

Sarbanes-Oxley (SOX) Training

Forvis Mazars

November 2026

Meet Our Speakers
Sarbanes-Oxley (SOX) Training



Allison Tanju

National Financial Reporting Partner | Financial Services



Prashant Panavalli

Principal, Internal Audit for Financial Services Leader

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Learning Objectives



By the end of this session, participants will be able to:

✓ **Roles & Responsibilities**	Identify the roles and responsibilities of process owners and control owners in maintaining an effective internal control environment
✓ **Control Execution & MRCs**	Apply leading practices for designing, executing, and documenting controls, including Management Review Controls (MRCs)
✓ **Auditor Expectations**	Recognize auditor expectations for control evidence, review precision, and support for key judgments and conclusions
✓ **Walkthrough Readiness**	Prepare for walkthroughs by maintaining effective narratives, flowcharts, and supporting documentation
✓ **IPE Completeness & Accuracy**	Understand Information Produced by the Entity (IPE), common IPE risks, and methods for demonstrating completeness and accuracy

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Introduction to Sarbanes-Oxley (SOX)

- This section will aim to define:
  - What is SOX? – SOX 302 and 404
  - Who must comply with SOX?
  - What are the most important sections of Sarbanes-Oxley for the organization?
  - How is the governance structured around Three Lines of Defense?
  - Who are the key players in SOX?



SOX at a Glance

2002
Passed after major corporate scandals

Trust
Investors and the public can rely on financial information

Accountability
Strong processes and controls; clear, accurate reporting

IT Impact
Access, security, and change controls over financial systems

Key SOX Sections

302
Accountability

The CEO and CFO must review and sign off on financial reports, confirming they are accurate and complete.

404
Internal Controls

Companies need processes in place that help ensure their financial reporting is reliable.

✓
Ongoing Assurance

Management has to regularly evaluates controls and reports any problems; external auditors also provide assurance that controls are working as expected.

Who Must Comply?

In Scope	Public U.S. companies, their subsidiaries, foreign companies listed in the U.S., and their audit firms
Preparing	Companies planning to go public (IPO) should start preparing early
Limited	Private companies and nonprofits don't follow all SOX rules (limited exceptions apply for nonprofits)
Protected	Whistle-blowers who report potential fraud; destroying company records carries serious consequences

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Who Must Comply with Section 404?

SOX 404(a)

Management Assessment

Applies to: all publicly traded companies

Management must annually assess and report on the effectiveness of internal controls over financial reporting, including any identified deficiencies.

SOX 404(b)

External Auditor Attestation

Applies to: depends on filer type (see below)

An independent auditor attests to the effectiveness of internal controls in the annual financial statements. More stringent, with more significant impacts.

Filer Type Determines SOX 404(b) Requirement

Filer Type	Public Float	Annual Revenue	SOX 404(a)	SOX 404(b)
Large Accelerated	$700MM or more	N/A	✓ Yes	✓ Yes
Accelerated (not SRC)	$250MM to less than $700MM	$100MM or more	✓ Yes	✓ Yes
SRC and Non-accelerated	Less than $75MM	N/A	✓ Yes	✕ No
	$75MM to less than $700MM	Less than $100MM	✓ Yes	✕ No
SRC and Accelerated	$75MM to less than $250MM	$100MM or more	✓ Yes	✓ Yes

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Proposed Changes to SOX 404(b)

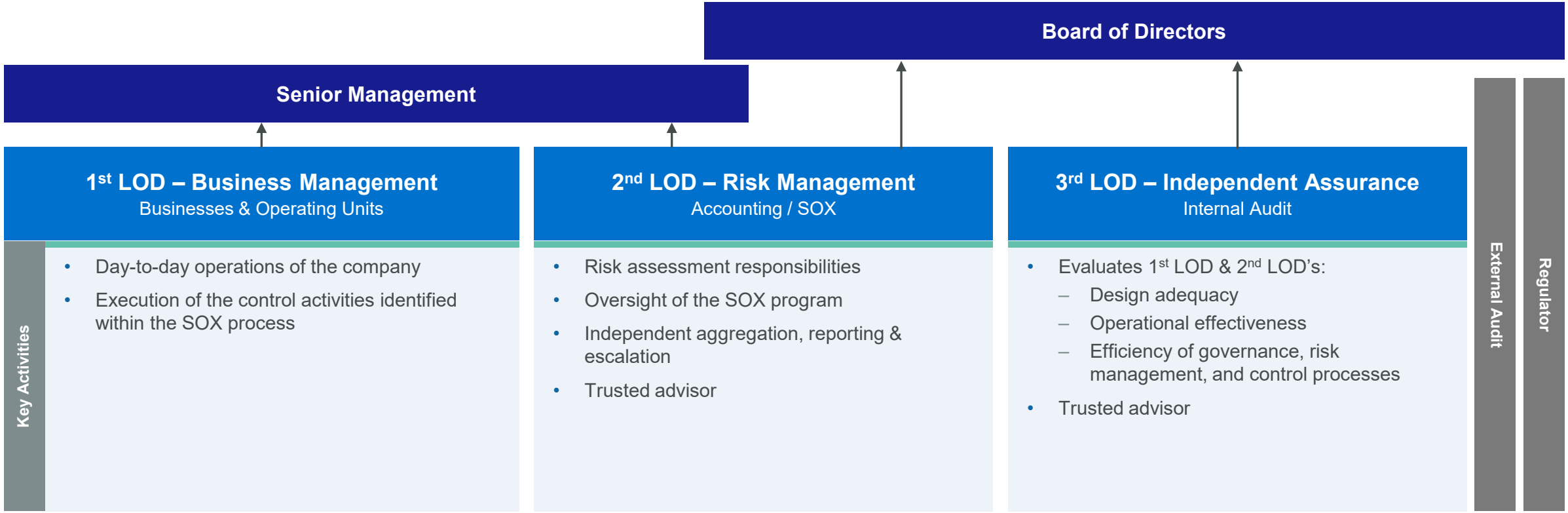
Proposed by SEC on May 19, 2026

- ❑ Only large accelerated filers would remain subject to Section 404(b)
- ❑ Thresholds proposed to increase for large accelerated filer status from current $700 million to $2 billion public float, based on the average stock price over the last 10 trading days of the second fiscal quarter
  - Threshold would have to be met for 2 consecutive years and would require at least 60 consecutive months of reporting before a company becomes a large accelerated filer

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Three Lines of Defense in Practice



© 2026 Forvis Mazars, LLP. All rights reserved.

Key Players in the SOX Process

WHO IS VESTED IN THE SOX PROCESS

External Users
Investors and creditors depend on reliable financial data and control structure

External Regulators
SEC (regulator of the reporting company) and PCAOB (regulator of the external auditors)

THE MOST IMMEDIATE PLAYERS YOU WILL ENCOUNTER DAILY

Control Owners
Responsible for execution of the control activities within the SOX process.

Accounting / SOX
Responsible for financial reports as well as establishing and maintaining the control environment.

Internal Audit
An independent, objective function of the organization that assists with management's assessment of the control environment and reports to the Audit Committee.

External Audit
Third party organization that performs testing and opines on the control environment and reports to the public.

SOX is only effective when everyone executes their respective roles and responsibilities

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Annual SOX Process

- This section will aim to define responsibilities for process owners for:
  - Why is What I Do Important?
  - What are MRCs?
  - How to Prepare for Walkthroughs?
  - What is IPE and Why Do I Care?
  - What are the leading practices for each phase?
  - How is AI being integrated into SOX for efficiency and value creation?

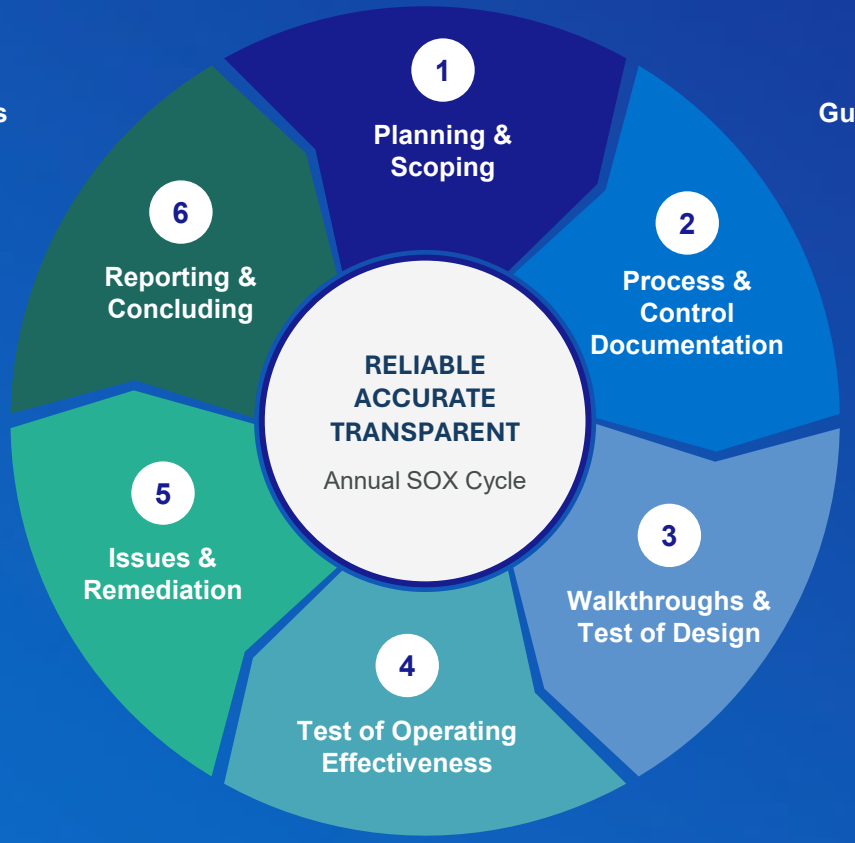


SOX Annual Process

Annually, each phase of the SOX process is executed and refreshed by the company

Annual outcomes

- Reliable financial reporting
- Stronger control environment
- Timely issue resolution
- Audit-ready evidence
- Investor & stakeholder trust



Guiding principles

- Risk-based scoping
- Top-down approach
- Clear control ownership
- Consistent evidence
- Continuous improvement

People | Process | Controls | Evidence | Reporting | Trust

SOX – Planning & Scoping
Key Activities & Roles

1

Risk Assessment

Focuses the evaluation on internal controls over financial reporting that adequately mitigate the risk of material misstatement of the financial statements.

2

Significant Accounts

The results of the evaluation determine the significant accounts, or priority areas, for SOX purposes.

Roles & Responsibilities

Management OWNER

Performs the risk assessment by evaluating external and internal factors that impact the inherent risk of a material misstatement due to error or fraud.

Control Owners EXECUTOR

Understand which processes are evaluated for SOX purposes and ensure the associated controls are executed.

Internal Audit FACILITATOR

Typically assists with facilitating the risk assessment based on management's evaluation. Decisions are made by management.

External Audit INDEPENDENT

Performs an independent risk assessment used to evaluate financial statement for significant accounts and establish materiality for misstatement.

Leading Practices

- Apply top-down, risk-based scoping approach that considers quantitative and qualitative materiality, significant accounts/disclosures, assertions, fraud risks, and nonroutine transactions.
- Assess systems, IPE, ITGCs, interfaces, service organizations, models, and regulatory-reporting dependencies
- Identify financial reporting risks and map to controls, processes and systems.
- Rationalize controls to a complete, precise key-control set with clear ownership and governance with focus on entity level controls.
- Engage business process leaders early to review the scoping fostering cross-function alignment and compliance embedded in daily operations.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

SOX – Control Owners
Why Control Owners are Important

Control Owners First Line of Defense	Control owners run controls day to day, putting them closest to the risks, gaps and misstatements a SOX program is designed to catch.

Why They Matter

Identify Risk DETECT
First line of defense to identify risk, gaps or misstatements.

Day-to-Day Oversight OVERSEE
Oversee the day to day.

Control Effectiveness OWN
Responsible for implementation, operation and ongoing effectiveness of control cycles.

Consistency ALIGN
Ensure consistent application and understanding of controls.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX - AI in Planning & Scoping
Use Case Considerations

AI USE CASES

- **Summarize audit history**
  Summarize prior audits, management letters, and regulator findings to ground the current-year plan.

- **Surface recurring themes**
  Extract recurring themes and open issues to inform current-year scope.

- **Draft planning inputs**
  Develop planning questions, scope considerations, and document request ideas.

- **Sharpen risk-based scoping**
  Analyze financial trends, prior findings, business changes, and emerging risks to identify higher-risk accounts, processes, systems, and assertions.

- **Accelerate risk & dependency mapping**
  Link accounts, assertions, processes, controls, systems, IPE, models, and third-party dependencies, highlighting potential coverage gaps.

- **Enable continuous risk sensing**
  Monitor changes in products, systems, organizational structures, transactions, and regulatory environments that may require SOX scope updates.

GUARDRAIL **AI should inform, not determine the SOX scope. Significant scoping judgments should remain explainable, validated, and approved by management.**

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Process & Controls Documentation
Documentation & Roles

Planning & Scoping | **Process & Control Documentation** | Walkthroughs & Test of Design | Test of Operating Effectiveness | Issues & Remediation | Reporting & Concluding

Risk & Control Matrix

One per process; maps controls to risks, flags key vs. non-key controls and names control owners.

Narrative

Written description of the process that identifies the key and non-key controls.

Process Flow

Visual diagram of the process that identifies the key and non-key controls.

Quarterly Certification: All process and control owners certify the financial statements and internal controls each quarter confirming the RCM and narratives are unchanged, or notifying Internal Audit of changes made or planned.

Roles & Responsibilities

Control Owners
MAINTAIN & EXECUTE

Keep documentation current with the process as it exists which can be ad hoc or at quarterly certification. Ensure the controls are being fully executed at the appropriate intervals and that evidence is being retained.

Internal Audit
ADVISOR

Assists with retaining process and control documentation and sharing recommendations and best practices; not responsible for executing controls.

External Audit
LEVERAGE

Uses process and control documentation developed by management to execute their audit. Management, Internal Audit, and External Audit should align documentation for consistency.

Leading Practices

- Maintain an integrated documentation set in which narratives, flowcharts, RCMs, application inventories, IPE inventories, and control descriptions align to one another.
- Write controls clearly: who, what, when, information used, criteria, exception handling, and evidence.
- Document each key control's objective, WCGW/risk, assertion, owner, frequency, preventive/detective nature, manual/automated classification, precision, evidence, IPE, IT and service-organization dependencies.
- Explicitly document management review control precision, including expectations, level of aggregation, quantitative and qualitative thresholds, investigation criteria, reviewer competence, follow-up procedures, and evidence of challenge.
- Enforce strict segregation of duties and maintain disciplined version control and change management over SOX documentation.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Control Owners
Documentation Essentials

Process Narratives & Flowcharts Matter

Cradle to Grave
Maintain narratives or flowcharts for each business cycle, described cradle to grave.

Owned by Management
Maintained by control owners / management and provided to Internal Audit.

Overall Process
Detail the overall process.

Thresholds & Roles
Document thresholds and who prepares or reviews within the cycle (titles work better than names).

What Should a Control Owner Document or Maintain

- **Sign Off**
  Who prepared, who reviewed + when
- **Procedures**
  What did the reviewer do? Use tickmarks or notes to detail and show tie-outs and checks performed
- **Precision**
  What thresholds were utilized by the reviewer and how were those applied?
- **Scope**
  What report / support was reviewed
- **Support**
  Maintain all support in one place (PDF, electronic or paper folder)
- **Review & Follow Up**
  What questions were asked, what variances were identified (if any), and what was the ultimate resolution?

> “
>
> **If you didn’t document it, you didn’t do it!**
>
> Narratives, flowcharts and review evidence are how control owners show a control was performed, at the right precision, by the right people.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

SOX – Review Control Evidence
Weak vs. Strong Documentation

EXAMPLE CONTROL **ACL calculation is reviewed quarterly for completeness and accuracy.**
Same control, same reviewer — is this good or bad control design and documentation? The evidence decides.

✕ WEAK EVIDENCE

Evidence retained
- ACL workbook signed by Controller
- Comment: “Reviewed and approved.”
- ACL calculation and entry attached

What’s missing
- ✕ No indication which tabs or calculations were reviewed
- ✕ No evidence assumptions were challenged
- ✕ No evidence management investigated changes in reserve
- ✕ No evidence the reviewer could detect a material error

AUDITOR CONCLUSION
Unable to determine whether the review control operated with sufficient precision.

VS

✓ STRONG EVIDENCE

Evidence retained
- ✓ ACL workbook signed by Controller
- ✓ Electronic tickmarks / comments showing which balances were recalculated and which were tied to prior quarter or other support (e.g., forecasts)
- ✓ Electronic tickmarks / comments showing tie-outs to the GL
- ✓ Final calculation agreed to the approved assumptions memo from the ACL Committee
- ✓ ACL calculation, supporting forecasts (and other information used in the review) and entry attached

AUDITOR CONCLUSION
Evidence demonstrates the reviewer performed procedures capable of identifying a material misstatement.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – AI in Process & Control Documentation
Use Case Considerations

AI USE CASES

- **Extract processes & controls**
  Pull process steps, key controls, owners, and frequencies from walkthrough notes, narratives, policies, and procedures.

- **Compare narratives to the RCM**
  Reconcile process narratives against the risk and control matrix to flag missing, outdated, or inconsistent controls.

- **Draft & refresh documentation**
  Accelerate documentation development by using captured process data to draft and refresh narratives, flowcharts, RCMs, control descriptions, test scripts, and process-change documentation.

- **Rationalize controls**
  Compare control descriptions across business units to identify overlapping, redundant, or contradictory controls to consolidate.

- **Improve quality & consistency**
  Identify mismatches across narratives, flowcharts, RCMs, IPE inventories, systems, risks, assertions, and controls.

GUARDRAIL **Control owners should validate AI-generated documentation, with appropriate version control, traceability, confidentiality, and change governance**

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Walkthrough & Test of Design
Key Activities & Roles

Walkthrough Sample of One	Meet with the process/control owner to walk through one current example of the control step by step, understand it and evaluate whether it is designed effectively.

Key Design Questions

Q1	Q2	Q3	Q4	Q5
Is the control designed effectively?	Was the control performed consistently?	Is it designed to be performed timely?	Will it mitigate the intended risk?	Does the control owner have the right authority & competencies?

Roles & Responsibilities

Control Owners PARTICIPATE
Walk the relevant parties through each control and answer follow-ups. Retain evidence of operation of control and provide it on request.

Internal Audit CONDUCT
Conducts walkthroughs with External Audit and/or alone, requesting documentation for the sample of one prior to, during or following the meeting.

External Audit COORDINATE & RELY
Coordinates with Internal Audit; selects its own sample or leverages IA's. Reliance depends on risk level of the process.

Leading Practices

- Trace transactions end-to-end from initiation to financial records, including systems, interfaces, accounting, and financial reporting.
- Use inquiry plus inspection, observation, or reperformance rather than inquiry alone.
- Evaluate whether controls have sufficient precision, frequency, competence, reliable information, and investigation criteria and corroborate IPE completeness and accuracy during walkthrough.
- Use walkthroughs to identify process changes, control gaps, IPE dependencies, and design weaknesses.
- Assess the points in the process where management could override controls or manipulate data.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Walkthrough & Test of Design
Running Effective Walkthroughs

TO MAKE WALKTHROUGH SESSIONS EFFECTIVE

PREPARE
Current-year example

Come prepared with a current-year example of the control.

UPDATE
Narratives & flowcharts

Come prepared with updated narratives or flowcharts, as relevant.

VALIDATE
Data used (IPE)

Ensure clarity around the use and validation of any data, known as information produced by the entity (IPE).

IMPORTANT
The person using IPE for a control needs to understand what type it is, and how it is covered, either by the control itself or by an upstream control that is performed.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – AI in Walkthrough & Test of Design
Use Case Considerations

AI USE CASES

- **Enhance walkthrough preparation**
  Analyze existing documentation and generate targeted questions focused on risks, control precision, IPE, IT dependencies, and process changes.

- **AI-guided walkthroughs**
  Support walkthroughs with AI-guided interviews that can help process steps, systems, risks, and controls.

- **Summarize walkthroughs & evidence**
  Summarize walkthroughs, organize walkthrough notes, and streamline evidence request collection.

- **Identify design gaps faster**
  Compare walkthrough discussions and evidence against documented processes, controls, systems, and expected attributes; AI proposes a preliminary design effectiveness assessment and structures design gaps.

- **Surface hidden dependencies**
  Analyze walkthrough information for previously unidentified IPE, spreadsheets, interfaces, automated controls, models, or third-party dependencies.

GUARDRAIL **AI can identify potential gaps and inconsistencies, but design conclusions should remain supported by human inquiry, inspection, observation, and corroborating evidence. The auditor calibrates severity and finalizes design effectiveness conclusions.**

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Test of Operating Effectiveness
Sample Testing & Roles

Test of Operating Effectiveness Sample Testing	Perform sample testing over key controls to validate that they are operating as intended over a period of time.

Sample Size Guidance

Frequency of Control	Assumed Population of Control Occurrences	Number of Control Occurrences to Test		
		Low	Mid	High
Annual	1		1	
Quarterly	4		2	
Monthly	12		2–5	
Weekly	52	5	10	15
Daily	250	20	30	40
Multiple times per day	Over 250	25	45	60

Roles & Responsibilities

Control Owners PROVIDE EVIDENCE
Provide all sample evidence to Internal and External Audit for testing and remain available during testing.

Internal Audit TEST
Conducts testing with External Audit and/or alone, requesting documentation for the selected samples.

External Audit COORDINATE & RELY
Coordinates with Internal Audit to understand processes and controls; selects its own sample or leverages IA's. Reliance depends on the risk level of the process.

Leading Practices

- Develop a risk-based testing strategy considering control frequency, financial-reporting risk, complexity, judgment, prior deficiencies, changes, reliance strategy, and the persuasiveness of evidence required.
- Validate population completeness before sample selection and retain sufficient evidence supporting the population, sampling methodology, selections, testing procedures, results, and conclusions.
- Expand testing insight beyond traditional sampling by using AI and analytics to analyze full populations, identify anomalies, and target higher-risk transactions or control executions.
- Test management review controls beyond sign-off by evaluating the reviewer's expectation, precision, thresholds, investigation of exceptions, challenge of assumptions, follow-up, and retained evidence.
- Establish the reliability of IPE and other information used in controls, including completeness, accuracy, report parameters, source data, extraction/query logic, interfaces, spreadsheets/EUC manipulation, and relevant ITGC dependencies

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Management Review Controls
Defining, Designing & Documenting

WHAT ARE MRCs?

Management Review Controls

A control where management reviews financial information, reports, or analyses and applies judgment to detect and investigate potential misstatements in financial reporting.

How they work

- Review estimates and other financial information
- Compare recorded amounts with expectations based on the control owner's knowledge and experience
- Investigate significant differences and act on the results

Typically **detective** (vs. preventive) controls that rely heavily on management's:

Review | **Challenge** | **Follow-up**

WHAT DOES A GOOD MRC LOOK LIKE?

WEAK CONTROL	STRONG (PCAOB-COMPLIANT) MRC
"Looks reasonable"	**Investigates specific thresholds / trends**
No evidence of questions	**Documents challenges and responses**
High-level review	**Uses defined expectations / criteria**
No follow-up	**Tracks and resolves exceptions**

How Can MRCs Be Documented?

- ✓ **Very detailed minutes**
  Including questions asked and their responses
- ✓ **Email chains**
  Showing questions raised and responses received
- ✓ **Notes & tickmarks**
  On supporting documents, showing the checks performed

Evidence must show the review, challenge and follow-up.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

SOX – Management Review Controls
Leading Practices & Documentation

LEADING PRACTICES FOR MRCs

Define the review objective & precision
Clearly link the MRC to the financial-reporting risk/assertion and establish expectations, aggregation level, and quantitative/qualitative investigation thresholds.

Evidence the review beyond sign-off
Document what was reviewed, procedures performed, questions/challenges raised, exceptions identified, and conclusions reached.

Demonstrate effective challenge of key judgments
Substantiate how significant assumptions, estimates, models, trends, and unusual items were evaluated and challenged.

Investigate & resolve exceptions
Retain evidence of follow-up, supporting analysis, adjustments, escalation, and final disposition of identified items.

Validate information used in the review
Establish the completeness and accuracy of reports, spreadsheets, model outputs, third-party data, and other IPE supporting the control.

WAYS TO DOCUMENT MRCs

Comments
Evidence questions, responses and resolutions (email or document); keep the original and final copies of the file reviewed.

Multiple Iterations
Retain each iteration of a document from draft to final, with corresponding updates.

Tie-Outs & Tick Marks
In PDFs, use text boxes to add notes, comments, tick marks and tie-outs.

Screenshots of Source
Screenshot totals from the source system or document and retain them with the file reviewed.

Signature
Sign off on the file once the review is complete, e.g. with Adobe PDF's signature function.

Workflow
Use workflow features in systems and applications to sign off and signify the review.

Questions to Ask

- ? What supporting documentation does the reviewer receive?
- ? What is considered an issue, unusual or out of the ordinary?
- ? What $ or % thresholds define an issue? Who set them, and are they documented?
- ? Who are issues escalated to?
- ? What is the timeline for resolution?
- ? When is an issue resolved? Are any unresolved?
- ? Where does the information come from, and how is its reliability verified?
- ? What corroborating evidence is gathered for issues?
- ? Could a manual process be automated? How long does preparation take?
- ? Are there guidelines to follow when an issue is found?
- ? Would this process prevent or detect material misstatements?

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Testing IPE
Types & Examples

WHAT IS IPE?

Information Produced by the Entity

Any information used in the execution of a control that is created by the company using applications, end-user computing tools or other means (including manually prepared). This includes information produced by third-party service providers / vendors.

> *IPE is used in the execution of many controls. The company must have controls in place to address its **completeness & accuracy.***

TYPES OF IPE

	WHAT IT IS	HOW TO GET COMFORT
Standard "Canned" system generated report	Designed by the application provider; typically can't be reconfigured by end users, though users may input parameters (e.g., dates).	Often relies on SOC 1 from vendors. Confirm it is canned if it's listed in SOC 1 coverage or in IT vendor handbook, else reach out to the vendor.
Custom Queried / ad-hoc report	Built or configured by IT (or by software provider at company's request) for specific needs, e.g., a SQL query on the application database; may be subject to change management. Includes ad-hoc queries created by end users in executing control, which are more likely to contain errors.	Maintain report parameters and review inputs as part of the control; apply additional scrutiny to ad-hoc queries.
Manual Manually prepared	Prepared by control owners, e.g., Excel files or schedules.	Ensure completeness and accuracy through control performed (e.g., recalculations, verify inputs) or ensure its covered by an upstream control.

COMMON EXAMPLES OF IPE

- System reports obtained from queries run by control owners or IT
- Third-party & external specialist reports (valuation firms, actuaries)
- Excel files manually prepared by control owners
- User access lists extracted from IT systems
- Presentations or memos used in MRCs
- Printed or PDF reports
- Text (.txt) files
- Information downloaded into Microsoft Access database
- System-generated reports from an application

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Testing IPE
IPE Risks & Validation

WHAT ARE THE RISKS RELATED TO IPE? *Following the data from source to end-user tool*

1

Source Data
Source data used in the IPE is not complete or accurate. Controls do not exist upstream or as part of the related control to ensure complete and accurate data input.

2

Extraction
A. Extracted data is not the intended data or is incomplete, query/extract was developed incorrectly B. User enters incorrect parameters when extracting.

3

Computation
Computations or categorizations performed in the extraction are not accurate.

4

Export to EUC
Data extracted from IT application to the end-user tool is not complete or accurate. The data did not export completely and accurately to the end user.

5

EUC Changes
Information added or changed using end-user tool is not complete or accurate. The data was manipulated incorrectly.

These risks are linear and may not all be applicable. Some may rely on 3rd party providers; others may rely on queries created by management.

HOW TO VALIDATE IPE

01 **Evaluate the program / query**
Obtain and evaluate the programs or queries generating the report.

02 **Evaluate parameters**
Obtain and evaluate the parameters used to run the report.

03 **Sample the data**
Sample data in the resulting report.

04 **Identify data sources**
Identify where the data comes from (database, system).

EVIDENCE RETAINED BY MANAGEMENT

- ✓ Program code / queries
- ✓ Screenshots of parameters used to run the report
- ✓ Report dates
- ✓ Report validation supporting documents

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – AI in Test of Operating Effectiveness
Use Case Considerations

AI USE CASES

- **Testing & anomaly detection**
  Help identify outliers using explainable criteria and automate population-level test coverage.

- **Continuous monitoring**
  Support monitoring of key risk indicators and control performance in real time.

- **Expand testing insight**
  Go beyond traditional sampling by using AI and analytics on full populations: validate evidence completeness, run population rules, flag anomalies and exceptions, and target higher-risk transactions or control executions.

- **Accelerate evidence review**
  Compare documents, organize support, identify missing evidence, and highlight inconsistencies across control executions.

- **Strengthen MRC & IPE testing**
  Identify unusual trends, missing thresholds, unresolved exceptions, report inconsistencies, or evidence that does not demonstrate sufficient reviewer challenge.

GUARDRAIL **AI-generated outputs used as audit evidence should be validated for reliability, traceability, and completeness**

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Issues & Remediation
Purpose, Roles & Responsibilities

Planning & Scoping | Process & Control Documentation | Walkthroughs & Test of Design | Test of Operating Effectiveness | **Issues & Remediation** | Reporting & Concluding

Issue Management Purpose	Guides how the company identifies, assesses, documents, tracks, manages and reports Issues and related Management Actions across the company. It provides a consistent, enterprise-wide approach and enables the company to manage risk effectively.

The Framework

Consistent guidance to all associates on managing Issues and Management Actions

Unified view of Issues across the company for leaders, committees and Boards to effectively understand and strategically manage risk

Standard definitions, rating scales, status indicators and processes that standardize issue management approaches and enable data aggregation

Roles & Responsibilities

Management OWN
Participates and provides feedback in the evaluation of deficiencies; helps determine the action plan and ensures it is fully executed.

Internal Audit ADVISE
Acts as a trusted advisor, providing recommendations for management action plans; tracks issues, action plans and remediation efforts.

External Audit ASSESS
Works with management once issues are identified and recommends action plans. At year-end, aggregates deficiencies to determine if they escalate to a Significant Deficiency or Material Weakness, each with specific disclosure requirements.

Leading Practices

- Evaluate every identified control deficiency based on likelihood and potential magnitude, considering relevant assertions, affected accounts/disclosures, compensating controls, aggregation with other deficiencies, and the possibility of material misstatement.
- Perform root-cause analysis, rather than correcting only the immediate exception, considering people, process, technology, data, governance, training, capacity, and control-design factors.
- Assign each remediation action a clear accountable owner, target milestone, escalation path, required evidence, and governance oversight, with heightened monitoring for significant deficiencies and potential material weaknesses.
- Require remediation to demonstrate both effective redesign and sufficient operating history; implementation of a new control alone should not automatically support closure.
- Independently retest remediation and update the broader ICFR environment, including RCMs, narratives, flowcharts, IPE inventories, application scope, testing plans, and related controls affected by the root cause.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Evaluation of Issues
Deficiency Types & Key Terms

TYPES OF CONTROL DEFICIENCIES increasing severity ▼

Control Deficiency
The design or operation of a control does not allow control owners to prevent or detect misstatements on a timely basis.

Significant Deficiency
A deficiency, or combination of deficiencies, less severe than a material weakness but important enough to be reported to leadership.

Material Weakness
A deficiency, or combination of deficiencies, with a reasonable possibility that a material misstatement will not be prevented or detected and corrected on a timely basis. Disclosed in the financial statements.

EVALUATING DEFICIENCIES individually and in aggregate

1. Is it a design or operating deficiency?
2. How often does it occur and how big is the impact? (severity)
3. Are there mitigating controls that lower the risk?

Issue Management - Key Terms

Finding Identified defect or non-conformance to standards, policy, guidelines, established process, best practices which may or may not rise to the level of an Issue or may be noted as Observations that do not require a formal Management Action to remediate.

Issue Condition, or set of conditions, which contributes to risk and requires management's attention. Occurs when a business area or supporting process is unable to mitigate risk to an acceptable level due to inadequate design, ineffective execution, or absence of an appropriate control. Have a negative impact on achieving business or strategic objectives and should be considered as part of an assessment of the control environment.

Observation Recommendation for improvement that is not required to achieve an acceptable level of control which do not require a formal Management Action and do not fit the criteria for an Issue.

Self-Identified Issue An Issue raised by the Issue Owner or within the Issue Owner's group/team.

Incident Unplanned event or chain of events, which causes a negative impact. They are caused by nature, human error, or certain technology failures and would not be considered Issues. It may result from an Incident if a formal remediation plan is needed to strengthen a control or mitigate risk.

Management Action The specific action to be taken to remediate an issue. Every Issue that will be remediated must have at least one Management Action to remediate the risk created by the Issue. An Issue may have more than one Management Action.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – AI in Issues & Remediation
Use Case Considerations

AI USE CASES

- **Draft issues & deficiency analysis**
  Draft issue write-ups and preliminary deficiency analysis, and structure root causes for auditor review.

- **Identify systemic issues earlier**
  Cluster deficiencies, exceptions, and audit findings to detect recurring themes across processes, systems, controls, and business units.

- **Strengthen root-cause analysis**
  Synthesize root causes by analyzing historical findings and related data to identify potential people, process, technology, data, or governance drivers.

- **Improve remediation monitoring**
  Track milestones, evidence, operating history, overdue actions, and indicators of potential repeat findings.

- **Route exceptions in real time**
  Route control breaks or unauthorized access attempts in real time to the appropriate business process owner for faster resolution.

GUARDRAIL **AI can support deficiency analysis, but management should determine deficiency severity, compensating-control effectiveness, remediation adequacy, and closure.**

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Reporting & Concluding
Management's Report on ICFR

Planning & Scoping | Process & Control Documentation | Walkthroughs & Test of Design | Test of Operating Effectiveness | Issues & Remediation | Reporting & Concluding

Annual SOX Requirement	At the conclusion of the annual SOX audit period, the company must provide a management report on Internal Controls over Financial Reporting (ICFR) containing four required items.

Four Required Items

Management's Responsibility STATEMENT
A statement of management's responsibility for establishing and maintaining adequate ICFR.

Evaluation Framework FRAMEWORK
A statement identifying the framework used by management to evaluate the effectiveness of ICFR.

Management's Assessment CONCLUDE
Management's assessment of ICFR effectiveness as of fiscal year-end, stating whether ICFR is effective and disclosing any material weakness identified by management.
Management is not permitted to conclude that their ICFR is effective if there are one or more material weaknesses in the company's ICFR.

Auditor Attestation ATTEST
For accelerated and large accelerated filers, a statement that the registered public accounting firm has issued an attestation report on ICFR.

Leading Practices

- Maintain a documented ICFR conclusion framework that brings together scope, design effectiveness, operating effectiveness, deficiencies, remediation status, compensating controls, and unresolved matters supporting management's conclusion.
- Use SOX sub-certifications and structured control-owner representations to surface process changes, control failures, fraud concerns, system changes, unresolved exceptions, and other matters relevant to Sections 302 and 404.
- Give the CFO, audit committee and external auditors real-time, risk-focused dashboards on a centralized platform, highlighting SDs/MWs, overdue remediation, failed or untested controls, repeat findings and high-risk areas well ahead of year-end, not just completion percentages.
- Coordinate proactively with the external auditor on significant judgments, control changes, MRCs, IPE, IT dependencies, SOC reports, deficiencies, remediation, and timing while preserving management's responsibility for its own ICFR assessment.

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – AI in Reporting
Use Case Considerations

AI USE CASES

- **Draft workpapers & reports**
  Draft workpaper narratives, issue write-ups, and executive summaries.

- **Turn reporting into insight**
  Generate risk-focused dashboards, trend analyses, management summaries, and audit committee reporting.

- **Surface concerns from certifications**
  Draft certification packs and analyze sub-certifications and control-owner responses for changes, exceptions, control failures, and unresolved risks requiring escalation.

- **Accelerate reporting & disclosure reviews**
  AI-assisted first-pass analysis highlights exceptions, inconsistencies, and areas requiring management or auditor attention.

- **Drive continuous improvement**
  Aggregate findings to surface themes for the CAE report, track remediation, monitor control signals, and refine processes over time.

GUARDRAIL **AI can synthesize evidence and highlight risks, but management remains responsible for evaluating deficiencies and concluding on ICFR effectiveness.**

© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Cross-Department Communications
Visibility & Ownership Across Teams

THE FORMULA

Clear communication
Shared understanding across teams

+

Defined ownership
Clear accountability for each control

=

Consistent SOX compliance
The outcome when both are in place

END-TO-END VISIBILITY

Teams need visibility into upstream and downstream processes

UPSTREAM
Processes and systems that feed into your team

→

YOUR TEAM
The risks and controls you own and perform

→

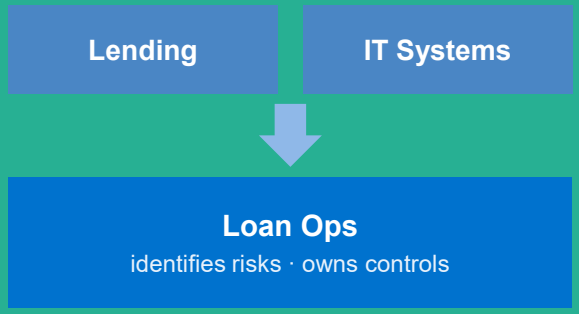
DOWNSTREAM
Processes that rely on your team's outputs

Understanding the handoffs helps each team identify risks and fulfill its control responsibilities.

EXAMPLE

Loan Operations

Loan Ops must understand Lending and related IT systems to identify risks and fulfill control responsibilities.



© 2026 Forvis Mazars, LLP. All rights reserved.

SOX – Common Control Deficiencies

- **Insufficient control precision**
  Controls, particularly management review controls, operate at too high a level, lack defined expectations or investigation thresholds, or do not demonstrate how a material error would be detected.

- **Inadequate control evidence**
  Documentation shows only “reviewed/approved” or a sign-off, without demonstrating procedures performed, reviewer challenge, exceptions identified, follow-up, and resolution.

- **IPE completeness and accuracy gaps**
  Reports, spreadsheets, model outputs, queries, or other information used in controls are relied upon without sufficient validation of source data, parameters, logic, interfaces, or relevant IT dependencies.

- **Weak support for estimates and significant judgments**
  Insufficient evidence of management’s review and challenge of assumptions supporting areas such as CECL/ACL, valuations, reserves, models, and other complex estimates.

- **Control design and coverage gaps**
  Key financial-reporting risks or assertions are not adequately addressed, controls are vaguely defined, or dependencies on ITGCs, automated controls, interfaces, and service organizations are incomplete.

- **Walkthrough and process-understanding deficiencies**
  Reliance on inquiry without sufficient inspection, observation, or reperformance. Process changes and new systems/IPE are not incorporated into the current-year control environment.

- **ITGC and third-party dependency issues**
  Weaknesses in access, change management, system dependencies, SOC 1/CUEC coverage, or compensating controls undermine reliance on automated and IT-dependent controls.

- **Deficiency evaluation and remediation weaknesses**
  Deficiencies are not appropriately aggregated or evaluated for severity, root causes are not addressed, or remediation is closed before sufficient operating history and retesting demonstrate effectiveness.

© 2026 Forvis Mazars, LLP. All rights reserved.

Contact

Forvis Mazars

Prashant Panavalli
Principal, Internal Audit for Financial Services Leader
201.957.2550
prashant.panavalli@us.forvismazars.com

Allison Tanju
National Financial Reporting Partner | Financial Services
404.575.8840
allison.tanju@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.