

“Yellow Book” and “Red Book”

The Risks, How to Handle, and What to Look for

Sam M. McCall, PhD, CPA, CGFM, CIA, CGAP, CIG



What We Will Cover Today

- Speakers involvement with the IIA and GAO
 - Each Organization's History and Structure
 - Applicability of the Standards to Practitioners
 - Overview of the Standards
 - A Comparison of Existing IIA and GAO Standards
 - Newly Revised IIA and Proposed GAO Standards
- * Whether auditor or auditee, everyone should have an understanding and appreciation for the standards that give direction to the auditing and accountability profession



Working With Both Organizations

- 1986 – FL Internal Audit Act
- 1990-1993 IIA - Government Relations Committee
- International Internal Audit Standards Board – 1994-2000
- 1998 – 16 member Guidance Task Force
 - Committee Chair of IPPF
 - Task force also defined internal auditing, addressed CPE, and quality control
- 2000-2010 - Professional Issues Committee
- 1991-1998 & 2000-2002 Government Auditing Standards Advisory Council
 - Independence Subcommittee
- 2012-2016 - Federal Accounting Standards Advisory Board
- * - Several articles written for *Internal Auditor* and *AGA Journal* on Red Book/Yellow Book



The Government Accountability Office

- Created by the Accounting and Budget Act of 1921
- The General Accounting Office is in the Legislative branch of government. Now the Government Accountability Office
- Internationally respected with several thousand staff
- GAO is headed by the Comptroller General of the U.S.
- CG appointed by the President with Congressional advice and Senate confirmation to one 15 year term
- First Yellow Books issued in 1972
- An updated exposure draft was issued in 2023



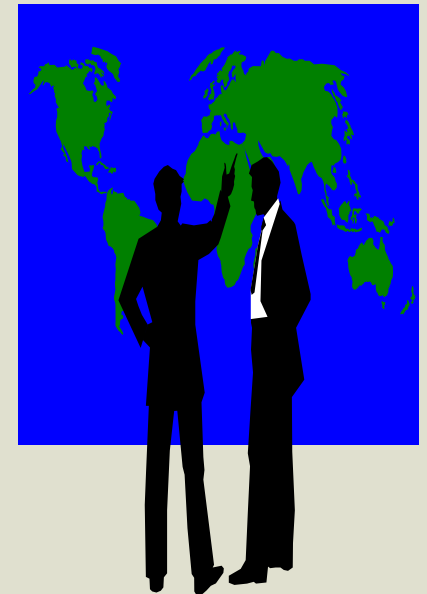
GAO/Comptroller General Responsibility

- To report to Congress on the results of financial and performance audits involving the receipt and expenditure of federal funds -wherever they may be spent
- CG appoints individuals to the Government Auditing Standards Advisory Council. The Standards have to be followed for financial audits of federal funds wherever spent
- The Standards are issued by the Comptroller General
- CG approves individuals to serve on the FASAB (the Federal Accounting Standards Advisory Board) along with the Secretary of the Treasury and Director of OMB



The IIA – Organization

- The Institute of Internal Auditors is an international organization
- Standards are global
- IIA membership includes the public, private, and nonprofit sector



IIA Milestones 1941 - 2024

- 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 1941 - 2024

- 1978 - The Standards are approved
- 1982 - California becomes the first state government to adopt the IIA Standards.
- 1992 - COSO defined internal control
- 1998 - 63,000 members, and the 16 person Guidance Task Force appointed – 20 years after the Standards were first issued
- 1999 – New definition of internal auditing and a new Framework for the Professional Practice of Internal Auditing issued
- 2024 - More than 245,000 global members and more than 193,000 CIA certifications worldwide.



Applicability of Standards

- IIA Standards
 - Can be required by law by a state or local government, by an internal audit charter, by a contract or by adoption by the internal audit organization.
- GAO
 - Federal Law, Uniform Guidance, Rule, or Regulation
 - State or local government law, rule, or regulation
 - Rules of the State Board of Accountancy
 - Other law, rule , regulation, contract, policy, or charter



Applicable Types of Audits

- IIA Standards apply to
 - Assurance Services
 - Consulting Services
- Both of the above are audits
- GAO Standards apply to
 - Financial Audits
 - Financial Statement
 - Financial Related
 - Attestation Engagements
 - Performance Audits
- CPA's conducting financial statement audits involving federal funds must follow GAO standards



Work of the CIA vs. CPA

- CIA's
 - Pass the CIA exam
 - Perform assurance and consulting services
 - Members of the IIA and must meet IIA requirements to maintain the certificate
 - Audits have “conclusions”
- CPA's
 - Must pass the CPA exam
 - Licensed by their respective State Board of Accountancy
 - Issue “opinions” on the audit of entity financial statements
 - Issue “conclusions” on performance audits



IIA's International Professional Practices Framework (IPPF)

Definition of Internal Auditing*
Code of Ethics*

*International Standards for the Professional Practice of Internal Auditing (Standards)**

- Attribute Standards:
 - Purpose, Authority, and Responsibility
 - Independence and Objectivity
 - Proficiency and Due Professional Care
 - Quality Assurance and Improvement Program
- Performance Standards:
 - Managing the Internal Audit Activity
 - Nature of Work (Governance, Risk Management, and Control)
 - Engagement Planning
 - Performing the Engagement (Identifying Information, Analysis and Evaluation, Documenting Information, and Engagement Supervision)
 - Communicating Results
 - Monitoring Progress
 - Resolution of Senior Management's Acceptance of Risks

GAO's Government Auditing Standards: GAGAS

Government Auditing:
Foundation and Ethical Principles

Standards for Use and Application of GAGAS

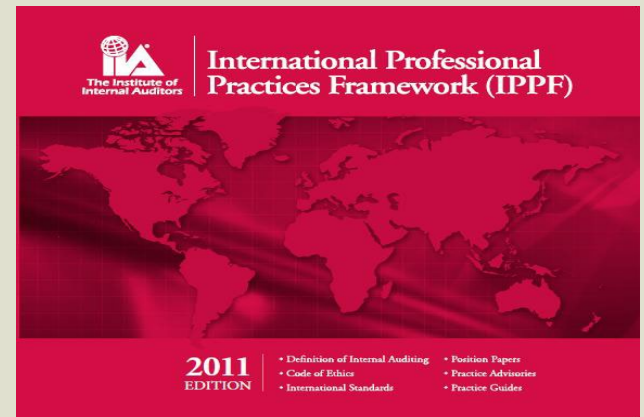
- General Standards:
 - Independence
 - Professional Judgment
 - Competence
 - Quality Control and Assurance
- Fieldwork Standards for Performance Audits:
 - Reasonable Assurance
 - Significance in a Performance Audit
 - Audit Risk
 - Planning
 - Supervision
 - Evidence
 - Audit Documentation
- Reporting Standards for Performance Audits:
 - Reporting
 - Report Contents
 - Distributing Reports



The International Professional Practices Framework

2017 IPPF

The “Red Book”

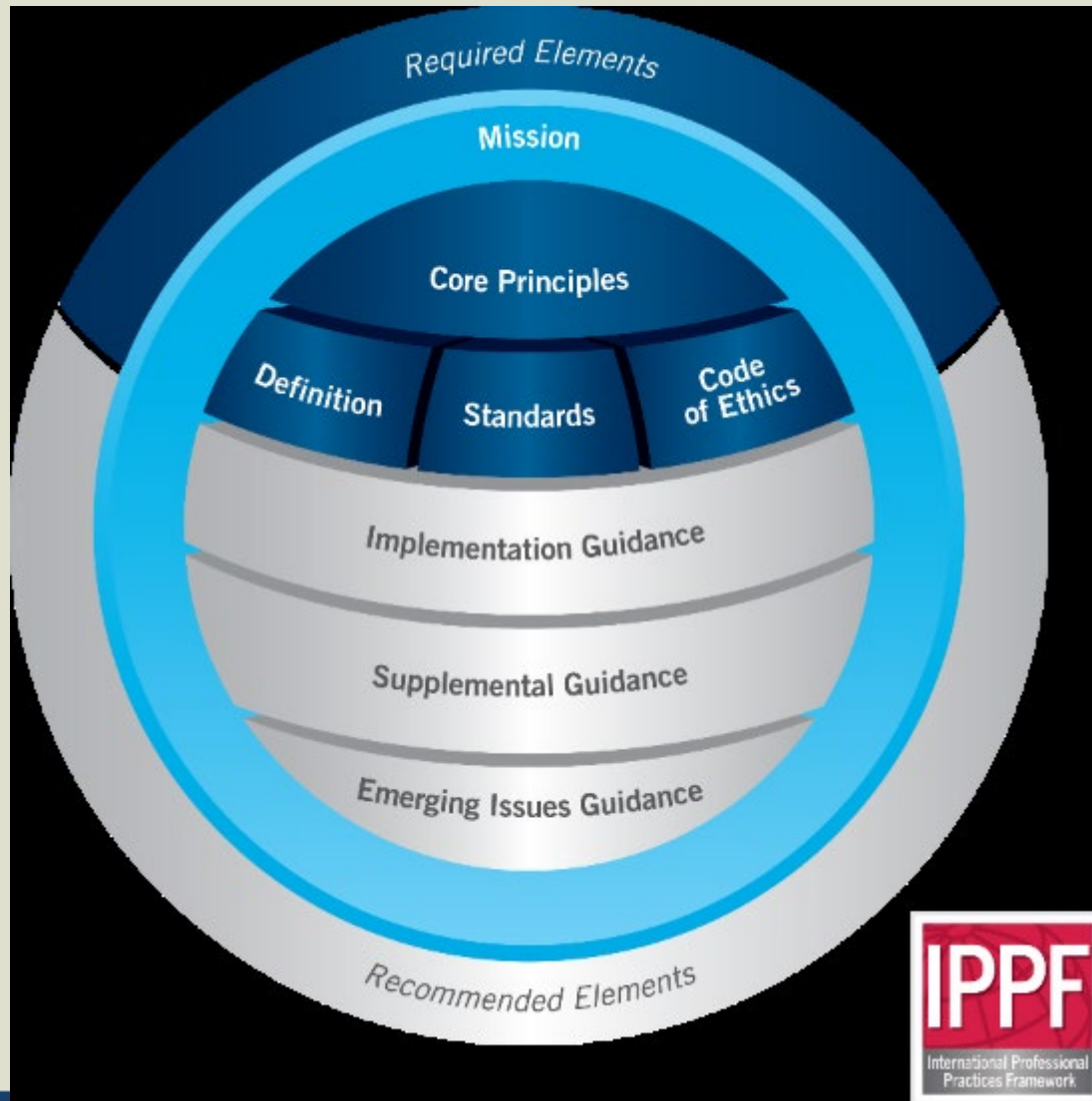


The IPPF is the conceptual framework that organizes authoritative guidance promulgated by the IIA.

The IPPF Establishes Mandatory and Recommended Guidance

- Mandatory Guidance
 - Core Principles for the Professional Practice
 - Definition of Internal Auditing
 - Code of Ethics
 - International Standards for the Professional Practice
- Recommended Guidance
 - Implementation Guidance
 - Supplemental guidance





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.

IIA Code of Ethics

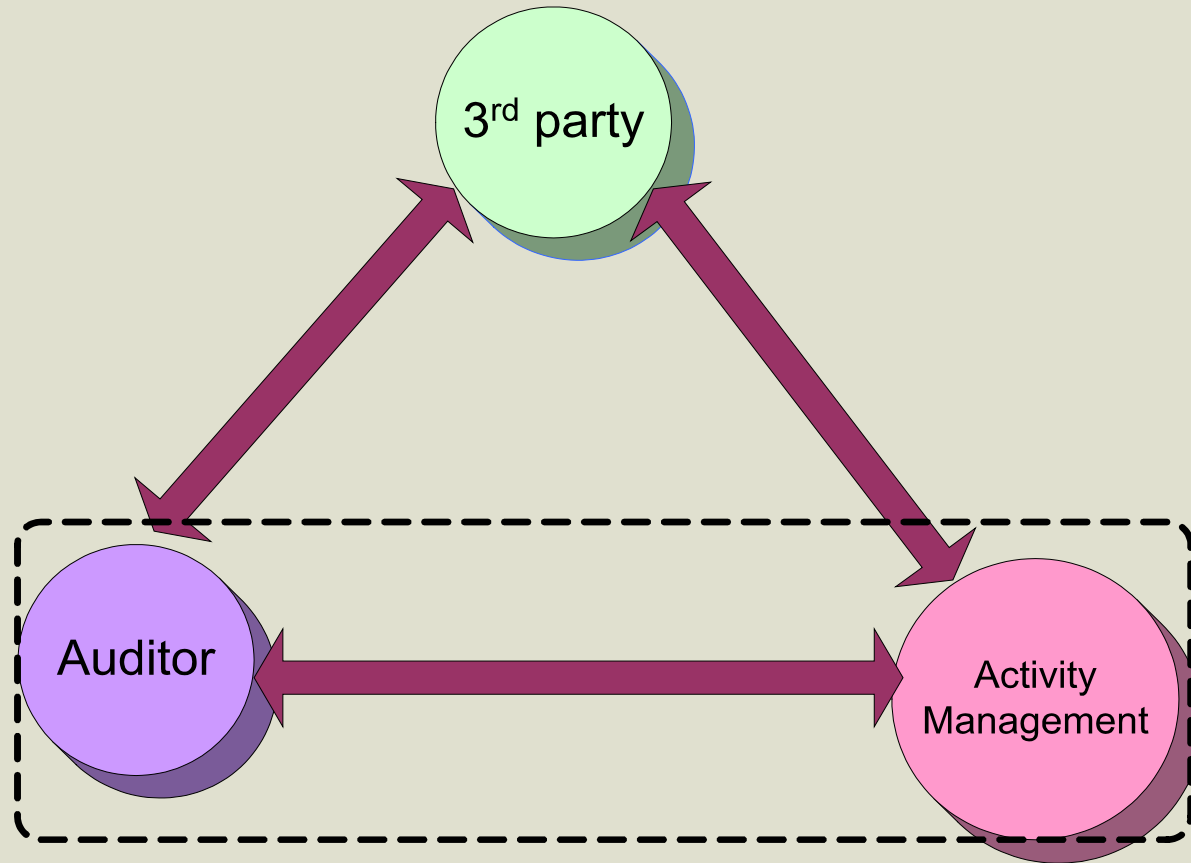
- **Integrity** - establishes trust and thus provides the basis for reliance on the auditor's judgment.
- **Objectivity** - a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others
- **Confidentiality** - do not disclose information without 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

Definition of Assurance Services

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
(see IIA *Auditor as Consultant*)



1100 – Independence and Objectivity

- The internal audit activity must be independent
- Internal auditors must be objective in performing their work.

GAO - Chapter 1 - Management Responsibilities for Carrying Out Public Functions

- The 5 E's
 - Economical
 - Efficient
 - Effective
 - Equitable
 - Ethical



GAO - Ethical “Principles”

- Ethical principles apply in preserving auditor independence
- Ethical principles that apply to performing work
 - The public interest
 - Integrity
 - Objectivity
 - Proper use of government information, resources, and positions
 - Professional behavior



GAO - Types of Audit Organizations

- External Audit Organizations
 - Structurally located outside (external to) the audited entity and report to third parties (ex - CPA firms)
- Internal Audit Organizations
 - Accountable to senior management and/or those charged with governance and generally do not report to 3rd parties
- Hybrid
 - A organization that is part of their respective organization and that reports externally like external auditors. They have a dual reporting responsibilities to their legislative body as well as to the agency head and management.
 - President Appointed IG with Congressional approval
 - Legislative appointed state auditor/city auditor
 - Elected City Auditor



GAO – Independence - Categories of Threats

1. Self interest threat
2. Self-review threat
3. Bias threat
4. Familiarity threat
5. Undue influence threat
6. Management participation threat
7. Structural threat



GAO - The Conceptual Framework

Applying the Conceptual Framework:

1. **Identify threats** to independence
2. **Evaluate** the significance of the **threats** identified, both individually and in the aggregate
3. **Apply safeguards** as necessary to eliminate the threats or reduce them to an acceptable level
4. **Evaluate** whether the safeguard is effective (independent in mind and independent in appearance)

Documentation Requirement:

Para 3.24: When threats are not at an acceptable level and require application of safeguards, auditors should **document** the safeguards applied.



GAO - Routine Audit Services and Nonaudit Services

Routine audit services pertain directly to the audit and include:

- **Providing advice** related to an accounting matter
- **Researching and responding** to an audited entity's technical questions
- **Providing advice** on routine business matters
- **Educating the audited** entity on technical matters

Other services **not directly related to an audit are considered nonaudit services**

Generally, routine audit services are insignificant for time incurred or resources expended and do not result in a formal report or formal work product.



GAO - Prohibited Nonaudit Services

Performing Management Responsibilities:

- **setting** policies and strategic direction for the audited entity;
- **directing and accepting responsibility** for the actions of the audited entity's employees in the performance of their routine, recurring activities;
- **having custody** of an audited entity's assets;
- reporting to those charged with governance on behalf of management;
- **deciding which** of the auditor's or outside third party's recommendations to implement;
- **accepting responsibility for management** of an audited entity's project;



GAO - Prohibited Nonaudit Services (cont.)

Performing Management Responsibilities (cont.):

- **accepting responsibility** for designing, implementing, or maintaining internal control;
- **providing services that are intended to be used as management's primary basis for making decisions** that are significant to the subject matter of the audit;
- **developing** an audited entity's performance measurement system when that system is material or significant to the subject matter of the audit; and
- **serving as a voting member** of an audited entity's management committee or board of directors.



GAO - Performance Audits

- Audits that provide findings or conclusions base on an evaluation of sufficient, appropriate evidence against criteria.
- Types
 - Program effectiveness
 - Internal control
 - Compliance
 - Prospective analysis
- A performance audit may have more than one overall objective.



GAO - Significance in Performance Audits

- The relative importance of a matter within the context in which it is being considered
- Auditor's must use professional judgment when evaluating significance
- The terms "significance" is comparable to the term "material" as used in financial statement engagements.



GAO - Fraud

- Maintain an attitude of professional skepticism
- Based on the risk assessment, design the audit to provide reasonable assurance of detecting any such fraud within the context of the audit objectives
- The assessment of fraud occurs throughout the audit process
- If fraud is identified notify appropriate persons with authority to investigate
- Fraud detected and not significant to the audit objectives may be reviewed as a separate engagement or referred to appropriate parties



GAO - Abuse

- Behavior that is deficient or improper
- Includes misuse of authority or position
- Abuse does not necessarily involve fraud
- When abuse **comes to your attention** determine if it is quantitatively or qualitatively significant to the audit objectives
- Auditors do not have to design the audit to identify abuse.



GAO - Ongoing Investigations

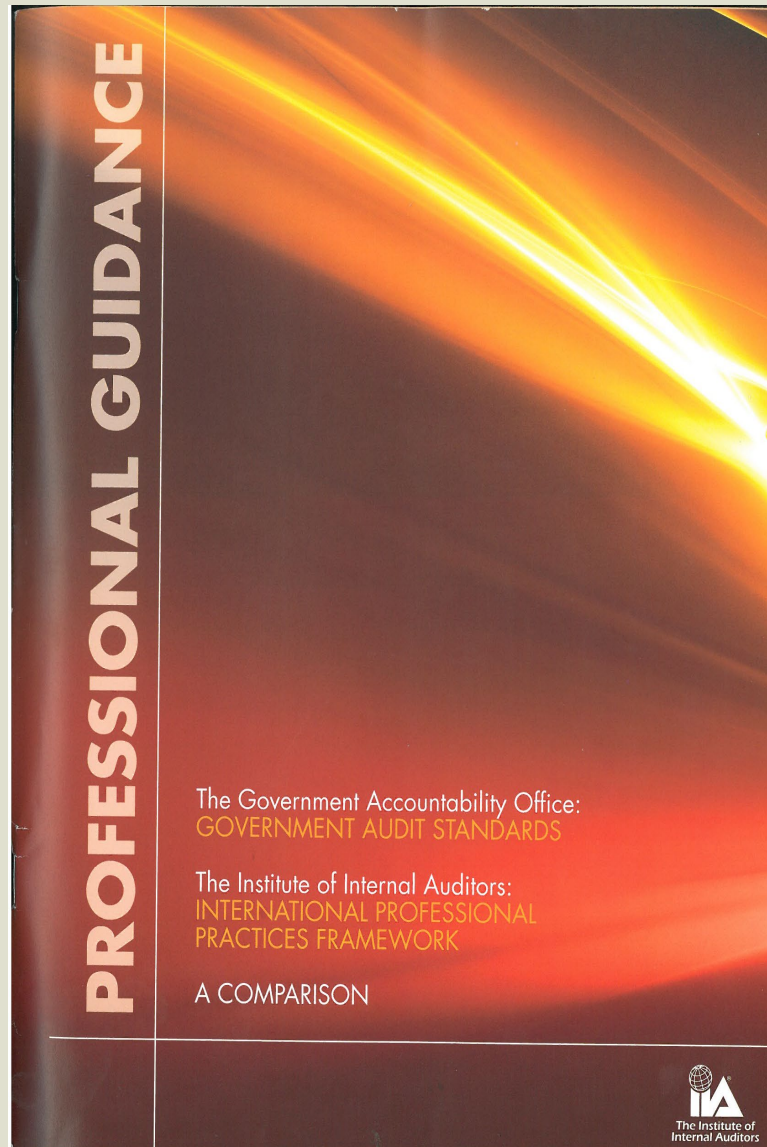
- In some cases it may be appropriate to work with investigators or legal authorities, or to withdraw from or defer further work on the audit to avoid interfering with an ongoing investigation
- Reporting what is already in the public record may be appropriate



Internal Control

- COSO has issued the Internal Control Integrated Framework
 - Control Environment
 - Risk
 - Control Activities
 - Information and Communication
 - Monitoring
- The GAO has issued the “Green Book”





Supplemental Guidance:
**IIA *INTERNATIONAL STANDARDS FOR
THE PROFESSIONAL PRACTICE
OF INTERNAL AUDITING***
**GOVERNMENT ACCOUNTABILITY OFFICE
GOVERNMENT AUDIT STANDARDS (GAGAS)**
A COMPARISON
2nd EDITION

 The Institute of
Internal Auditors | *Global*



Difference 1 - Consulting

- IIA –
 - Internal auditing is an independent, objective assurance and consulting activity. When performing consulting the auditor should not assume a management responsibility
- GAO – Consulting (advisory services) is a nonaudit service when assuming any management responsibilities. It is a type of service other than audits and attestation engagements. * Reconciliation – consulting under IIA is comparable to **performance auditing** under the GAO. The key is to be independent.



Difference 2 – Independence in Performing Audit Services

- IIA
 - Impairment if providing assurance services in an area where auditor had responsibility in the last year. For consulting no time limit stated.
- GAO – Be independent in mind and appearance and apply the conceptual framework. Identify threats to independence.
 - * Reconciliation – the CAE should document rationale, factors, and standards in making assignments.



Difference 3 – Performing Nonaudit Services

- IIA
 - Internal auditors performing nonaudit services should disclose that information to the Board.
- GAO – Performing nonaudit services when safeguards cannot overcome should be disclosed and the GAGAS compliance statement modified.
- Reconciliation – follow more detailed GAGAS. Consider safeguards and affect on audit organization.



Difference 4 – Reviewing Organization Ethics

- IIA
 - Requires (must make a) review of entire organization ethics objectives, program, and activities.
- GAO
 - Establishes ethical principles and expectation for government officials

Reconciliation – follow more rigorous IIA standards with periodic evaluation and note or memo to the file, or through an audit



Difference 5 – Risk Assessment for Overall Planning

- IIA
 - Requires documented annual risk- based audit plan based on organization goals. Input of Board and Senior Management must be considered
 - GAO
 - GAGAS focuses on planning individual engagements
- Reconciliation –
Comply with more
rigorous IIA Standard



Difference 6 – External Quality Assurance Review

- IIA
 - Requires independent review every 5 years
- GAO
 - Requires independent review every 3 years

Reconciliation –
suggest combined
review every 3 years



Difference 7 – Quality Assurance Systems

- IIA

- Organization must have internal and external quality assurance program and report results of internal assessments annually

- GAO

- Organization must annually analyze and summarize monitoring procedures with I.D. of corrective actions

Reconciliation – follow more detailed GAGAS to annually analyze and summarize



Difference 8 – Reporting Compliance with Standards

- IIA

- Organizations without a QIP may not be able to make this statement.

- GAO

- GAGAS provides specific language for compliance statement as to standards followed

Reconciliation – If appropriate, make reference to both GAO and IIA Standards.



Difference 9 – Referencing the Standards

- IIA
 - Reference to Standards cannot be made until a determination of compliance. There is a five-year grace period. Reference can be made when the IA activity formally adopts the Standards
 - GAO
 - Can make GAGAS statement and must have a QAIP review within 3 years of beginning first audit.
- Reconciliation – May reference GAGAS but not IIA until standards formally adopted**



Difference 10 - Fraud

- IIA
 - Evaluate fraud risk
 - Have knowledge to evaluate risk of fraud
 - Not expected to have expertise of an investigator
 - Use due care
- GAO
 - Have competence in fraud detection
 - Brainstorm fraud risk in planning
 - Design audit to detect fraud material/significant to audit objectives
 - Report findings to mgmt. and those in governance

Reconciliation – Rely on both and more on GAGAS



Difference 11 – Follow-up on Previous Audits

- IIA
 - CAE must have a system to monitor and follow up on previous audit findings
 - System addresses whether corrective action was taken or risk assumed
- GAO
 - Auditors should assess management follow up in context of “planned audit objectives”

Reconciliation - follow more detailed IIA standards and do not assume mgmt. responsibility



Difference 12 – Continuing Professional Education

- IIA
 - 40 hours per year for CIA's
 - IIA does not specify the number of hours required for staff that are not certified. CAE should make the determination
 - IIA encourages staff to become certified
 - GAO
 - Requires 24 hours CPE every two years in the government environment. If charging 20 % or more time on audits, requires an additional 56 hours. (i.e. - 80 hours every two years)
 - No distinction made between certified vs. noncertified staff
- Reconciliation – Follow the more detailed GAGAS**



IIA Standards

- 2017 – Previously the most recent edition
- 2023 – “Standards for the Professional Practice of Internal Auditing” renamed the “Global Internal Auditing Standards”
- New Standards issued January 2024
- Standards are effective January 2025, 12 months after release
- A new Quality Assurance Manual will follow in late 2024



New “Global Internal Audit Standards” issued January 9, 2024

- Free Webinars for Members and Non Members
 - 1-24-2024 Get to Know the New Global Internal Audit Standards (three times)
 - 2-13-2024 What the New Standards Mean to Quality Assessments





Notable Changes to Global Standards

- Strengthens the governance framework to respond to rapidly changing business environments
- Specific guidance for internal auditors in the public sector and small audit functions
- More flexible framework for auditors in different parts of the world
- Specific guidance and standards on critical issues like cybersecurity

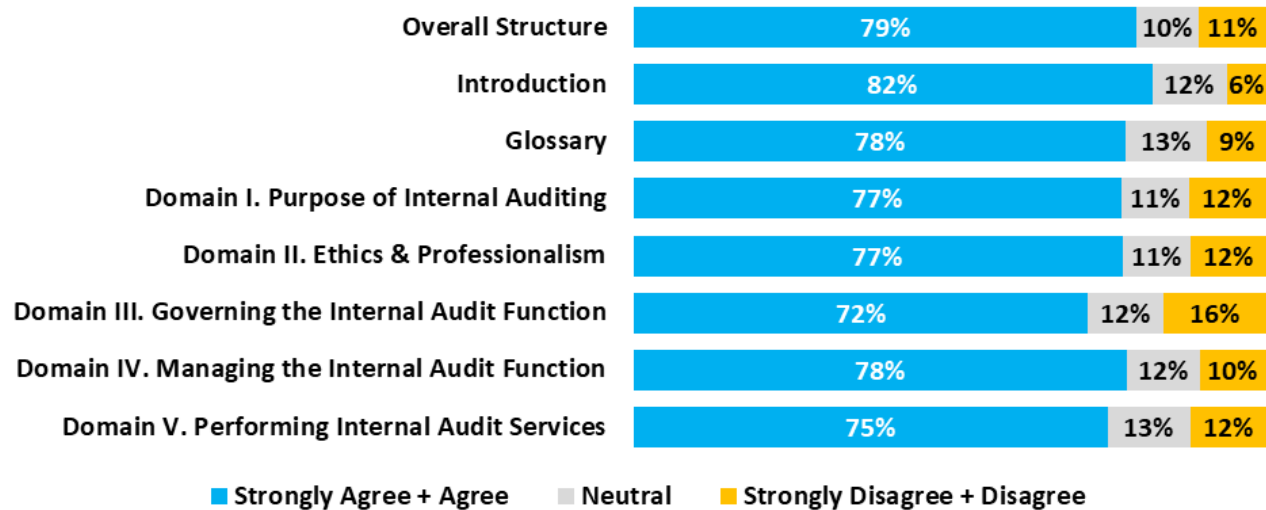


Global Internal Audit Standards Survey Results



Level of agreement among respondents

(required questions)



Total Completed Surveys: 1,612 Countries & Territories: 135 Specific comments: 18,964



Government Auditing Standards

- 2018 - Last full edition of GAGAS
- April 2021 – Technical update released
- January 2023 – Exposure Draft
- When issued, the latest draft will supersede the April 2021 and 2018 revision with a new focus on quality management
- 2023 Revision focus
 - Quality management system to be designed and implemented within two years of issuance
 - Evaluation of the system within three years of issuance



Focus of the New GAO Standards

- Organization leadership should proactively manage quality of its engagements and require a **risk-based approach** to design, implement, and operate a system of quality management.
- Risk should consider size, number of offices and geographic dispersion, knowledge of personnel, complexity of engagement work, and cost benefit considerations.
- New Standards harmonizes with new quality standards of
 - The International Auditing and Assurance Standards Board (IAASB)
 - Auditing Standards Board of the AICPA



Questions the Auditor Should Ask Management at an Entrance/Exit Conference

- For the proposed scope and objectives for this audit, what three things do you believe management/the Board would most want to know?
- If there were fraud or significant abuse in the program being audited, where would it most likely exist
- What keeps you up at night thinking about this program



The Auditors Responsibility

- To identify material/significant fraud within the scope and objectives of the audit
- To cover completely each audit objective
- If fraud occurred outside the audit objectives or if management or the Board ask why something was not addressed in an audit - respond unapologetically that it was not part of this audit. If important to them, the question could likely be addressed in another audit.



Questions Management Should Ask at an Entrance/Exit Conference

- What are the specific objectives of this audit – i.e. what questions do you intend to answer?
 - Go back over these objectives at the end of the audit – if the objectives changed during the audit ask why, and why was management not timely informed of the change



Questions Management Should Ask at an Entrance/Exit Conference

- What is the scope of the audit – i.e. the time period of the audit
 - Is the auditor looking at something that has subsequently been changed in terms of program operations. There is no current significant benefit to pointing out issues that have been addressed or subsequently corrected prior to starting the audit. Is the issue still relevant? Is it actionable?



Timeliness - IIA and GAO Audits

- The longer the time from when an audit starts to the time the audit ends, the more likely the issue has passed by the auditor and the less relevant the audit findings and conclusions
- Do we have **findings** or **issues for resolution**?



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



According to Richard Chambers – ACUA Annual Meeting - September 2016

- No one wants to hear their baby is ugly.
- There is a problem with the culture of the organization if management tries to seize control of internal audit at the time the CAE is about to retire.
- **A CAE has to have a strong internal compass**
- To add value
 - Think strategically
 - Know the business
 - Present alternatives
 - Jointly find solutions



Richard Chambers, David Walker, and Jim Thomas on Auditing

- Chambers on understanding organization culture
 - Tone at the top
 - Buzz at the bottom
 - Mood in the middle
- Walker on auditors providing value
 - Have hindsight, insight, and foresight
- Thomas – auditors should be “coaches” rather than “catchers”



McCall on Auditing

- Keep your Board /Agency Head informed as to the issues, what you are doing to address the issues, what they can expect next, and how **you** plan to address and resolve the issue.
- People at the top do not get upset an issue has occurred. They do have a right to get upset when the person working on the issue allows it to get out of hand such that it lands on their desk to handle
- Sometimes there are Differences of Opinion
 - Don't get drawn into an argument and make comments you will later regret.
 - Stay at a professional level – ask staff to read your draft comments for signs of personal bias and tone. Remind yourself to “always stay on a higher plain.” Do not try to make yourself look good at someone else's expense.
 - People bother you because you let them bother you.
 - Search for the truth and be clear enough to be proven wrong.
- If you have something to say, say it in the report. You can neither change, add to, or take back written comments once the report is publically issued.



Where to Find IIA Standards

- theiia.org
- For more information, or if you have a question related to guidance or advocacy, please send an e-mail to CustomerRelations@theiia.org, or call +1-407-937-1111.
- Suggestions and comments regarding the *Standards* can be sent to:
 - The Institute of Internal Auditors
Professional Practices Department
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746
E-mail: standards@theiia.org
Web: <http://www.theiia.org>



Where to Find the Yellow Book

- The Yellow Book is available on GAO's website at:

<https://www.gao.gov/yellowbook>



Parting Thought

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

Thank you for being here today!



Contact for Advice or for me to Conduct an IIA or GAO QAR

- Sam M. McCall
- Cell (850) 688-0754
- [E-mail: smmccall@fsu.edu](mailto:smmccall@fsu.edu)

