

SAS 145 Overview

- Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement
- Issued by AICPA Auditing Standards Board
- Effective for audits of periods ending on or after Dec. 15, 2023
- Enhances risk assessment procedures

Objectives of SAS 145

- Improve audit quality through better risk identification
- Enhance linkage between risk assessment and audit response
- Modernize guidance for technology and complexity
- Increase professional skepticism

Key Changes from SAS 122

- Expanded guidance on IT and controls
- More emphasis on inherent risk factors
- Refined definitions of significant risks
- Stronger documentation requirements

Audit Risk Model

- Audit Risk = Inherent Risk × Control Risk × Detection Risk
- Focus on risk of material misstatement (RMM)
- Guides audit procedures
- Central to audit planning

Inherent Risk Explained

- Susceptibility of assertion to misstatement
- Before considering controls
- Varies by account and assertion
- Affected by complexity and judgment

Skepticism keeps surprises expensive for others.

Spreadsheets are helpful, not magical.

Fraud rarely sends a calendar invite.

Control Risk Explained

- Risk that controls fail to prevent or detect misstatements
- Depends on design and implementation
- Evaluated through control testing
- Key for reliance strategy

Detection Risk Explained

- Risk that audit procedures miss misstatements
- Controlled by auditor
- Managed through nature, timing, extent
- Inverse relationship with RMM

Risk of Material Misstatement

- Combination of inherent and control risk
- Assessed at financial statement and assertion levels
- Drives audit procedures
- Central concept in SAS 145

Understanding the Entity

- Industry, regulatory environment
- Nature of operations
- Ownership and governance
- Financial performance measures

Internal Control Framework

- Control environment
- Risk assessment process
- Information system
- Control activities
- Monitoring controls

*Controls earn trust through testing.
If it happened at year-end, curiosity is warranted.*

High risk deserves high attention.

Information Technology

- IT environment critical in SAS 145
- General IT controls (GITCs)
- Automated controls
- Risks from system changes

Inherent Risk Factors

- Complexity
- Subjectivity
- Change
- Uncertainty
- Susceptibility to misstatement due to bias or fraud

Spectrum of Inherent Risk

- Low to high spectrum
- Drives extent of audit procedures
- Higher risk requires more persuasive evidence
- Visual assessment approach

Significant Risks

- Require special audit consideration
- Often high inherent risk
- Fraud risks included
- Require specific responses

Fraud Risk Considerations

- Management override
- Revenue recognition
- Unusual transactions
- Journal entry testing

Professional Skepticism

- Questioning mind
- Critical assessment of evidence
- Alert to contradictions
- Essential under SAS 145

Risk Assessment Procedures

- Inquiry of management
- Analytical procedures
- Observation and inspection
- Walkthroughs

Walkthroughs

- Trace transactions through system
- Identify controls
- Validate understanding
- Required for key processes

Analytical Procedures

- Trend analysis
- Ratio analysis
- Compare expectations
- Identify unusual relationships

Assertions

- Existence
- Completeness
- Accuracy
- Valuation
- Rights and obligations
- Presentation and disclosure

Financial Statement Level Risks

- Pervasive risks
- Impact overall audit strategy
- Examples: weak governance
- Lead to broad responses

Assertion Level Risks

- Specific to accounts and disclosures
- More granular
- Drive detailed testing
- Linked to assertions

Identifying Risks

- Use understanding of entity
- Consider inherent risk factors
- Evaluate controls
- Document rationale

Assessing Risks

- Assess inherent and control risk separately
- Place on risk spectrum
- Determine significant risks
- Update continuously

Responding to Risks

- Design audit procedures
- Test controls if relying
- Substantive testing
- Adjust based on findings

Tests of Controls

- Evaluate design and implementation
- Test operating effectiveness
- Use sampling
- Necessary for reliance

*Controls earn trust through testing.
If it happened at year-end, curiosity is warranted.*

High risk deserves high attention.

Substantive Procedures

- Tests of details
- Substantive analytical procedures
- Address RMM directly
- Required for all material classes

Evidence and Documentation

- Sufficient appropriate evidence
- Link risks to procedures
- Document judgments
- Support conclusions

Scalability

- Applies to all entities
- Tailor to size and complexity
- Small entity considerations
- Avoid over-auditing

Smaller Entity Considerations

- Less formal controls
- More management involvement
- Simpler processes
- Alternative procedures

IT Risks

- Access controls
- Change management
- Data integrity
- Cybersecurity implications

Data Analytics

- Enhanced audit procedures
- Full population testing
- Pattern identification
- Supports risk assessment

Journal Entry Testing

- Focus on unusual entries
- End-of-period entries
- Manual adjustments
- Fraud detection

Accounting Estimates

- High inherent risk
- Management judgment
- Use of specialists
- Retrospective review

*Controls earn trust through testing.
If it happened at year-end, curiosity is warranted.*

High risk deserves high attention.

Related Parties

- Identify relationships
- Understand transactions
- Risk of concealment
- Disclosure requirements

Going Concern

- Assess viability
- Review forecasts
- Consider events
- Disclosures required

Subsequent Events

- Events after reporting period
- Adjusting vs non-adjusting
- Inquiry and review
- Disclosure considerations

Engagement Team Discussion

- Brainstorm risks
- Share insights
- Focus on fraud
- Enhance skepticism

Use of Specialists

- Valuation experts
- IT specialists
- Actuaries
- Integrate findings

Quality Management

- Firm-level controls
- Engagement quality review
- Monitoring
- Continuous improvement

Documentation Requirements

- Risk assessment process
- Identified risks
- Link to procedures
- Conclusions

Risk without response is just optimism.

Risk assessment is the steering wheel of the audit.

Undocumented skepticism is just private concern.

Common Pitfalls

- Overreliance on prior year
- Insufficient skepticism
- Poor documentation
- Ignoring IT risks

*Controls earn trust through testing.
If it happened at year-end, curiosity is warranted.*

High risk deserves high attention.

Best Practices

- Early planning
- Robust walkthroughs
- Continuous reassessment
- Strong documentation

Municipal Case Study Overview

- Mid-size municipal city with water utility, police, streets, and federal grants

Municipal Case Study Risks

- Inventory valuation
- System change risks
- Revenue cutoff
- Management bias

*Skepticism keeps surprises expensive for others.
Spreadsheets are helpful, not magical.*

Fraud rarely sends a calendar invite.

Municipal Case Study Responses

- Inventory observation
- IT control testing
- Cutoff testing
- Enhanced analytics

Emerging Risks

- Cyber threats
- AI systems
- Regulatory changes
- Global operations

Audit Strategy

- Overall approach
- Resource allocation
- Timing
- Supervision

Materiality

- Planning materiality
- Performance materiality
- Revision during audit
- Impact on procedures

Linking Risks to Procedures

- Direct relationship
- Higher risk → more testing
- Tailored procedures
- Avoid generic responses

Reassessment of Risk

- Continuous process
- New information
- Adjust procedures
- Update documentation

Communication with Governance

- Share significant risks
- Discuss findings
- Internal control deficiencies
- Required communications

Controls are promises until tested.

Risk assessment is where audits are won or quietly doomed.

Evidence is the language of assurance.

Internal Control Deficiencies

- Significant deficiency
- Material weakness
- Communicate timely
- Remediation suggestions

*Skepticism keeps surprises expensive for others.
Spreadsheets are helpful, not magical.*

Fraud rarely sends a calendar invite.

Audit Completion

- Evaluate evidence
- Final analytics
- Review disclosures
- Form opinion

*Materiality is precision with judgment.
Sampling is efficient until it samples chaos.*

Skepticism is professional courtesy with brakes on.

Audit Opinion

- Unmodified
- Qualified
- Adverse
- Disclaimer

Good planning is silent efficiency.

If everyone agrees instantly, ask one more question.

Documentation is memory that survives review.

SAS 145 Summary

- Enhanced risk focus
- Improved audit quality
- Greater emphasis on IT
- Better linkage to procedures

Key Takeaways

- Understand entity deeply
- Assess risks thoroughly
- Respond appropriately
- Document clearly

Risk without response is just optimism.

Risk assessment is the steering wheel of the audit.

Undocumented skepticism is just private concern.