Standards for the Professional Practice of Internal Auditing
The IIA “Red Book
The Basics of Internal Auditing
January 23-24, 2014

Sam McCall, PhD, CPA, CGFM, CIA, CGAP
Chief Audit Officer
Florida State University

What We Will Cover Today

- IIA Organization and Purpose
- The Professional Practice Framework
  - Mandatory Guidance
    - Code Ethics
    - The Definition of Internal Auditing
    - The Standards
  - Strongly Recommended Guidance (not Standards)
    * Revisions that are effective 1-1-13

Why Standards are Important

- Peace of mind for stakeholders and confidence in the quality product.
- They lay the ground work for the ultimate goal.
- They are the bar that every auditor should comply with.
- Help audit to be viewed as adding value.
- Help improve the dialogue about the profession.
- Broad perspective on what you’re supposed to be doing.
- Why Standards are Important
The IIA – Organization

- The Institute of Internal Auditors is an international organization
- Standards are global
- IIA membership includes the public, private, and nonprofit sector
- Government represents an important but relatively small percentage (approx. 10 - 12%) of the membership

IIA Milestones 1941 - 1974

- 1941 - IIA is established in NY
- 1947 - The Statement of Responsibilities is issued
- 1968 - The Code of Ethics is approved
- 1972 - The IIA moves to Florida – Altamonte Springs
- 1973 - 8000 CIA’s are grand-fathered
- 1974 - The first CIA Exam

IIA Milestones 1978 - 2012

- 1978 - The Standards are approved
- 1982 - California becomes the first state government to adopt the IIA Standards.
- 1986 – State of Florida passes the Chief Internal Audit Act
- 1992 - COSO defines internal control
- 1998 - 63,000 members, and the Guidance Task Force appointed
- 1999 – New definition of internal auditing and a new Framework for the Professional Practice of Internal Auditing
- 2014 – More than 180,000 members. Over 160 chapters with 70,000 members in North America
The International Professional Practices Framework

2012 IPPF

The “Red Book”

The IPPF & the professional practice of internal auditing

The International Professional Practices Framework (IPPF) organizes The IIA’s authoritative guidance. It provides a framework for performing and promoting internal auditing. It includes:

- **Mandatory Guidance**: Mandatory requirements consisting of Statements of basic requirements for professional practice of internal auditing and for evaluating the effectiveness of its performance, which are internationally applicable at organizational and individual levels. Includes Attributes, Performance, and Implementation Standards.
- **Practice Guides**: Detailed guidance for undertaking internal audit activities. Includes detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, including examples of deliverables.
- **Position Papers**: International Standards, Code of Ethics, Practice Advisories, etc.

AUTHORITATIVE GUIDANCE

**Mandatory**

**Non-mandatory**

**Strongly recommended**

**Definition**

Detailed guidance for conducting internal audit activities, including tools and techniques, programs, and step-by-step approaches, including examples of deliverables.

**Elements**

<table>
<thead>
<tr>
<th>IPPF Elements</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code of Ethics</td>
<td>Statement of fundamental purposes, roles, and scope of internal auditing.</td>
</tr>
<tr>
<td>International Standards</td>
<td>Mandatory requirements consisting of Statements of basic requirements for professional practice of internal auditing and for evaluating the effectiveness of its performance, which are internationally applicable at organizational and individual levels. Includes Attributes, Performance, and Implementation Standards.</td>
</tr>
<tr>
<td>Practice Guides</td>
<td>Detailed guidance for undertaking internal audit activities. Includes detailed processes and procedures.</td>
</tr>
<tr>
<td>Position Papers</td>
<td>USA statement to assist a wide range of interested parties, including those not in internal auditing profession, in understanding significant governance, risk, or control issues and delineating internal roles and responsibilities of internal auditing.</td>
</tr>
</tbody>
</table>

**IPPFF Framework**

**Mandatory Guidance**

- **Mandatory**
- **Non-mandatory**
- **Strongly recommended**
**IIA Code of Ethics**

- **Integrity** - establishes trust and thus provides the basis for reliance on the auditor’s judgment.
- **Objectivity** - a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others.
- **Confidentiality** - do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.
- **Competency** - apply the knowledge, skills, and experience needed in the performance of internal auditing services.

**Ethics**

- Red Book requires a periodic evaluation of the design, implementation, and effectiveness of the organization’s ethics-related objectives, programs, and activities.
  – This evaluation should be documented through a note or memos to the file, or through an audit on the subject matter.

**IIA Definition of Internal Auditing**

- Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
Assurance services involve the internal auditor's objective assessment of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Assurance Services
A 3-Party Arrangement

IIA - Definition of Consulting
• 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.
Consulting Services
A 2-Party Arrangement

Overview of the IIA Standards

Attribute Standards:
- Purpose, Authority and Responsibility .......... (1000)
- Independence and Objectivity ................... (1100)
- Proficiency and Due Professional Care .......... (1200)
- Quality Assurance and Improvement Program .. (1300)

Performance Standards:
- Managing the Internal Auditing Activity ........ (2000)
- Nature of Work ..................................... (2100)
- Engagement Planning ............................... (2200)
- Performing the Engagement ..................... (2300)
- Monitoring Progress ............................... (2400)
- Communicating the Acceptance of Risks ........ (2500)

Summary of Changes Effective 1-1-2013

- Clarify responsibilities for conforming with the Standards
- Increased focus on Quality Assurance & Improvement
- Clarify the CAE’s role to communicate unacceptable risk
- Explicitly require timely audit plan adjustments
- Emphasize coverage of risks to strategic objectives
- Changes to Glossary Terms

Source: IIA Website PowerPoint
Responsibilities for Conformance

Adding the following wording to the Introduction of the Standards:

The Standards apply to individual internal auditors and internal audit activities. All internal auditors are accountable for conforming with the Standards related to individual objectivity, proficiency, and due professional care. In addition, internal auditors are accountable for conforming with the Standards, which are relevant to the performance of their job responsibilities. Chief audit executives are accountable for overall conformance with the Standards.

Source: IIA Website PowerPoint

Exposure Results: Yes: 87%, No: 4.1%, No Opinion: 5.8%

Standards Board Decision: Adopt the exposed change

IIA Attribute Standards

- 1000 - Purpose, Authority, & Responsibility
- 1100 - Independence & Objectivity
- 1200 - Proficiency & Due Professional Care
- 1300 - Quality Assurance & Improvement Programs

1100 – Independence and Objectivity

- The internal audit activity must be independent, and internal auditors must be objective in performing their work.
Interpretation of 1110 - Organizational Independence

- Interpretation: Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:
  - Approving the internal audit charter;
  - Approving the risk based internal audit plan;
  - Approving the internal audit budget and resource plan;
  - Receiving communications from the chief audit executive on the internal audit activity’s performance relative to its plan and other matters;
  - Approving decisions regarding the appointment and removal of the chief audit executive; and
  - Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.

Proficiency - 1200

- 1230 - Continuing Professional Development
  - Hours are not stated in the Standards – Practice Advisory 1230-1 states IA’s should obtain CPE to satisfy requirements for certifications held.
  - CIA’s are required to obtain 80 hours every two years and to self-report.

Quality Assurance Systems - 1300

- Red Book requires the CAE to develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity:
  - Both internal and external assessments
  - Ongoing monitoring of the performance of the internal audit activity and periodic assessments performed through self-assessment or by other persons within the organization
- The results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually.
Quality Assurance Program - 1300

- Internal Assessments
  - On going monitoring and self assessment of work
- External Assessments
  - Should be conducted at least once every five years
  - Results of external reviews should be communicated to the Board

Increased Focus – Quality Assurance

1312 - External Assessments

External assessments must be conducted at least once every five years by a qualified, independent reviewer or assessment team from outside the organization. The chief audit executive must discuss with the board:

- The need for more frequent form and frequency of external assessments; and
- The qualifications and independence of the external reviewer or assessment team, including any potential conflict of interest.

Interpretation:

External assessments can be in the form of a full external assessment, or a self-assessment with independent external validation.

Source: IIA Website PowerPoint

Exposure Results: Yes: 86.5%, No: 7.6%, No Opinion: 5.9%

Standards Board Decision: Modify the exposed change

Change to Interpretation to 1312 – External Assessments

...In the case of an assessment team, not all members of the team have to have all of the competencies; it is the team as a whole that is qualified. The Chief Audit Executive uses professional judgment when assessing whether an assessor or assessment team demonstrates sufficient competence to be qualified.
Referencing the Standards

• According to the Red Book, CAE may state that the internal audit activity conforms with IIA standards:
  – Only if the results of the quality assurance and improvement program support this statement
  – Initial use of the conformance phrase is not appropriate until an external review has demonstrated that the internal audit activity is in conformance with the Definition, the Code of Ethics, and the Standards

IIA Performance Standards

• 2000 - Managing The Internal Auditing Activity
  • Planning
  • Risk assessment based
  • Communication and approval
  • Resource management
  • Policies and procedures
  • Coordination
  • Reporting to the Board and Senior Management
  • External Service Provider and Organizational Responsibility for Internal Auditing (New)

IIA - Performance Standards

• 2000 - Managing The Internal Auditing Activity

• 2100 - Nature of Work
  • Risk management
  • Control
  • Governance

• 2200 - Engagement Planning
  • Planning considerations
  • Engagement Objectives
  • Engagement Scope
  • Engagement Resource Allocation
  • Engagement Work Program

• 2300 - Performing the Engagement

• 2400 - Communicating Results

• 2500 - Monitoring Progress

• 2600 - Management’s Acceptance of Risk
Timely Audit Plan Adjustments

2010—Planning
The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals.

Interpretation:
The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization’s risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization’s business, risks, operations, programs, systems, and controls.

Source: IIA Website PowerPoint

Exposure Results: Yes: 92.5%, No: 4.3%, No Opinion: 3.2%
Standards Board Decision: Adopt the exposed change

Risk Assessment for Overall Audit Planning

• Red Book requires that the head of audit establish risk-based plans to determine the priorities of the internal audit activity
• Red Book further requires that the internal audit activity’s plan of engagements be based on
  – A documented risk assessment undertaken at least annually
  – The input of senior management and the board/audit committee
Risk Management Standard 2120

- Standard 2120 – Risk Management - The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes
- Interpretation – the internal audit activity may gather the information to support this assessment during multiple engagements. The results of their engagements, when viewed together, provide an understanding of the organization’s risk management processes and their effectiveness.

Inclusion of Strategic Risk 2120.A1

The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems regarding:

- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.

Source: IIA Website PowerPoint

Exposure Results: Yes: 90.6%, No: 5.9%, No Opinion: 3.5%
Standards Board Decision: Adopt the exposed change

Inclusion of Strategic Risk 2130.A1

The internal audit activity must evaluate the adequacy and effectiveness of controls responding to risks within the organization’s governance, operations, and information systems regarding the:

- Achievement of the organization’s strategic objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programs;
- Safeguarding of assets; and

Source: IIA Website PowerPoint

Exposure Results: Yes: 90.9%, No: 5.7%, No Opinion: 3.4%
Standards Board Decision: Adopt the exposed change
Suggested Risk Assessment Criteria for All Programs

- Risk Associated With:
  - Fiscal Impact
  - Strength of Management
  - Sensitivity and Public Relations
  - Loss, Non-Compliance, Corruption, or Fraud
  - Complexity of Activity
  - Risk to Public Welfare

Disseminating Results

2440 – Disseminating Results
The chief audit executive must communicate results to the appropriate parties.

Interpretation:
The chief audit executive or designee is responsible for reviewing and approving the final engagement communication before issuance and decides for deciding to whom and how it will be disseminated. When the chief audit executive delegates these duties, he or she retains overall responsibility.

Source: IIA Website PowerPoint

Exposure Results: Yes: 84.7%, No: 11.8%, No Opinion: 3.5%
Standards Board Decision: Modify the exposed change

IIA – Communicating Results (2400)

- Internal auditors should communicate the results of engagement results
  - Criteria for communicating – objectives, scope, conclusions, recommendations, and action plans
  - Quality of communication – accurate, objective, concise, constructive, complete, and timely
  - Errors and omissions – send corrected information to all parties that received the original report
IIA – Communicating Results (2400)

• Cont’d
  – Engagement disclosure of noncompliance with the standards – disclose standard, with reasons, and impact
  – Disseminating Results – communicate to appropriate parties. Consult with senior management prior to releasing to outside parties

Standard 2450
Overall Opinions

• Overall opinions must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.
  – Interpretation – identify
    • Scope and scope limitations
    • Risk, control framework, or other criteria used for the overall opinion
    • The overall opinion, judgment, or conclusion reached
    • Reasons for an unfavorable opinion must be stated

IIA – Monitoring Progress (2500)

• The CAE should maintain a system to monitor the disposition of results communicated to management
Follow up on Previous Audits

- Red Book requires the head of audit to
  - establish and maintain a system to monitor the disposition of results communicated to management
  - establish a follow-up process to monitor and ensure management actions have been effectively implemented or that senior management has accepted the risk of not taking actions
- To do this, auditors
  - Ask management of the audited entity to identify previous audits or studies that directly relate to the objectives of the audit, including whether recommendations have been implemented
  - Auditors use this information in assessing risk and determining the nature, timing, and extent of the current audit work

Acceptance of Risk

2600 – Resolution of Senior Management’s Communicating the Acceptance of Risks
When the chief audit executive believes concludes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is chief audit executive determines that the matter has not been resolved, the chief audit executive must report communicate the matter to the board for resolution.

Interpretation:
The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.

Source: IIA Website PowerPoint

Exposure Results: Yes: 89%, No: 7%, No Opinion: 4%
Standards Board Decision: Adopt the exposed change

Clarify the Definition of “Board”

Board –
A 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 chief audit executive may functionally report.

The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organization. Typically, this includes an independent group of directors (e.g., a board of directors, a supervisory board, or a board of governors or trustees). If such a group does not exist, the “board” may refer to the head of the organization. “Board” may refer to an audit committee to which the governing body has delegated certain functions.

Exposure Results: Yes: 88%, No: 5.7%, No Opinion: 6.3%
Standards Board Decision: Modify the exposed change
Practice Advisories
• Practice Advisories assist internal auditors in applying the Definition of Internal Auditing, the Code of Ethics, and the Standards. PA’s address approaches and methodologies but not detailed processes and procedures.

Practice Guides
• Practice Guides – provide detailed guidance for conducting audits. They include in-depth processes and procedures such as tools and techniques, programs, and step-by-step approaches.
  – The Global Technology Audit Guide
  – The Guide to Assessment of IT Risk

Position Papers
• Position Papers assist a wide range of interested parties in understanding governance, risk, or control issues.
  – The Role of Internal Auditing in Enterprise Risk Management
  – The Role of Internal Auditing in Resourcing the Internal Audit Activity
Example PIC Projects

- Small Audit Shops – How to Implement the Standards
- CAE Interaction with the Board
- Maturity Models
- Top-down and Risk Based Engagement Planning
- Organizational Governance
- Ethical Culture of an Organization
- Coordinating Risk and Management Assurance
- Anti-Corruption/Bribery
- Audit Department Strategy
- Independence
- Reasonable Assurance
- Root Cause
- Business Continuity Management
- Opinions

According to Richard Chambers – IIA President – The Key Challenges Facing Government Auditors

- Fiscal stress on government agencies
- Corresponding stress on agency and elected officials
- Constrained budgets of the audit function
- The pressure to demonstrate value
- The ageless challenge to do more with less
- Integrating risk assessment into audit processes
- Educating elected officials on auditor independence

Parting Thought

“You and your audit organization are perfectly designed to expect the results you achieve.”

Thank you for being here today!
Where to Find IIA Standards

- For more information, or if you have a question related to guidance or advocacy, please send an e-mail to guidance@theiia.org, or call +1-407-937-1100.
- Suggestions and comments regarding the Standards can be sent to:
  - The Institute of Internal Auditors
    Professional Practices Department
    247 Maitland Avenue
    Altamonte Springs, FL 32701-4201, USA
    E-mail: standards@theiia.org
    Web: [http://www.theiia.org](http://www.theiia.org)

Thank you

Name: Sam McCall
Office: (850) 644-0651
Mobile: (850) 688-0754
Email: smmccall@fsu.edu

Questions or Comments?