisory 1110-A1-1: Disclosing Reasons for Information Requests
- Practice Advisory 1110-1: Organizational Independence
- Practice Advisory 1110-2: Chief Audit Executive (CAE) Reporting Lines
Definition of Impairments

- Impairments to individual objectivity and organizational independence may include personal conflicts of interest, scope limitations, restrictions on access to records, personnel and properties, and resource limitations (funding).

Attribute Standard 1120: Individual Objectivity

- Internal auditors should have an impartial, unbiased attitude and avoid conflicts of interest (Practice Advisory 1120-1).
  - Impartial and Unbiased Attitude
  - Conflict of Interest is any relationship that is or appears to be not in the best interest of the organization.
  - Conflict of interest would prejudice an individual’s ability to perform his or her duties and responsibilities objectively.

Attribute Standard 1130: Impairments to Independence or Objectivity

- If impaired in fact or appearance, the details should be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.
  - Implementation Standard 1130.A1 – Internal auditors should refrain from auditing specific operations for which they were previously responsible.
    - Objectivity is presumed to be impaired if auditor had responsibility within the previous year.
  - Implementation Standard 1130.A2 – Audits for functions over which the CAE has responsibility should be overseen by a party outside the internal audit activity.
  - Implementation Standard 1130.C1 – Auditors may provide consulting services to operations for which they had previous responsibilities.
  - Implementation Standard 1130.C2 – If auditors have potential impairments relating to proposed consulting services, disclosure should be made to the client prior to the engagement.
Standard 1130 – Endorsed and Strongly Recommended Guidance

• Practice Advisory 1130-1: Impairments to Independence or Objectivity
• Practice Advisory 1130-A1-1: Assessing Operations for Which Internal Auditors were Previously Responsible
• Practice Advisory 1130-A1-2: Internal Audit Responsibility for Other (Non-Audit) Functions

IIA Attribute Standard 1200 – Proficiency and Due Professional Care

• Engagements should be performed with proficiency and due professional care (Practice Advisory 1200-1).
  – Attribute Standard 1210: Proficiency
  – Attribute Standard 1220: Due Professional Care
  – Attribute Standard 1230: Continuing Professional Development

Attribute Standard 1210: Proficiency

• Internal auditors should possess the knowledge, skills and other competencies needed to perform their individual responsibilities. The audit activity collectively should possess or obtain the knowledge, skills and other competencies needed to perform its responsibilities.
  – Implementation Standard 1210.A1 – The CAE should obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills or other competencies needed for all or part of the assurance engagement.
  – Implementation Standard 1210.A2 – Auditors should have sufficient knowledge to identify the indicators of fraud, but is not expect to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
  – Implementation Standard 1210.A3 – 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 auditors are expected to have the expertise of an auditor whose primary responsibility is information technology auditing.
  – Implementation Standard 1210.C.1 – The CAE should decline consulting engagement or obtain competent advice and assistance if the audit staff lacks the knowledge, skills or other competencies needed to perform all or part of an engagement.
Standard 1210 – Endorsed and Strongly Recommended Guidance

• Practice Advisory 1210-1: Proficiency
• Practice Advisory 1210-A1-1: Obtaining Services to Support or Complement the Internal Audit Activity
• Practice Advisory 1210-A2-1: Auditor’s Responsibilities Relating to Fraud Risk Assessment, Prevention and Detection
• Practice Advisory 1210-A2-2: Auditor’s Responsibilities Relating to Fraud Investigation, Reporting, Resolution and Communication

Indicators of Fraud

• Any illegal acts characterized by deceit, concealment or violation of trust.
• These acts are not dependent upon the application of threat of violence or of physical force.
• Frauds are perpetrated by parties and organizations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage.

The Fraud Triangle

- Incentive/Pressure
- Opportunity
- Attitude/Rationalization
Attribute Standard 1220: 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 (Practice Advisory 1220-1).

  – Implementation Standard 1220.A1 – Auditors should exercise due professional care by considering the:
    • Extent of work need 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 non-compliance.
    • Cost of assurance in relation to potential benefits.

Attribute Standard 1220: Due Professional Care - Continued

• Implementation Standard 1220.A2 – In exercising due professional care the auditor should consider the use of computer-assisted audit tools and other data analysis techniques.

• Implementation Standard 1220.A3 – Auditors should be alert to significant risks that might affect objectives, operations or resources.
  – However, assurance procedures alone, even when performed with due care, do not guarantee that all significant risks will be identified.

Technology-Based Audit Techniques

• IIA’s Global Technology Audit Guides:
  – GTAG-1: IT Controls, March 2005
  – GTAG-2: Change and Patch Management Controls, June 2005
  – GTAG-3: Continuous Auditing, October 2005
  – GTAG-4: Management of IT Auditing, March 2006
  – GTAG-6: Managing and Auditing IT Vulnerabilities, October 2006
  – GTAG-7: Information Technology Outsourcing March 2007
  – GTAG-8: Auditing Application Controls, July 2007
Technology-Based Audit Techniques - Continued

- IIA’s Global Technology Audit Guides:
  - GTAG 11: Developing the IT Audit Plan, July 2008
  - GTAG 12: Auditing IT Projects, March 2009
  - GTAG 14: Auditing User-developed Applications, June 2010
  - GTAG 15: Information Security Governance, June 2010

What is GTAG?

GTAG - Global Technology Audit Guide

- To provide easy-to-understand information technology audit guides to Chief Audit Executives, Audit Committees and Executive Management
- To provide a mechanism to quickly address new IT Issues
- To produce technical audit guides on a global scale

Who is GTAG target audience?

Primary target - Chief Audit Executive (CAE)

- Many CAEs face the challenge to understand technology, which is necessary to plan and conduct internal audit.
- CAEs are not well-served by many existing guides, such as Cubit, which tend to target technical IT auditor and IT management
- Given the broad responsibility of CAEs, GTAG series provide them a high level overview on risk management and control related to IT.

GTAG is practically immeasurable to busy executives who need to quickly understand technology issues and evaluate the impact on their organization.
Who are involved in GTAG development?

- Advanced Technology Committee – select topics based on the member’s needs; oversee development of guides and develop contents
- Partners with other professional organization – broaden audience for guides and contribute to content
  – AICPA, NACD, CIS, FEI, ISSA, Sans Institute, Carnegie Mellon SEI
- IIA global affiliates participate the reviewing process

GTAG-1
Information Technology Controls

It covers:
- Understanding of IT controls
- Importance of IT controls
- Organizational roles and responsibilities for ensuring IT controls
- Analyzing risks
- Monitoring and techniques
- IT control assessment

GTAG-2
Change and Patch Management Controls: Critical for Organizational Success

It covers:
- Why IT change and patch management controls are foundational to a healthy IT environment
- How IT change and patch management controls help manage IT risks and costs
- What works and doesn’t work in practice
- Describes sources of change and the likely impact on business objectives
GTAG-3
Continuous Auditing:
Implications for Assurance, Monitoring, and Risk Assessment

It covers:
• Role of continuous auditing in today's internal audit environment
• Relationship of continuous auditing, continuous monitoring, and continuous assurance
• The application and implementation of continuous auditing
• Benefits of a continuous, integrated approach

GTAG-4
Management of IT Auditing

It covers:
• Defining IT
• IT-related Risks
• Defining IT Audit Universe
• Executing IT Auditing
• Managing IT Auditing
• Emerging Issues

GTAG-5
Managing and Auditing Privacy Risks

It covers:
• What is Privacy
• Privacy Principles and Frameworks
• Privacy Impacts and Risk Model
• Privacy Controls
• Good and Bad Performers
• Internal Auditing's Role
• Auditing Privacy
• CAE's Top 10 Privacy Questions
GTAG-6
Managing and Auditing IT Vulnerabilities

It covers:
• Define the vulnerability management lifecycle
• The scope of a vulnerability management audit
• Organizational maturity
• Metrics to measure vulnerability management practices
• Top 10 vulnerability management questions

GTAG-7
Information Technology Outsourcing

It covers:
• How to choose the right IT outsourcing vendor?
• What are the best ways to manage outsourcing contract agreements?
• What are the main outsourcing risks and how to mitigate them?
• What are the key outsourcing control considerations from the standing points of both client operations and service provider operations?
• Which is the most effective framework for establishing outsourcing controls?

GTAG-8
Auditing Application Controls

It covers:
• What is application control?
• What is the relationship between application control and general controls?
• Why rely on application controls?
• How to scope a risk-based application control review?
• What are the steps to conduct an application controls review?
• A list of key application controls
• A sample audit program
GTAG 9 - Identity and Access Management

- Matters to consider:
  - Who has access to what information?
  - Is the access appropriate for the job being performed?
  - Is the access and activity monitored, logged and reported appropriately?

GTAG 10 – Business Continuity Management

- Matters covered:
  - How continuity planning can minimize operation disruptions
  - The components of an effective continuity plan
  - How impact analysis can help identify which operations need to be recovered first following a disruption
  - Ways to maximize audit's values in continuity planning

GTAG 11 – Developing the IT Audit Plan

- Provides guidance to:
  - Explore the relationship between IT and operation
  - Define IT audit universe
  - Develop IT audit plan form the IT audit universe
  - Provide examples of developing an IT audit plan
GTAG 12 – Auditing IT Projects

• What is covered:
  – The case for auditing IT projects
  – Understanding the impact
  – Statistics on project failures
  – Purpose and benefits of audit involvement
  – Five key focus areas for project audits
  – Project audit planning

GTAG 13 – Fraud Prevention and Detection in an Automated World

• What's covered:
  – The fraud-related standards
  – Identifying IT fraud risks and schemes
  – Implementing IT fraud risk assessments
  – Using technology to prevent and detect fraud
  – Utilize data analysis to detect fraud

GTAG 14 – Auditing User-developed Applications

• Topics covered:
  – Definitions
  – User-developed applications risks
  – Internal audit’s role
  – Best practices, tools & techniques

106
GTAG 15 – Information Security Governance

- Major points:
  - Audits can help an organization understand the risks and options to create and effective ISG activity
  - ISG provides a framework for the organization to make appropriate risk mitigation decisions to protect and react to external and internal threats
  - ISG allows continuous feedback from line management to those charged with governance

What IIA members think of GTAG?

- GTAG survey tells that:
  - On Average, 92.4% participants think GTAG topics are important to their organization.
  - On Average, 81% participants think GTAG are useful or very useful to their organization.

Definition of Risk

- Risk is the possibility of an event occurring that will have an impact on the achievement of objectives.
  - Risk is measured in terms of impact and likelihood.
- Risk Management is a process to identify, assess, manage and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.
  - Residual Risk is the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.
Guide to the Assessment of IT Risk (GAIT)

• The GAIT Methodology, issued August 2007
• GAIT for IT General Control Deficiency Assessment, issued March 2008
• GAIT for Business and IT Risk, issued March 2008
  – Case Studies of Using GAIT, issued September 2008

Attribute Standard 1220:
Due Professional Care - Continued

• Implementation Standard 1220.C1 – Auditors should exercise due care during a consulting engagement 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.

Attribute Standard 1230:
Continuing Professional Development

• Internal auditors should enhance their knowledge, skills and other competencies through continuing professional development (Practice Advisory 1230-1).
  – Effective January 1, 2005 all IIA members must now report their CPE hours based upon their membership number, and not according to the certificate number (CIA, CCSA, CGAP, CFSA) as previously required.
IIA Attribute Standard 1300 – 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 (Practice Advisory 1300-1).
  – Attribute Standard 1310: Quality Program Assessments
  – Attribute Standard 1311: Internal Assessments
  – Attribute Standard 1312: External Assessments
  – Attribute Standard 1320: Reporting on the Quality Program
  – Attribute Standard 1330: Use of “Conducted in Accordance with the Standards”
  – Attribute Standard 1340: Disclosure of Non-Compliance

Attribute Standard 1310:
Quality Program Assessments

• The internal audit activity should adopt a process to monitor and assess the overall effectiveness of the quality program (Practice Advisory 1310-1).
  – The process should include both internal and external assessments.
    • Each part of the program should be designed to help the internal audit 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.

Attribute Standard 1311:
Internal Assessments

• Internal assessments should include (Practice Advisory 1311-1):
  – Ongoing reviews of the performance of the internal audit activity; and
  – Periodic Reviews performed through self-assessment or by other persons within the organization, with knowledge of internal audit practices and the Standards.
    • IIA’s Self-Assessment Guide – Tool 2A
**Attribute Standard 1312: External Assessments**

- External assessments, such as quality assurance review, should be conducted at least once every five (5) years by a qualified, independent reviewer or review team from outside the organization.
  - IIA’s Quality Assessment Manual
    - Chapter 1: The Evolving Internal Audit Landscape
    - Chapter 2: External Quality Assessment: A Business-focused Quality Assessment
    - Chapter 3: Self-assessment with Independent Validation
    - Chapter 4: Internal Quality Assessment
    - Chapter 5: Overview of Tools for Quality Assessment

**Standard 1312 – Endorsed and Strongly Recommended Guidance**

- Practice Advisory 1312-1: External Assessments
- Practice Advisory 1312-2: Eternal Assessment - Self Assessment with Independent Validation

**Attribute Standard 1320: Reporting on the Quality Program**

- The CAE should communicate the results of external assessments to those responsible for (Practice Advisory 1320-1).
  - Governance is the combination of processes and structures implemented by the board in order to inform, direct manage and monitor the activities of the organization toward the achievements of its objectives.
  - The Board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a non-profit organization, or any other designated body of the organization, including the audit committee, to whom the CAE may functionally report.
Attribute Standard 1330: Use of “Conducted in Accordance with the Standards”

- Internal auditors are encouraged to report that their activities are “conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.” – Practice Advisory 1330-1
  - However, auditors may use the statement only if assessments of the quality improvement program demonstrate that the activity is in compliance with the Standards.

Attribute Standard 1340: Disclosure of Non-Compliance

- Although the internal audit activity should achieve full compliance with the Standards and auditors with the Code of Ethics.
  - When non-compliance impacts the overall scope or operation of the activity, disclosure should be made to senior management and the board.

IIA Performance Standards

- Standard 2000 – Managing the Internal Audit Activity
- Standard 2100 – Nature of Work
- Standard 2200 – Engagement Planning
- Standard 2300 – Performing the Engagement
- Standard 2400 – Communicating Results
- Standard 2500 – Monitoring Progress
- Standard 2600 – Resolution of Management’s Acceptance of Risks
IIA Performance Standard 2000 – Managing the Internal Audit Activity

- The CAE should effectively manage the internal audit activity to ensure it adds value to the organization (Practice Advisory 2000-1).
  - Standard 2010 – Planning
  - Standard 2020 – Communication and Approval
  - Standard 2030 – Resource Management
  - Standard 2040 – Policies and Procedures
  - Standard 2050 – Coordination
  - Standard 2060 – Reporting to the Board and Senior Management

Definition of Added Value

- Value is provided by improving opportunities to achieve organizational objectives, identifying operational improvement and/or reducing risk exposure through both assurance and consulting services.

IIA Performance Standard 2010 – Planning

- The CAE should establish risk-based plans to determine the priorities of the activity, consistent with the organization’s goal.
  - Implementation Standard 2010.A1 – The 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.
  - Implementation Standard 2010.C1 – The CAE should consider accepting purposed consulting engagements based on the potential to improve management of risks, add value and improve the organization’s operations.
    - Those accepted should be included in the plan.
Standard 2010 – Endorsed and Strongly Recommended Guidance

- Practice Advisory 2010-1: Planning
- Practice Advisory 2010-2: Linking the Audit Plan to Risk and Exposures

Standard 2020 – Communication and Approval

- The CAE should communicate the activity’s plans and resource requirements, including significant interim changes, to senior management and to the board for review and approval (Practice Advisory 2020-1).
  - The CAE should also communicate the impact of resource limitations.

More of IIA’s Performance Standard 2000 – Managing the Internal Audit Activity

- Standard 2030 – Resource Management: The CAE should ensure that internal audit resources are appropriate, sufficient and effectively deployed to achieve the approved plan.
- Standard 2040 – Policies and Procedures: The CAE should establish policies and procedures to guide the internal audit activity.
- Standard 2050 – Coordination: The CAE should share information and coordinate activities with other internal and external providers of relevant assurance and consulting services to ensure proper coverage and minimize duplication of efforts.
Endorsed and Strongly Recommended Guidance

- Practice Advisory 2030-1: Resource Management
- Practice Advisory 2040-1: Policies and Procedures
- Practice Advisory 2050-1: Coordination
- Practice Advisory 2050-2: Acquisition of External Audit Services

Standard 2060 – Reporting to the Board and Senior Management

- The CAE should report periodically to the board and senior management on the activity’s purpose, authority, responsibility and performance relative to its plan.
  - Reporting should also include significant risk exposures and control issues, governance issues and other matters needed or requested by the board and senior management.

Standard 2060 – Endorsed and Strongly Recommended Guidance

- Practice Advisory 2060-1: Reporting to Board and Senior Management
- Practice Advisory 2060-2: Relationship with the Audit Committee
IIA Performance Standard 2100 – Nature of Work

• The internal audit activity should evaluate and contribute to the improvement of risk management, control and governance process using a systematic and disciplined approach.
  – Standard 2110: Risk Management
  – Standard 2120: Control
  – Standard 2130: Governance

Standard 2100 – Endorsed and Strongly Recommended Guidance

• Practice Advisory 2100-1: Nature of Work
• Practice Advisory 2100-2: Information Security
• Practice Advisory 2100-3: Internal Audit’s Role in the Risk Management Process
• Practice Advisory 2100-4: Internal Audit’s Role in Organization Without a Risk Management Process
• Practice Advisory 2100-5: Legal Considerations in Evaluating Regulatory Compliance Programs
• Practice Advisory 2100-6: Control and Audit Implications of e-Commerce Activities
• Practice Advisory 2100-7: The Internal Auditor’s Role in Identifying and Reporting Environmental Risks

Additional Std. 2100 – Endorsed and Strongly Recommended Guidance

• Practice Advisory 2100-8: The Internal Auditor’s Role in Evaluating An Organization’s Privacy Framework
• Practice Advisory 2100-9: Applications Systems Review
• Practice Advisory 2100-10: Audit Sampling
• Practice Advisory 2100-11: Effect of Pervasive IS Controls
• Practice Advisory 2100-12: Outsourcing the IS Controls
• Practice Advisory 2100-13: Effect on Third Parties on an Organization’s IT Controls
• Practice Advisory 2100-14: Audit Evidence Requirement
Standard 2110: 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.

Standard 2110: Risk Management - Continued

• Implementation Standard 2110.A2 – The activity should evaluate risk exposures relating to governance, operations and information systems regarding the:
  – Reliability and integrity of financial and operational information.
  – Effectiveness and efficiency of operations.
  – Safeguarding of assets.
  – Compliance with laws regulations and contracts.
• Implementation Standard 2110.C1 – During consulting engagements, internal auditors should address risk consistent with the engagement’s objectives and be alert to the existence of other significant risks.
• Implementation Standard 2110.C2 – Internal auditors should incorporate knowledge of risks gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization.

Standard 2110 – Endorsed and Strongly Recommended Guidance

• Practice Advisory 2110-1: Assessing the Adequacy of Risk Management Processes
• Practice Advisory 2110-2: The Internal Auditor’s Role in the Business Continuity Process
Standard 2120: Control

- The internal audit activity should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvements.
  - What are the IIA’s definitions of controls, control processes, control environment and adequate controls?

Standard 2120 – Endorsed and Strongly Recommended Guidance

- Practice Advisory 2120.A1-1: Assessing and Reporting on Control Processes
- Practice Advisory 2120.A4-1: Control Criteria

IIA Definitions

- **Control** – Any action taken by management, the board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.
  - Management plans, organizes and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
- **Control Processes** – The policies, procedures and activities that are part of a control framework, designed to ensure that risks are contained within the risk tolerances established by the risk management process.
IIA Definitions - Continued

• Control Environment – The attitude and actions of the board and management regarding the significance of controls within the organization.

• Adequate Controls – Present if management has planned and designed in a manner that provides reasonable assurance that the organization’s risks have been managed effectively and that the organization’s goals and objectives will be achieved efficiently and economically.

Assurance Implementation Standards for Performance Standard 2120

• 2120.A1 – Based on the results of the risk assessment, the activity should evaluate the adequacy and effectiveness of controls encompassing the organization’s governance, operations and information systems.

• 2120.A2 – Auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.

• 2120.A3 – 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 as intended.

• 2120.A.4 – Adequate criteria are needed to evaluate controls.

Consulting Implementation Standards for Performance Standard 2120

• 2120.C1 – Internal auditors should address controls consistent with the engagement’s objectives and be alert to the existence of any significant control weaknesses.

• 2120.C2 – Internal Auditors should incorporate knowledge of controls gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organizations.
Standard 2130: Governance

• The internal audit activity should assess and make appropriate recommendations for improving and governance process in its accomplishment of the following objectives:
  – 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.

Implementation Standards for Standard 2130: Governance

• **Assurance Standard 2130.A1** – The internal audit activity should evaluate the design, implementation and effectiveness of the organization’s ethics-related objectives, programs and activities.

• **Consulting Standard 2130.C1** – Consulting engagements objectives should be consistent with the overall values and goals of the organization.

Standard 2130 – Endorsed and Strongly Recommended Guidance

• **Practice Advisory 2130-1**: Role of the Internal Audit Activity and Internal Auditor in the Ethical Culture of an Organization
IIA Performance Standard 2200 – Engagement Planning

- Internal auditors should develop and record a plan for each engagement, including the scope, objectives, timing and resource allocations.
  - Standard 2201: Planning Considerations
  - Standard 2210: Engagement Objectives
  - Standard 2220: Engagement Scope
  - Standard 2230: Engagement Resource Allocation
  - Standard 2240: Engagement Work Program

Standard 2201 – Planning Considerations

- In planning the engagement, internal auditors should consider:
  - The objectives of the activity being reviewed and the means by which the activity controls its performance.
  - 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.
  - The adequacy and effectiveness of the activity’s risk management and control systems compared to a relevant control framework or model.
  - The opportunities for making significant improvements to the activity’s risk management and control systems.

Implementation Standards for Standard 2201 – Planning Considerations

- **Assurance Standard 2201.A1** – 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 results of the engagement and access to engagement records.
- **Consulting Standard 2201.C1** – Auditors should establish an understanding with clients about objectives, scope, respective responsibilities and other client expectations.
  - For significant engagements, this understanding should be documented.
“COSO”
Committee of Sponsoring Organizations of the Treadway Commission’s
*Internal Control – Integrated Framework*
Definition of Internal Controls

“The plan of organization and methods and procedures adopted by management to ensure that resource use is consistent with laws, regulations, and policies; that resources are safeguarded against waste, loss, and misuse; and that reliable data are obtained, maintained, and fairly disclosed in reports.”
Management Control Objectives

- An integral component of an organization’s management that provides reasonable assurance that the following objectives are being achieved:
  - Effectiveness and efficiency of operations,
  - Reliability of financial reporting, and
  - Compliance with applicable laws and regulations

Single Audit Requirement

“…each audit shall determine and report in writing whether the government, department, agency, or establishment undergoing the audit has internal control systems to provide reasonable assurance that it is managing federal financial assistance programs in compliance with applicable laws and regulations.”

Internal Controls = Management Controls

- Organization, policies and procedures that provide reasonable assurance that agencies:
  - Achieve intended program results
  - Use resources consistent with their mission
  - Deter fraud, waste and mismanagement
  - Follow laws and regulations
  - Obtain and report accurate information
  - Resolve audit findings promptly
Purpose of the Integrated Framework

• Establish a common definition serving the needs of different parties.
• Provide a standard against which organizations can assess their control systems and determine how to improve them.

What Internal Control Can Do

• Help achieve performance goals and objectives
• Help prevent loss of resources
• Help ensure reliable reporting
• Help ensure compliance with laws and regulations

What Internal Control Cannot Do

• Internal Controls can only help an entity achieve its goals and objectives
  – They cannot change inherently poor management or shifts in government policy
  – They cannot provide absolute assurance, only reasonable assurance
  – They cannot prevent simple errors or mistakes
  – They can be circumvented
Five Interrelated Components

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Control Environment

- Control Environment Factors
  - Integrity and Ethical Values
  - Incentives and Temptations
  - Providing and Communicating Moral Guidance
- Commitment to Competence
  - Management’s Philosophy and Operating Style
  - Organization Structure
  - Assignment of Authority and Responsibility

Risk Assessment

- Categories of Objectives
  - Operations Objectives
    - Mission (Outcomes/Outputs)
    - Efficiency, Effectiveness and Economy
  - Financial Reporting Objectives
    - Existence or Occurrence
    - Completeness
    - Rights and Obligations
    - Valuation or Allocation
    - Presentation and Disclosure
  - Compliance Objectives
    - Laws and Regulations
    - Terms and Conditions
Risk Assessment - Continued

• Risk Identification
  – Entity Level
    • External Factors
    • Internal Factors
  – Activity Level
    • Major units or functions
    • Involvement of management
    • Restructuring (Rapid Growth or Right-sizing)
    • New activities or technology

Control Activities

• Types of Control Activities
  – Top Level Reviews
  – Direct Functional or Activity Management
  – Information Processing
  – Physical Controls
  – Performance Indicators
  – Segregation of Duties

Control Activities - Continued

• Controls over Information Systems
  – General Controls
    • Data Center Operations Controls
    • System Software Controls
    • Access Security Controls
    • Application System Development and Maintenance Controls
  – Application Controls
    • Completeness and accuracy
    • Authorization and validity
**Information & Communication**

- **Information**
  - Strategic and Integrated Systems
    - Systems Support Strategic Initiatives
    - Integration with Operations
    - Coexisting Technologies
  - Information Quality
    - Content is appropriate
    - Information is timely
    - Information is current
    - Information is accurate
    - Information is accessible

---

**Information & Communication**  
*Continued*

- **Communication**
  - Internal
  - External

- **Means of Communication**
  - Verbal
  - Non-verbal

---

**Monitoring**

- Separate Evaluations
  - Scope and Frequency
  - Who Evaluates
  - The Evaluation Process
  - Methodology
  - Documentation
  - Action Plan
Monitoring - Continued

- Reporting Deficiencies
  - Sources of Information
  - What Should Be Reported
  - To Whom to Report
  - Reporting Directives

GAO Internal Control Standards

- GAO’s Internal Control Standards, June 1983
- GAO’s Standards for Internal Control in the Federal Government, November 1999

1999 GAO Standards for Internal Control in the Federal Government

- The Five (5) Standards for Internal Control
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communications
  - Monitoring
Control Environment
“Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.”

Risk Assessment
“Internal control should provide for an assessment of the risks the agency faces from both external and internal sources.”

Control Activities
“Internal control activities help ensure that management’s directives are carried out. The control activities should be effective and efficient in accomplishing the agency’s control objectives.”
Examples of Control Activities

- Top Level Reviews of Actual Performance
- Reviews by Management at the Functional or Activity Level
- Management of Human Capital
- Controls Over Information Processing
- Physical Control Over Vulnerable Assets
- Establishment and Review of Performance Measures and Indicators

Examples of Control Activities

Continued

- Segregation of Duties
- Proper Execution of Transactions and Events
- Accurate and Timely Recording of Transactions and Events
- Access Restrictions to and Accountability for Resources and Records
- Appropriate Documentation of Transactions and Internal Control

Control Activities Specific for Information Systems

- General Control
- Application Control
Information and Communications

“Information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities.”

Monitoring

“Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.”

Standard 2210 – Engagement Objectives

• Objectives should be established for each engagement.
  • Engagement objectives should reflect the results of this assessment.
  – Implementation Standard 2210.A2 – Auditors should consider the probability of significant errors, irregularities, non-compliance and other exposures when developing the engagement objectives.
  – Implementation Standard 2210.C1 – Consulting engagement objectives should address risks, controls and governance processes to the extent agreed upon with the client.
IIA Definitions

• **Engagements** are specific internal audit assignment, task or review activity, such as an internal audit, Control Self-Assessment review, fraud examination or consultancy.
  - An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.
• **Engagement Objectives** are broad statements developed by internal auditors that define intended engagement accomplishments.
• **Engagement Work Plan** is a document that lists the procedures to be followed during an engagement, designed to achieve the engagement plan.

Standard 2220 – Engagement Scope

• The established scope should be sufficient to satisfy the objectives of the engagement.
  - **Implementation Standard 2220.A1** – The scope should include consideration of relevant systems, records, personnel and physical properties, including those under the control of third parties.
  - **Implementation Standard 2220.A2** – 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.
  - **Implementation Standard 2220.C1** – In performing consulting, auditors should ensure that the scope of the engagement is sufficient to address the agreed-upon objectives.

Standard 2230 – Engagement Resource Allocation

• Internal auditors should determine appropriate resources to achieve engagement objectives.
  - Staffing should be based on an evaluating of the nature and complexity of each engagement, time constraints and available resources.
Standard 2240 – Engagement Work Program

- Auditors should develop work programs that achieve the engagement objectives. These work programs should be recorded.
  - Implementation Standard 2240.A1 – Work programs should establish the procedures for identifying, analyzing, evaluating and recording information during the engagement.
  - Work plans should be approved prior to implementation, and any adjustments approved promptly.
  - Implementation Standard 2240.C1 – Work programs may vary in form and content depending upon the nature of the engagement.

Standard 2200 – Endorsed and Strongly Recommended Guidance

- Practice Advisory 2200-1: Engagement Planning
- Practice Advisory 2210-1: Engagement Objectives
- Practice Advisory 2210.A1-1: Risk Assessment in Engagement Planning
- Practice Advisory 2230-1: Engagement Resources Allocation
- Practice Advisory 2240-1: Engagement Work Program
- Practice Advisory 2240.A1-1: Approval of Work Program

IIA Performance Standard 2300 – Performing the Engagement

- Auditors should identify, analyze, evaluate and record sufficient information to achieve the engagement’s objectives.
  - Standard 2310: Identifying Information
  - Standard 2320: Analysis and Evaluation
  - Standard 2330: Recording Information
  - Standard 2340: Engagement Supervision
Implementing Performance Standard 2300 – Performing the Engagement

• **Standard 2310: Identifying Information** – Internal auditors should identify sufficient, reliable, relevant and useful information to achieve the engagement’s objectives.

• **Standard 2320: Analysis and Evaluation** – Auditors should base conclusions and engagement results on appropriate analyses and evaluations.

Standard 2330: Recording Information

• Auditors should record relevant information to support the conclusions and engagement results.
  – **Implementation Standard 2330.A1** – The CAE should control access to engagement records.
  • The CAE should obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.
  – **Implementation Standard 2330.A2** – The CAE should develop retention requirements for engagement records.
  – **Implementation Standard 2330.C1** – The CAE should develop policies governing the custody and retention of records, as well as their release.

Standard 2340: Engagement Supervision

• Engagements should be properly supervised to ensure objectives are achieved, quality is assured and staff is developed.
Standard 2300 – Endorsed and Strongly Recommended Guidance

- Practice Advisory 2310-1: Identifying Information
- Practice Advisory 2320-1: Analysis and Evaluation
- Practice Advisory 2330-1: Recording Information
- Practice Advisory 2330.A1-1: Control of Engagement Records
- Practice Advisory 2330.A1-2: Legal Considerations in Granting Access to Engagement Records
- Practice Advisory 2330.A2-1: Retention of Records
- Practice Advisory 2340-1: Engagement Supervision

IIA Performance Standard 2400 – Communicating Results

- Internal auditors should communicate the engagement results.
  - Standard 2410: Criteria for Communicating
  - Standard 2420: Quality of Communications
  - Standard 2421: Errors and Omissions
  - Standard 2430: Engagement Disclosure of Non-Compliance with the Standards
  - Standard 2440: Disseminating Results

Standard 2410: Criteria for Communicating

- Communications should include the engagement’s objectives and scope as well as applicable conclusions, recommendations and action plans.
  - Implementation Standard 2410.A1 – Final communication of results should, where appropriate, contain the auditor’s overall opinion and/or conclusions.
  - Implementation Standard 2410.A2 – Auditors are encouraged to acknowledge satisfactory performance in engagement communications
  - Implementation Standard 2410.A3 – When releasing results to parties outside the organization, the communication should include limitations on distribution and use of the results
  - Implementation Standard 2410.C4 – Communication of the consulting progress and results will vary in form and contents depending upon the nature of the engagement and the needs of the client.
Implementing Performance Standard 2400 – Communicating Results

- **Standard 2420: Quality of Communications** – Communications should be accurate, objective, clear, concise, constructive, complete and timely.

- **Standard 2421: Errors and Omissions** – If a final communication contains a significant error or omission, the CAE should communicate corrected information to all parties who received the original communication.

Standard 2430: Engagement Disclosure of Non-Compliance with the Standards

- When non-compliance with the Standards impacts a specific engagement, communication of the results should disclose the:
  - Standard(s) with which full compliance was not achieved,
  - Reason(s) for non-compliance, and
  - Impact of non-compliance on the engagement.

Standard 2440: Disseminating Results

- The CAE should communicate results to the appropriate parties.
  - **Implementation Standard 2440.A1** – The CAE is responsible for communicating the final results to parties who can ensure that the results are given due consideration.
  - **Implementation Standard 2440.A2** – If not otherwise mandated by legal, statutory or regulatory requirements, prior to releasing results to parties outside the organization, the CAE should:
    - Assess the potential risk to the organization.
    - Consult with senior management and/or legal counsel as appropriate.
    - Control dissemination by restricting the use of the results.
Implementing Consulting Standards for Standard 2440: Disseminating Results

- **Standard 2440.C1** – The CAE is responsible for communicating the final results of consulting engagements to Clients.
- **Standard 2440.C2** – During consulting engagements, risk management, control and governance issues may be identified. Whenever these issues are significant to the organization, they should be communicated to senior management and the board.

Standard 2400 – Endorsed and Strongly Recommended Guidance

- Practice Advisory 2400-1: Legal Considerations in Communicating Results
- Practice Advisory 2410-1: Communication Criteria
- Practice Advisory 2420-1: Quality of Communications
- Practice Advisory 2440-1: Recipients of Engagement Results
- Practice Advisory 2440-2: Communications Outside the Organization
- Practice Advisory 2440-3: Communicating Sensitive Information Within and Outside of the Chain of Command

IIA Performance Standard 2500 – Monitoring Progress

- The CAE should establish and maintain a system to monitor the disposition of results communicated to management.
  - **Implementation Standard 2500.A1** – The CAE should establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.
  - **Implementation Standard 2500.C1** – The internal audit activity should monitor the disposition of results of consulting to the extent agreed upon with the client.
IIA Performance Standard 2600 – Resolution of Management’s Acceptance of Risks

• When the CAE believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the CAE should discuss the matter with senior management.
  – If the decision regarding residual risk is not resolved, the CAE and senior management should report the matter to the board for resolution.

Standards 2500 and 2600 – Endorsed and Strongly Recommended Guidance

• Practice Advisory 2500-1: Monitoring Progress
• Practice Advisory 2500.A1-1: Follow-up Process
• Practice Advisory 2600-1: Management’s Acceptance of Risks

IIA Code of Ethics

• Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. Internal auditors are expected to apply and uphold the following principles:
  – Integrity
  – Objectivity
  – Confidentiality
  – Competency
Independence

- The freedom from conditions that threaten objectivity or the appearance of objectivity. Such threats to objectivity must be managed at the individual auditor, engagement, functional and organizational levels.
  - **Objectivity** = An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made.
    - Objectivity requires the auditors to subordinate their judgment on audit matters to that of others.

Integrity

- The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment. Internal auditors:
  - Shall perform their work in honesty, diligence and responsibility.
  - Shall observe the law and make disclosures expected by the law and the profession.
  - Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession or to the organization.
  - Shall respect and contribute to the legitimate and ethical objective of the organization.

Objectivity

- Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstance and are not unduly influenced by their own interests or by others in forming judgments.
  - Internal auditors:
    - Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment.
      - This includes activities or relationships that may be in conflict with the interests of the organization.
    - Shall not accept anything that may impair or be presumed to impair their professional judgment.
    - Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.
Confidentiality

• Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so. Internal auditors:
  – Shall be prudent in the use and protection of information acquired in the course of their duties.
  – Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objective of the organization.

Competency

• Internal auditors apply the knowledge, skills and experience needed in the performance of internal auditing services. Internal auditors:
  – Shall engage only in those services for which they have the necessary knowledge, skills and experience.
  – Shall perform internal auditing services in accordance with the IIA Standards.
  – Shall continually improve their proficiency and the effectiveness and quality of their services.