
GAO Standards Update

2016 Midwestern Intergovernmental Audit Forum
September 27, 2016

Yellow Book Update

A revised Yellow Book
Expected in 2017



Proposed Yellow Book Changes

- Structural/Format Update
 - Convergence with Other Standards
 - Ethics
 - Independence and Nonaudit Services
 - Competence/Continuing Professional Education
 - Quality Control and External Peer Review
 - Financial Audits
 - Performance Audits
-

**Proposed Yellow Book Changes:
Structural/Format Update**

- Yellow Book to follow a **clarified format** with requirements and application guidance separated
- **Application guidance** directly follows the related requirements
- **Simplifies** identification of requirements and facilitate linking requirements and related application guidance

**Proposed Yellow Book Changes:
Convergence with Other Standards**

We are working toward **convergence** with other standard-setting organizations, such as:

- The American Institute of Certified Public Accountants (AICPA)
- The Council of Inspectors General on Integrity and Efficiency (CIGIE)
- The International Auditing and Assurance Standards Board (IAASB)
- The International Organization of Supreme Audit Institutions (INTOSAI)

**Proposed Yellow Book Changes:
Ethics and Independence**

- **Ethics and independence combined** in a single section to highlight the interrelationship of these subjects
- **Promotes ethical requirements** rather than simply ethics principles and guidance
- Move toward **greater consistency** with other major audit standard setters

**Proposed Yellow Book Changes:
Independence and Nonaudit Services**

- Additional guidance on assessing sufficiency of management's **skills, knowledge, and experience** to evaluate the results of provided non-audit services
- Clarified guidance on provision of **investigations** and similar engagements as non-audit services

**Proposed Yellow Book Changes:
Competence/Continuing Professional Education
(CPE)**

- Additional initial **4 hour CPE requirement** to be Yellow Book Qualified ("YBQ")



**Proposed Yellow Book Changes:
Competence/Continuing Professional Education
(CPE)**

- **24 hour government CPE would remain:**
 - Yellow Book qualified counts toward the hours
 - 20 hours in other standards, statutory requirements, regulations, criteria, and guidance applicable to auditing or the objectives for the engagement(s) being performed
- No change to 80 hour CPE requirement for 2 year cycle

**Proposed Yellow Book Changes:
Quality Control**

- **Enhanced base** peer review and quality control requirements
- **Convergence/consistency** with other standard setters' requirements and guidance
- Annual **written affirmations of compliance** with policies and procedures on independence

**Proposed Yellow Book Changes:
External Peer Review**

- Peer review programs administered by many organizations meet the **minimum GAGAS peer review requirements**
- **Flexibility to select any peer review program**, so long as it meets the minimum GAGAS peer review requirements
- Additional **requirement to have a written agreement** on the fundamental aspects of the peer review

**Proposed Yellow Book Changes:
External Peer Review**

- Additional requirement to include **terminated engagements** in audit selection population
- Additional requirement to include **prior peer review reports** in scope of the peer review
- Clarification of **peer review risk**

**Proposed Yellow Book Changes:
Financial Audits**

- New guidance on understanding and **considering internal control** in the context of a GAGAS engagement
- Guidance on how overseas auditors can use **CPA equivalent internationally** to perform GAGAS audits
- **Providing peer review reports** when contracting for GAGAS audits
 - Moved from peer review section in current Yellow Book to financial audits section

**Proposed Yellow Book Changes:
Performance Audits**

- New guidance on **understanding and considering internal control** in the context of a GAGAS engagement
- Guidance on the **different approaches** to performance audits
- **Criteria** can be drawn from a broad continuum of sources, depending on the audit objective

**Proposed Yellow Book Changes:
Performance Audits**

- Clarification that assertions and **management representation letters are not required**
- Audit reports should be made **available to the public** unless restricted by the terms of the engagement or classified

Upcoming Attest Changes

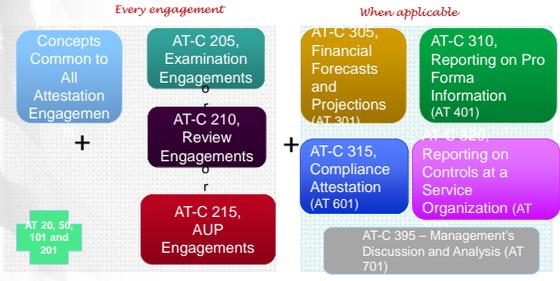
**Yellow Book incorporates the ATs
By reference from the Audit Standards Board
(ASB)**

**Recently Issued ASB Standards
....To be incorporated into the Yellow
Book**

**SSAE #18, *Attestation Standards: Clarification
and Recodification***

- Issued April 2016
- Effective for practitioners' reports dated on or after May 1, 2017
- Clarified, converged and restructured
- Will be codified in AT-C sections

SSAE #18 – Recodification and Structure



SSAE #18: Key Changes

- Requires a written assertion from responsible party.
 - If the responsible party is not the engaging party, the written assertion is not required but report is required to be restricted and include a statement that that the responsible party did not provide an assertion.
- Required representation letter.
- Risk assessment for examination engagements.
- More detailed requirements, such as to obtain an engagement letter.
- Moves guidance for reporting on internal control in an integrated audit (AT 501) to SASs.
- Retains guidance for MDA examinations (AT701) "as is".

SAS No. 130: Audit of ICFR Integrated with Audit of Financial Statements

- Moved from attestation standards (AT 501) to auditing standards.
- Applies when auditor is required to examine and report on effectiveness of internal control over financial reporting.
- Effective for integrated audits for periods ending on or after December 15, 2016.

Key Provisions of SAS No.130

- Removes option to examine and report on management's assertion about the effectiveness of internal control; required to examine and report directly on the effectiveness of ICFR.
- Highlights that COSO's *Internal Control – Integrated Framework* and the GAO's *Standards for Internal Control in the Federal Government*, provide suitable and available criteria.
- Clarifies that the risk factors considered in audit of ICFR are the same as those in the financial statement audit.
- Allows the auditor to use the work of internal audit

Current Topics in Auditing

- Direct Engagements
 - New Attestation section that would not require an assertion from the responsible party.
- Specified Procedures Engagements
- Sustainability Reporting
- Generic Internal Control Attestation Engagements
 - Engagements to examine internal control other than an examination of internal control over financial reporting that is integrated with an audit of financial statements.

Current Topics in Auditing

- Data Analytics
 - New auditing guide to replace Analytical Procedures Guide
 - Address use of data analytics and other analytical procedures
- Cyber Security
 - What's the effect on the audit of historical financial statements?
 - What types of attestation engagements could be performed?

Green Book

Revised Green Book: Standards for Internal Control in the Federal Government

Revised Green Book

Overview

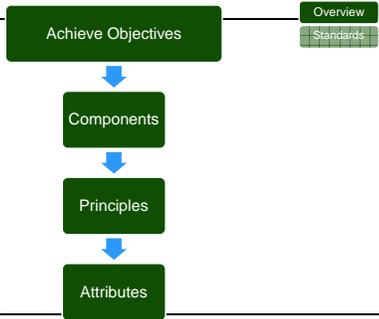
Standards





- Consists of two sections:
 - Overview
 - Standards
- Establishes:
 - Definition of internal control
 - Categories of objectives
 - Components and principles of internal control
 - Requirements for evaluating effectiveness

Overview: Components, Principles, and Attributes



Control Environment

1. Demonstrate Commitment to Integrity and Ethical Values
2. Exercise Oversight Responsibility
3. Establish Structure, Responsibility, and Authority
4. Demonstrate Commitment to Competence
5. Enforce Accountability

Risk Assessment

6. Define Objectives and Risk Tolerances
7. Identify, Analyze, and Respond to Risk
8. Assess Fraud Risk
9. Analyze and Respond to Change

Control Activities

10. Design Control Activities
11. Design Activities for the Information System
12. Implement Control Activities

Information & Communication

13. Use Quality Information
14. Communicate Internally
15. Communicate Externally

Monitoring

16. Perform Monitoring Activities
17. Remediate Deficiencies

An Effective Internal Control System

Evaluating the Effectiveness of an Internal Control System

Evaluating the Effectiveness of an Internal Control System

- An effective internal control system provides reasonable assurance that the entity will achieve its objectives.

- An effective internal control system has
 - each of the five components of internal control effectively designed, implemented, and operating and
 - the five components operating together in an integrated manner.
 - The 17 principles support the effective design, implementation, and operation of the associated components and represent requirements necessary to establish an effective internal control system.

Evaluating an Internal Control System – Key Controls

- Key controls often have one or both of the following characteristics:
 - Their failure might materially affect the entity's objectives, yet not reasonably be detected in a timely manner by other controls, and/or
 - Their operation might prevent other control failures or detect such failures before they have an opportunity to become material to the entity's objectives.

Evaluating the Effectiveness of an Internal Control System – Summary Determination

- For each principle, management makes a summary determination as to whether the principle is designed, implemented, and operating effectively.
 - Management considers the impact of deficiencies identified in achieving documentation requirements.
 - If a principle is not designed, implemented, or operating effectively, then the respective component cannot be effective.

- Based on the results of the summary determination for each principle, management concludes on the design, implementation, and operating effectiveness of each of the five components of internal control.

Evaluating the Effectiveness of an Internal Control System— Significance of Internal Control Deficiencies

Management evaluates the significance of a deficiency by considering the magnitude of impact, likelihood of occurrence, and nature of the deficiency.

- **Significance** refers to the relative importance of a deficiency to the entity achieving a defined objective
- **Magnitude of impact** refers to the likely effect that the deficiency could have on the entity achieving its objectives and is affected by factors such as the size, pace, and duration of the deficiency's impact.
- **Likelihood of occurrence** refers to the possibility of a deficiency affecting an entity's ability to achieve its objectives.
- **The nature of the deficiency** involves factors such as the degree of subjectivity involved with the deficiency and whether the deficiency arises from fraud or misconduct.

An Effective Internal Control System

Remediating Deficiencies

Remediating Deficiencies

- Management assigns responsibility and delegates authority to remediate the internal control deficiency.
- When determining the appropriate corrective actions to remediate an internal control deficiency, management considers the significance of the deficiency.
- Identifying the root cause of a deficiency can result in more meaningful corrective actions, which can help prevent the deficiency from recurring.

Remediating Deficiencies (cont.)

- Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis.
- Management, with oversight from the oversight body, monitors the status of remediation efforts so that they are completed on a timely basis.
- Management and the oversight body determine when the entity has sufficiently completed the corrective actions needed to remediate the deficiency.

Why Is Fraud Risk Management Important?

- Fraud poses a significant risk to the integrity of federal programs and erodes public trust in government.
- Fraud can be financial as well as nonfinancial (e.g., passport fraud), and it is difficult to measure fraud in a reliable way.
- Based on our prior reviews, we saw a need for federal managers to take a more strategic, risk-based approach to managing fraud risks.
- Effective fraud risk management helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are safeguarded.

Approaches to Considering Internal Control

- Process Audit Approach
- Program Audit Approach
- Entity Audit Approach





Examples of Objectives

Entity-level objectives	Transaction-level objectives
An organization's mission is to provide safe, affordable housing for low-income families, seniors, and people with disabilities.	A purpose of one of the organization's programs is to provide housing subsidies for seniors.
An organization's strategic goal is to improve the effectiveness of its communication with the public.	An objective of one of the organization's departments is to develop a plan for revising the organization's website to make it more user-friendly for the public.
An organization's vision is to be a trustworthy and reliable source of financial aid for college students.	An objective of one of the organization's processes is to monitor schools' compliance with federal student aid requirements.



Control Environment

Green Flags	Red Flags
✓ Management has developed an organizational structure with clearly defined roles.	✗ It is difficult to determine the entities or individuals that have responsibility for programs or particular parts of a program.
✓ Programs are in place to train personnel and reinforce standards of conduct.	✗ Personnel do not understand what behavior is acceptable or unacceptable.
✓ Management displays concern for internal control and is responsive to deviations or recommendations to improve internal control.	✗ Top management is unaware of actions taken at the lower level of the entity and does not promote an atmosphere of integrity within the organization.



Risk Assessment

Green Flags	Red Flags
✓ Management acknowledges risk exists and assesses and analyzes risk throughout the organization.	✗ The organization does not have a process in place to detect risks and only reacts to issues once they have become pervasive within the organization.
✓ The organization has programs in place to combat fraud, waste, and abuse.	✗ The organization is unaware of obstacles to its mission.
✓ The organization plans for and quickly adjusts to internal and external changes.	✗ The organization is not able to overcome obstacles to its mission efficiently or at all.

Information and Communication

Green Flags	Red Flags
✓ Staff are aware of and implement changes made by management.	✗ Management is using poor quality information or outdated information for making decisions.
✓ Management continually evaluates sources of data to ensure information is reliable and accurate.	✗ Management does not have reasonable assurance that the information it is using is accurate.
✓ Information is accessible and reliable for use internally and externally.	✗ Staff are frustrated by requests for information because it is time-consuming and difficult to provide the information.

Control Activities

Green Flags	Red Flags
✓ There are documented policies and procedures that are routinely reviewed and updated.	✗ Operating policies and procedures have not been developed, are outdated, or are not followed.
✓ Control activities described in policy and procedures are applied properly.	✗ Key steps to a process are not being performed.
✓ Designed control activities are clearly linked to the organization's objectives and related risks.	✗ Personnel and management are uncertain why processes are being performed or how processes are related to goals or objectives.

Monitoring

Green Flags	Red Flags
✓ Management implements changes to the control structure to enhance efficiency and effectiveness of procedures.	✗ Management does not evaluate programs or processes on an ongoing basis.
✓ Supervisor timely conduct and document reviews to detect and correct problems.	✗ Significant problems exist in controls and management is unaware of problems until a bigger problem occurs.
✓ Management documents and implements corrective action plans to ensure control deficiencies are addressed.	✗ There are unresolved problems with the other components: control environment, risk assessment, control activities, and information and communications.

Fraud Framework

GAO Issued

Relationship Between the Green Book and the Framework

Green Book	Fraud Framework
Provides standards and is required for managers.	Provides an implementing framework
Requires managers to assess fraud risks (Principle 8).	Provides guidance for implementing this requirement.
Includes principles and attributes related to all aspects of internal control.	Adapts Green Book principles and attributes to a fraud-specific context.

When Should You Consider Using the Framework?

- Auditors should consider using the Framework when engagement objectives relate to managers' efforts to
 - identify or assess fraud risks; or
 - prevent, detect, or respond to fraud.
- The concepts and practices are intended to apply to all fraud types, including
 - internal and external fraud;
 - financial and nonfinancial fraud; and
 - beneficiary fraud, contract fraud, etc.

How Does the Framework Relate to Existing Federal Efforts to Combat Fraud?

- The Framework complements existing federal efforts, including
 - the revised *Standards for Internal Control in the Federal Government* (effective Oct. 1, 2015);
 - improper-payments legislation; and
 - Office of Management and Budget guidance on improper payments (OMB A-123).
- However, the Framework is fraud-specific and applies to nonfinancial, as well as financial, fraud risks.

Who Can Use the Framework?

- The Framework's leading practices serve as a guide for **federal program managers** to use when developing or enhancing efforts to combat fraud in a strategic, risk-based manner.
 - Managers can use the Framework to help implement Principle 8 of *Standards for Internal Control in the Federal Government* – "Assess Fraud Risks."
 - Managers can tailor the Framework to their programs' operations and environment, including existing risk management efforts.



How Can Others Use the Framework?

- **Auditors** can use the Framework to help assess managers' fraud risk management efforts.
- **Managers of state, local, and foreign government agencies**, as well as **managers of nonprofit entities**, may find the Framework's concepts and practices useful for their fraud risk management efforts.

The Fraud Risk Management Framework



The Framework

- encompasses control activities to **prevent, detect, and respond** to fraud, with an emphasis on prevention;
- recognizes **environmental factors** that influence or help managers achieve their objective to mitigate fraud risks; and
- highlights the importance of **monitoring and incorporating feedback**.

What Are the Components of the Framework?

- **Commit:** Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
- **Assess:** Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
- **Design and Implement:** Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
- **Evaluate and Adapt:** Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.



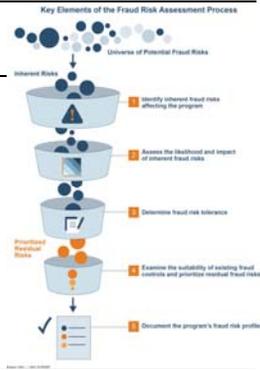
What Are the Components of the Framework? (cont.)

- **Commit:** Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
- **Assess:** Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
- **Design and Implement:** Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
- **Evaluate and Adapt:** Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.



How Can Managers Assess Fraud Risks?

- **Identify** fraud risks and **assess** their likelihood and impact.
- **Determine** fraud risk tolerance, and **examine** existing fraud controls.
- **Document** the program's **fraud risk profile**, including risk tolerance, prioritization of risks, and other key findings and conclusions.



What Are the Components of the Framework? (cont.)

- **Commit:** Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
- **Assess:** Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
- **Design and Implement:** Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
- **Evaluate and Adapt:** Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.



What Are the Components of the Framework? (cont.)

- **Commit:** Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
- **Assess:** Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
- **Design and Implement:** Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
- **Evaluate and Adapt:** Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.



**What Are the Components of the Framework?
(cont.)**

- **Assess:** Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
 - Tailor the assessment to the program and involve relevant stakeholders.
 - Assess the likelihood and impact of fraud risks, determine risk tolerance, and examine existing controls.
 - Document the program's fraud risk profile, including risk tolerance, prioritization of risks, and other key findings and conclusions.



**What Are the Components of the Framework?
(cont.)**

- **Design and Implement:** Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
 - Develop, document, and communicate an antifraud strategy.
 - Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
 - Establish collaborative relationships (such as working groups) and create incentives.



**What Are the Components of the Framework?
(cont.)**

- **Evaluate and Adapt:** Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.
 - Conduct risk-based monitoring on an ongoing basis and conduct evaluations periodically.
 - Collect and analyze data on instances of detected fraud to monitor fraud trends.
 - Use results of monitoring, evaluation, and investigations to improve prevention, detection, and response.



Ornate Desk (\$26,180)



Page 64

And

With a new desk, you would need a matching

65

Pictures of Desk Inscription and Matching Ornate Chair



Page 66

And

- Of course you would also need...

67

A Aeronautical GPS Unit

- Purchased for \$4,578 as a split purchase to circumvent the control of approval of purchases over \$2,500



Page 68

GPS + A Private Plane



- Perhaps use of a private plane to fly students.

- Dr. Program Manager stated:

“if students can navigate in a plane around the country, then they would be able to navigate themselves around the campus... and through life.”

Page 69

Warning Signs ...

- Internal Auditor had never performed an audit of the program or any internal audits for that matter
- Inadequate program documentation
- Unclearly communicated program objectives

70

Further Examination

- A review of expenditures by lead on the program, Dr. Program Manager, revealed that Dr. Program Manager took students on vacation like trips to areas all over the United States, including:



Page 71

Orlando, Florida



Page 72

Universal Studio Tours



Page 73

Student Activities

- During these trips students participated in conventions and retreat/resort activities such as white water rafting



Page 74

Catered Meals



Page 75

Data Analytics Could Help

8-Mar-06	Georgian Terrace Hotel-02052006	26-Feb-06	87.72
8-Mar-06	Chevron 00202298-02032006	26-Feb-06	39.05
8-Mar-06	Daily A Garage 2-02052006	26-Feb-06	80.00
8-Mar-06	Staples #148-02052006	26-Feb-06	70.20
8-Mar-06	Zyzyx-02022006	26-Feb-06	1,180.00
8-Mar-06	Zyzyx-02022006	26-Feb-06	2,500.00
8-Mar-06	Zyzyx-02022006	26-Feb-06	2,500.00
8-Mar-06	Umcop Cashier-02022006	26-Feb-06	60.00
8-Mar-06	Avis Rent-A-Car 1-02052006	26-Feb-06	447.88
8-Mar-06	Fedex Kinko'S #1814-02022006	26-Feb-06	4.71
8-Mar-06	Fedex Kinko'S #1814-02012006	26-Feb-06	25.18
8-Mar-06	Fedex Kinko'S #1814-02022006	26-Feb-06	202.23

Page 75

Data Analytics

14-Jun-06	Fedex Kinkos-04222006	26-May-06	11.32
14-Jun-06	Fedex Kinkos-04222006	26-May-06	1.89
14-Jun-06	Fedex Kinkos-04222006	26-May-06	7.32
14-Jun-06	The Gift Shop At Reg-04222006	26-May-06	124.84
14-Jun-06	Seattle Avionics Inc-03302006	26-May-06	2,484.00
14-Jun-06	Xm Satellite Radio-04202006	26-May-06	104.99
14-Jun-06	Seattle Avionics Inc-03312006	26-May-06	2,093.97

- Highlighted the transactions we found through data mining that looked questionable for both credit card expenditures and accounts payables expenditures

Page 77

Internal Controls

- What signs may have existed in the five key components of key controls?
- How would the 17 principles relate?
- What would be performance audit considerations?

78

Fraud Framework

- How could the GAO Fraud Framework help?

79

Data Analytics

- How could data analytics have helped in monitoring or at the audit?

80



Where to Find Us

- The Yellow Book is available on GAO's website at:
www.gao.gov/yellowbook
- The Green Book is available on GAO's website at:
www.gao.gov/greenbook
- For technical assistance, contact us at:
yellowbook@gao.gov or greenbook@gao.gov
or call (202) 512-9535

Page 81
