
New Audit Standards – Assessing Risk and Evaluating Internal Controls

Effects on IT Testing

Mickie E. Gray & David B. Hayes
U. S. Government Accountability Office

**MIDWESTERN
INTERGOVERNMENTAL AUDIT FORUM**

Topics

- Comparison of standards between financial and performance audits
 - Overview of the new standards
 - The new definitions and emphasis on evidence
 - The increased emphasis on recognition and consideration of risk
 - The new expectation on auditors' understanding of their auditee
 - How the new standards change the IT work needed to support audit engagements
-

Comparison of Standards – Financial and Performance Audits

- According to the Yellow Book, material = significant
 - Financial auditors “obtain sufficient appropriate audit evidence...to afford a reasonable basis for an opinion”
 - Performance auditors “provide reasonable assurance that evidence is sufficient and appropriate to support...conclusions”
 - Standards for assessment of risk, evaluation of internal controls, understanding of the entity and quality of evidence are the same
-

Required Reading

- SAS 109 – *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatements*
 - SAS 110 – *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*
 - SAS 112 – *Communicating Internal Control Related Matters Identified in an Audit*
 - AICPA Audit Risk Alert – *Understanding the New Auditing Standards Related to Risk Assessments*
 - *Government Audit Standards*, January 2007 Revision
 - *Internal Control - Integrated Framework Executive Summary*, www.coso.org
-

Understanding and Managing Audit Risk

Audit Risk = Risk of Material/Significant Error x Detection Risk

Auditors must access the quantity and quality of evidence available to meet their audit objectives (and control audit risk)

What types and levels of risk exist?

- Inherent risk – not controllable
 - Control risk – effected by the entity
 - Detection risk – addressed by audit procedures designed to reasonably detect error
-

Internal Control in the Context of the Audit

- SAS #105 states: “The auditor must obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures.”
 - The scope and level of IT testing should be determined by:
 1. The degree the subject of the audit relies upon information technology to support its operations
 2. The availability of sufficient and appropriate audit evidence from sources external to the IT control environment being evaluated
-

Evidence and Audit Procedures Responsive to Risk – at the detail level

Provide a clear linkage between audit procedures and risk

Each IT test procedure is determined by:

1. Significance of the risk
 2. Likelihood of a material/significant error
 3. Characteristic of the business process (or transaction)
 4. Nature of the control – manual or automated
 5. Ability of the auditor to perform substantive tests
-

What's New – How is IT Testing Different Under the New Standards? Staffing

- Requirement for sophisticated understanding and analysis of risk
 - Increased requirement to understand and assess internal controls
 - Increased level of documentation
-

What's New – How is IT Testing Different Under the New Standards? Field Work

- IT testing must be more closely tied to the audit objective – much more coordination between the subject matter experts (auditors) and IT specialists
 - IT testing of internal controls must be completed and conclusions supported prior to the design of the auditors' procedures (audit planning phase)
 - IT testing must cover a broader scope of the audit, including control testing over the auditee's preparation of information to be used as evidence
-

What's New – How is IT Testing Different Under the New Standards? Deliverables

- Documented understanding of the entity's information technology environment and operations
 - Documented identification and assessment of risks associated with IT
 - Detailed audit work programs that are directly tied to the auditors' need for detailed IT support
 - Improved documentation related to audit evidence
-

Contact Information

Mickie E. Gray, Senior Auditor, Financial Management
and Assurance Team, 202-512-6396, graym@gao.gov

David B. Hayes, Assistant Director, Applied Research and
Methods Team, 202-512-6306, hayesd@gao.gov
