SOX Without Consuming The Audit Plan

SOX should enhance audit coverage and connected risk insights – not consume the entire audit function's capacity.

Adam Pajakowski
Partner
+1 (216) 623-7539

Justin Mahoney
Senior Manager
+1 (404) 442-1673

August 2026

Learning Objectives

1. Leveraging AI-enabled automation to streamline SOX testing, improve risk coverage, and reduce manual effort
2. Leveraging SOX insights, risk data, and controls to drive operational and strategic audit projects
3. Applying a connected risk approach to align SOX activities with broader enterprise risks
4. Rationalizing controls and testing to improve efficiency and maximize audit coverage
5. Avoiding “SOX-ification” by balancing compliance execution with value-driven assurance activities
6. Understanding benchmarking across the internal audit landscape on areas of focus and time spent in SOX

© 2026 Crowe LLP

Table Of Contents

© 2026 Crowe LLP

Crowe

Opening: The SOX Capacity Challenge

Balancing required compliance with the risks the business cannot afford to miss

The Core Tension

SOX is essential – but it should not become the audit plan.

SOX provides necessary discipline

- ICFR structure, accountability, & cadence
- Deficiency evaluation and remediation follow-up
- Control documentation and evidence standards
- External audit coordination and reliance potential

The audit mandate keeps expanding

- Cyber and technology risk
- Transformation and ERP programs
- Third-party and operational resilience
- Fraud, compliance, and regulatory risk
- AI, data governance, & model risk
- Strategic and emerging risks

Audit capacity is finite. Risk coverage cannot be static.

The goal is not less assurance. The goal is better assurance with more capacity for the risks that matter most.

© 2026 Crowe LLP

Crowe

Why This Matters to Internal Audit Leaders

Turning compliance effort into broader audit impact

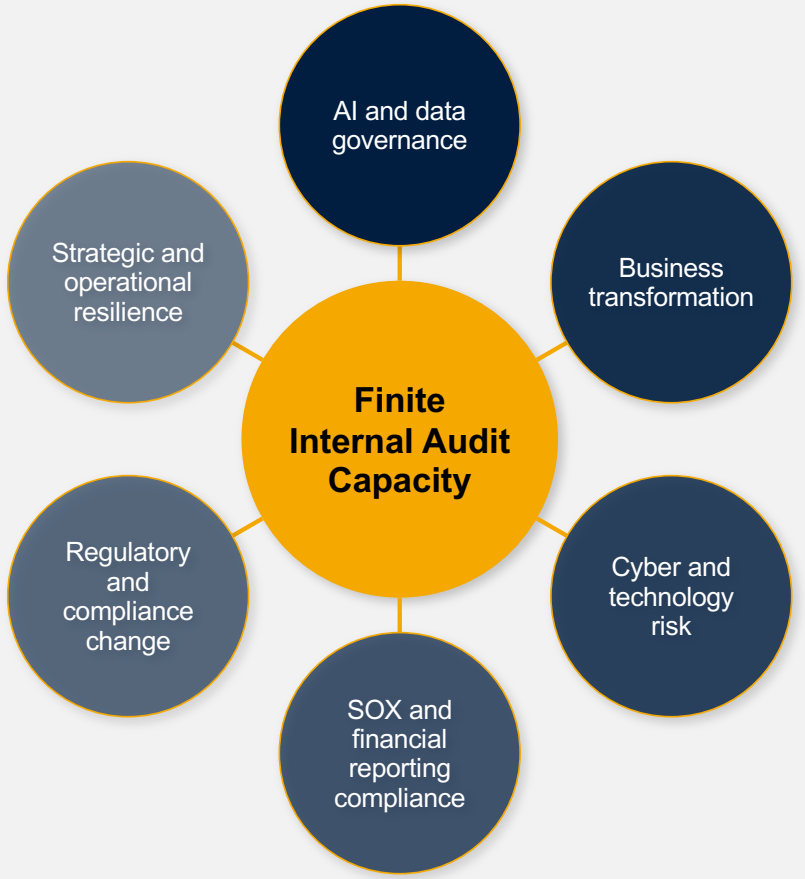
Why This Matters Now

The audit plan is under pressure from every direction.

Internal audit leaders are balancing a growing risk universe against limited capacity, higher expectations, and recurring compliance demands.

The challenge is not whether these risks matter.

The challenge is how internal audit creates capacity to cover them.



© 2026 Crowe LLP

Crowe

Benchmarking the Internal Audit Landscape

What audit-plan allocation reveals about SOX capacity trade-offs

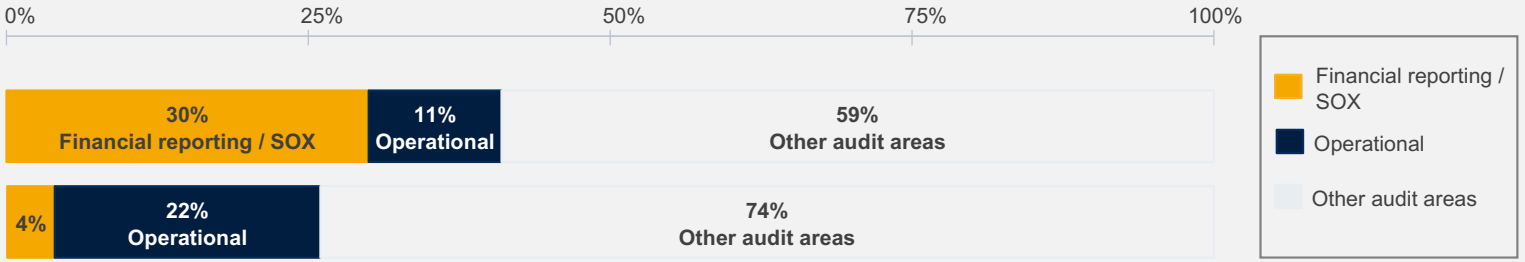
Benchmarking: Where Internal Audit Time Goes

The IIA 2026 Pulse Report highlights the SOX capacity trade-off.

SOX changes the shape of the audit plan

Audit plan allocation: SOX implemented vs. SOX not implemented

IIA 2026 Pulse • Exhibit 3.1



+26 pts	Financial reporting / SOX allocation where SOX is implemented
-11 pts	Operational audit allocation where SOX is implemented
Trade-off	SOX does not just add work – it changes audit plan shape.

Other audit areas include: Compliance/regulatory excluding SOX, cybersecurity, IT, non-ICFR financial areas, ERM, fraud, third-party relationships, external audit support, governance/culture, cost reduction, sustainability/non-financial reporting, and other risk categories.

Key Takeaway: Where SOX is implemented, financial reporting and SOX testing can take nearly one-third of the audit plan.

Source: The IIA / Internal Audit Foundation, 2026 North American Pulse of Internal Audit, Exhibit 3.1; Q26; n=371.

© 2026 Crowe LLP

What Benchmarking Tells Us

Use the IIA Pulse data to test whether SOX effort is aligned to risk, value, and audit capacity.

The question is not **"How much SOX is too much?"** It is **"What is SOX effort producing for the broader audit plan?"**

Benchmarking should trigger better questions

Ask	What It May Reveal
How much of the plan is tied to SOX / ICFR?	Whether recurring compliance is crowding out coverage of operational, technology, and emerging risks.
Are we testing the right controls?	Whether the control population has expanded beyond truly key risks and key assertions.
How manual is the testing model?	Where automation, analytics, evidence reuse, and reliance can create capacity.
How are SOX results used after testing?	Whether deficiencies and themes are informing operational and strategic audit projects.

Benchmark Signal

In SOX environments, financial reporting and SOX testing can take nearly one-third of the audit plan.

30% Financial reporting / SOX where SOX is implemented

11% Operational audit allocation where SOX is implemented

59% Remaining audit plan across other risk areas

Move the Benchmark Conversation From Effort to Maturity

Compliance burden
Manual • duplicate • static

→

Efficient SOX program
Rationalized • automated • relied upon

→

Connected risk intelligence
SOX insights inform the enterprise audit plan

Source: The IIA / Internal Audit Foundation, 2026 North American Pulse of Internal Audit, Exhibit 3.1.

© 2026 Crowe LLP

Crowe

Current State: Where SOX Consumes Capacity

Identifying the activities that turn required compliance into recurring capacity drain

Capacity Pressure

How SOX Consumes Audit Capacity

SOX overload is usually not one problem – it is the accumulation of repeatable friction.

Common Capacity Drains

Evidence Chasing

Recurring PBC requests, follow-ups, status meetings, and version control issues.

Manual Testing

Large sample sizes, manual re-performance, and spreadsheet-heavy documentation.

Duplicate Requests

Management, internal audit, and external audit request similar evidence at different times.

Control Creep

Controls accumulate over time without equivalent retirement or consolidation.

Deficiency Churn

Repeat issues, remediation tracking, and retesting consume capacity late in the cycle.

Low Insight Reuse

SOX outputs remain in compliance reporting instead of informing the broader audit plan.

Impact On The Audit Plan

Less capacity for operational, technology, fraud, transformation, third-party, and strategic risk coverage.

Typical Symptom

The audit plan becomes deadline-driven instead of risk-driven.

© 2026 Crowe LLP

Root Causes of SOX Overload

Many SOX programs carry legacy design choices that no longer align with current risk.

Root Cause	How It Shows Up	Capacity Impact
Static Risk Assessment	Controls stay in scope after systems, processes, or risk levels change	Testing effort remains high even where risk has moved
Control Population Growth	New controls are added, but old or duplicate controls are not retired	Control volume grows faster than audit capacity
Manual Evidence Model	Evidence requests, completeness checks, and testing are spreadsheet driven	Auditors spend time collecting and formatting, not analyzing
Limited Reliance Strategy	Management, IA, and external audit perform duplicative procedures	Testing is repeated instead of coordinated
Over-documentation Mindset	Workpapers prioritize volume of documentation over quality of conclusion	SOX rigor spills into every audit activity

SOX optimization starts by separating risk-based requirements from inherited habits.

© 2026 Crowe LLP

Crowe

Connected Risk: Using SOX Insights Beyond Compliance

Converting SOX results into signals for broader enterprise risk coverage

Connected Risk Approach

SOX data can be a hub for broader enterprise risk insight.

The same control signals that support ICFR can reveal operational, technology, fraud, transformation, and third-party risks.

© 2026 Crowe LLP

Using SOX Insights to Shape the Audit Plan

SOX findings should create audit leads – not just compliance reports.

SOX Insight / Trigger	Potential Audit Project	Value Question
Repeated user access exceptions	**Identity and access management review**	Could unauthorized access or segregation conflicts affect more than ICFR?
Manual journal entry control issues	**Close process and journal entry analytics**	Are error or fraud indicators present across the close process?
Recurring reconciliation deficiencies	**Data quality / process automation audit**	Are upstream data issues creating operational inefficiency or reporting risk?
Change management ITGC gaps	**ERP transformation governance review**	Are technology changes outpacing control design and monitoring?
Revenue control exceptions	**Order-to-cash / revenue leakage review**	Are control failures signaling broader process leakage or customer experience issues?
SOC report delays or user control gaps	**Third-party risk and resilience audit**	Are outsourced processes creating unmanaged dependencies?

Planning implication SOX themes should feed the annual and dynamic risk assessment.

SOX output becomes a risk signal when it changes where internal audit looks next.

© 2026 Crowe LLP

Crowe

AI-Enabled Automation in SOX

Using automation to reduce manual effort and increase testing precision

Crowe

Automation

AI-Enabled Automation Across the SOX Lifecycle

AI can reduce friction across planning, evidence, testing, evaluation, and reporting.

1 Plan and Scope
- Risk Refresh
- Control Mapping
- Scoping Support

2 Request Evidence
- PBC Drafting
- Owner Routing
- Completeness Checks

3 Test Controls
- Population Analysis
- Attribute Extraction
- Exception Identification

4 Evaluate Results
- Exception Clustering
- Deficiency Themes
- Root-cause Support

5 Report and Monitor
- Status Summaries
- Narrative Updates
- Remediation Tracking

Where AI-enabled Automation Can Help

Convert Unstructured Evidence into Structured Testing Inputs
Invoices, approvals, tickets, reconciliations, SOC reports, policy documents

Compare Current-year Documentation to Prior-year Narratives
Identify changes, inconsistencies, obsolete process descriptions, and missing control attributes

Draft Status and Exception Reporting
Summarize testing progress, open items, deficiencies, and remediation themes

Automation Guardrail AI should accelerate evidence handling and analysis, while auditors retain judgment over risk assessment, control design, exceptions, and conclusions.

© 2026 Crowe LLP

Where AI Helps Most

Prioritize use cases with repeatable procedures, large evidence volume, and clear human review points.

High-value AI Use Cases

Evidence Intake and Indexing
Classify evidence, extract dates/owners, flag missing documents.

Population Validation Support
Compare system reports, identify duplicates, gaps, and outliers.

Narrative and Control Change Detection
Compare prior/current narratives and highlight changes for review.

Exception Triage
Group exceptions by type, root cause, process, owner, or control.

Deficiency Theme Analysis
Identify recurring patterns across processes, systems, or locations.

Reporting Drafts
Create first-pass status summaries, issue descriptions, and remediation updates.

Prioritization Filter
- High manual effort
- Repeatable testing logic
- Reliable source data
- Clear exception rules
- Human review and approval

Start with pilots where the risk of error can be controlled and the effort reduction is visible.

Keep Human Judgment Central — AI can support testing, documentation, and analysis — but auditors still evaluate control design, operating effectiveness, materiality, deficiency severity, and assurance conclusions.

Best First Move: target manual evidence work that is repetitive, rule-based, and already quality-reviewed.

© 2026 Crowe LLP

VIDEO

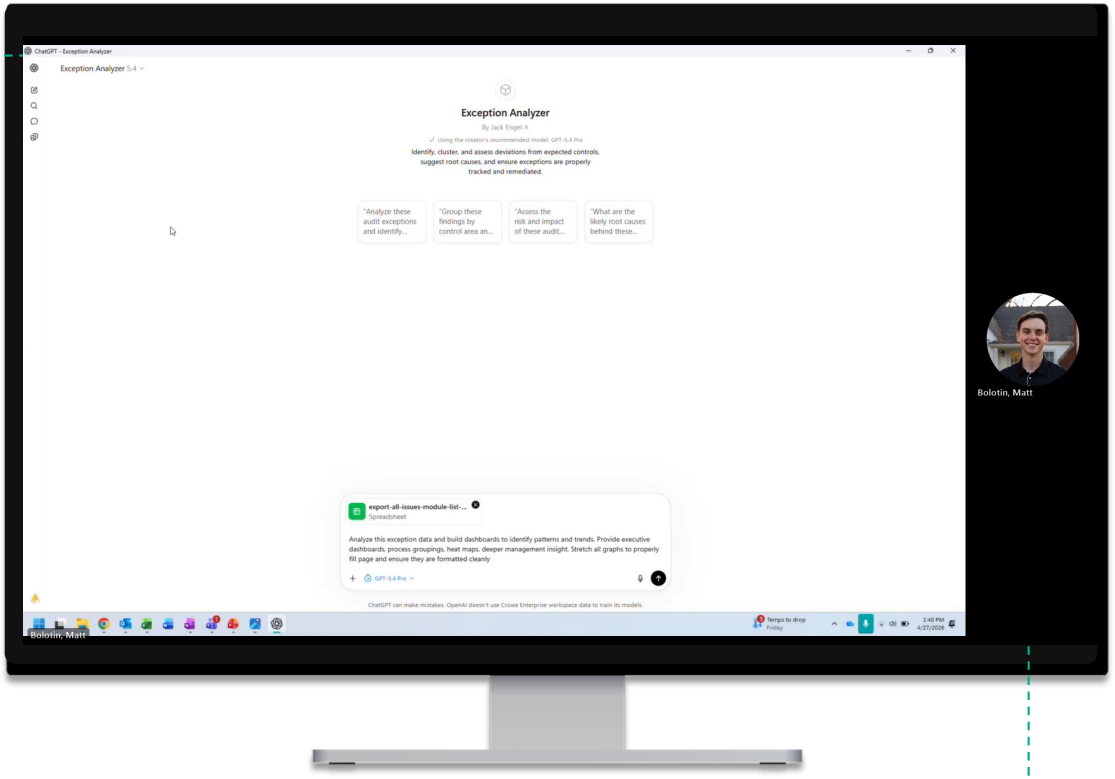
AI Exception Analyzer

Purpose:
The Exception Analyzer helps leadership understand where risk is concentrated and what actions will most effectively reduce exposure.

Inputs:
The GPT intakes exported controls deficiencies and recommendations via Optro.

Outputs:
The result delivers structured insights on trends, hotspots, recurrence, and aging. As well as highlights what the data means, assesses risk impact, and provides targeted actions to address root causes and reduce chronic issues.

Next Steps / Improvements:
Molding the GPT to perform cross-systems.



© 2026 Crowe LLP

VIDEO

AI Narrative Generator

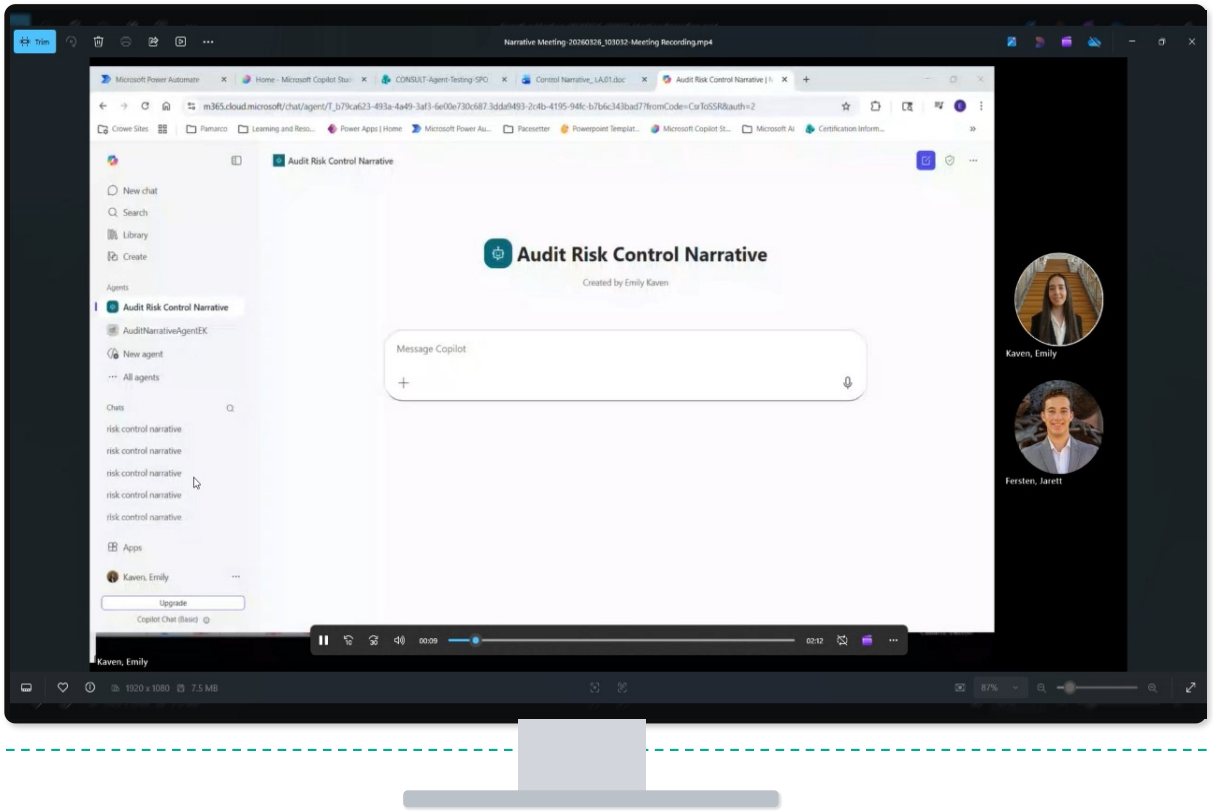
From RCM + transcript to a SharePoint-ready narrative.

Demo flow

1. **Trigger agent**
   Use a keyword such as “Risk Control Narrative”.
2. **Upload inputs**
   Add the RCM and walkthrough transcript.
3. **Generate narrative**
   Click Generate Narrative.
4. **Confirm files**
   Verify the correct files are attached.
5. **Save and review**
   Pick the SharePoint folder, then review the file.

Output: Narratives saved to SharePoint

Audit Risk Control Narrative agent walkthrough



© 2026 Crowe LLP

Rationalizing Controls and Testing

Reducing control burden while preserving assurance quality

Control Rationalization: Doing Less, Better

Focus on key risks and key controls — not control volume.

Rationalization Funnel

Full Control Universe
All documented controls across in-scope processes

Risk-aligned Controls
Controls mapped to financial reporting risks and key assertions

Key Controls
Controls that directly address material risks

Efficient Test Plan
Right-sized testing, evidence reuse, and automation

Practical Rationalization Moves

1. **Map Controls to Risks and Assertions**
   Confirm each key control addresses a material risk or assertion.
2. **Remove Duplicates and Low-precision Controls**
   Retire activities that do not materially improve the assurance conclusion.
3. **Shift to Automated and Preventive Controls**
   Favor controls designed into systems and workflow.
4. **Align Testing with Risk and Change**
   Vary timing, frequency, and approach based on risk and stability.
5. **Document the Rationale**
   Create a defensible basis for scope changes and external audit alignment.

Rationalization is not about weakening control coverage. It is about concentrating effort where control assurance matters most.

© 2026 Crowe LLP

Rationalize

Testing Efficiency Levers

Efficiency comes from changing the testing model – not simply asking auditors to work faster.

Risk-based Frequency
Adjust interim, year-end, rotational, or walkthrough depth based on risk and change.

Evidence Reuse
Use common evidence libraries and coordinated requests across management, IA, and external audit.

Automated Controls
Increase reliance on system-enforced controls, configurable workflows, and preventative logic.

Population Analytics
Validate completeness and identify exceptions through data, not manual sampling alone.

Centralized PBC Model
Standardize requests, owners, deadlines, and evidence quality expectations.

Reliance Strategy
Coordinate testing approach and documentation expectations with external audit early.

Control Owner Enablement
Provide templates, examples, and self-service dashboards to reduce rework.

Deficiency Triage
Use root-cause patterns to prioritize remediation and retesting effort.

Design Principle Reduce manual effort where controls are stable and data is reliable; increase precision where risk is higher or change is occurring.

Efficiency should improve both speed and quality: less chase, more analysis, clearer conclusions.

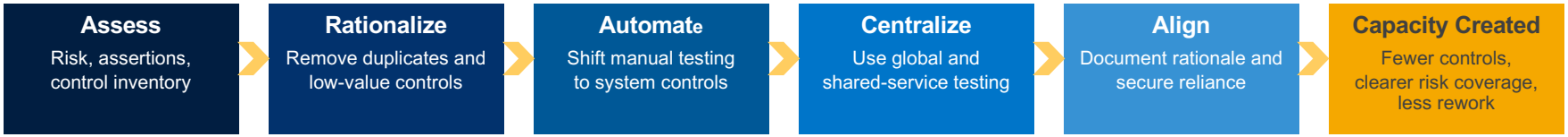
© 2026 Crowe LLP

Rationalize

Control Rationalization in Practice

How we reduce effort without reducing assurance.

Optimization Pathway



What This Looks Like in Practice

Decrease Key Control Count
Retain controls that directly address material risks; retire redundant or low-precision activities.

Manual → Automated Controls
Move from recurring sample-based reviews to configurable ERP/workflow controls where feasible.

Location-based → Global Controls
Replace inconsistent local controls with standardized global or process-level controls.

Local Testing → Shared-service Testing
Centralize evidence, testing protocols, and IPE standards for shared-service processes.

Downstream Testing → Upstream Reliance
Use upstream controls and preventive validations to reduce repetitive downstream checks.

External Audit Alignment
Agree early on scope changes, rationale, evidence standards, and reliance expectations.

Rationalization is not a control purge. It is a risk-based redesign of the control set and testing model.

© 2026 Crowe LLP

Example

Business Case: SOX Optimization in Action

Global pharmaceutical company, approximately $1B annual revenue – anonymized example.

Client Need: Outsource SOX execution while optimizing the control matrix as the company transitioned from pre-revenue to revenue-based operations.

1 What Crowe Changed

- Reviewed key control matrix for right-sizing opportunities
- Combined controls where risk coverage overlapped
- Relied on upstream controls instead of repetitive downstream activities
- Supported design of revenue and inventory controls

2 Examples Applied

- Decreased key business-process control count
- Moved manual reviews toward automated or system-enabled controls
- Created global controls in place of duplicative location controls
- Used shared-service center testing and standardized evidence

3 Capacity / Risk Assessment

- Reduced unnecessary testing and documentation burden
- Improved consistency across business units and locations
- Created a more proactive external audit relationship
- Right-sized the control matrix to company size and growth path

© 2026 Crowe LLP

Crowe

Avoiding “SOX-ification”

Keeping SOX discipline without turning every audit into a compliance exercise

Balance

Avoiding “SOX-ification”

Keep SOX discipline — but do not apply a SOX-heavy execution model to every audit.

SOX-ification: The tendency to make every audit look like SOX – heavy documentation, control-by-control testing, static scope, and compliance-first reporting even when the audit objective requires a different approach.

What To Keep From SOX

- Clear objectives and scope
- Evidence-based conclusions
- Consistent issue evaluation
- Accountability for remediation
- Quality control over workpapers

What To Avoid Outside SOX

- Testing every activity like a key control
- Over-documenting low-risk observations
- Treating all audits as compliance audits
- Using static programs when risk is changing
- Reporting only exceptions, not insights

Right-sized rigor: match the audit approach to the objective, risk, pace of change, and stakeholder need.

The broader audit plan should be disciplined, but it also needs to be agile, risk-informed, and business-relevant.

© 2026 Crowe LLP

Crowe

Roadmap: From Compliance Burden to Assurance Advantage

A practical path to rebalance, rationalize, automate, and connect SOX

Operating Model Considerations

Sustainable SOX optimization requires governance, data, technology, reliance, talent, and metrics.

1 Governance and Accountability

Clear ownership for SOX scope, control changes, remediation, and external audit alignment.

2 Data and Technology

Reliable system reports, evidence repositories, workflow, analytics, and automation controls.

3 Methodology

Risk-based scoping, rationalization criteria, documentation standards, and testing playbooks.

4 Reliance and Coordination

Early alignment among management, internal audit, and external audit to reduce duplication.

5 Talent and Delivery Model

SOX, IT, data analytics, automation, and business process skills deployed intentionally.

6 Metrics and Reporting

Track effort, cycle time, control volume, automation rate, reliance, deficiencies, and audit plan coverage.

Metrics That Tell the Capacity Story

- % Audit Plan Hours in SOX
- Control Count and Key Control Ratio
- Testing Cycle Time
- Automated Evidence Rate
- External Audit Reliance
- Audit Plan Coverage Shift

A better SOX operating model should make capacity visible and manageable.

© 2026 Crowe LLP

Roadmap: Rebalance, Rationalize, Automate, Connect

A phased path from compliance burden to assurance advantage.

1 Diagnose
0–60 days

- Benchmark SOX effort
- Map controls to risks
- Identify friction points

2 Rationalize
60–120 days

- Retire duplicates
- Refine key controls
- Align with external audit

3 Automate
3–6 months

- Pilot evidence automation
- Use data for populations
- Standardize reporting

4 Connect
6–12 months

- Feed SOX themes into risk assessment
- Launch SOX-informed audits
- Track capacity shift

Quick wins Start with high-volume, low-judgment evidence and controls with obvious duplication.

Sustain Measure capacity released and redirect it to risk areas underrepresented in the audit plan.

Optimization is complete only when the audit plan changes — not merely when SOX testing gets faster.

© 2026 Crowe LLP

Key Takeaways

Three actions to protect audit capacity and expand risk coverage

Key Takeaways / Q&A

SOX should be efficient, insight-rich, and connected to broader enterprise risk.

1 Streamline SOX Without Weakening Assurance

Rationalize controls, reduce duplication, align reliance, and focus testing where risk is highest.

2 Turn SOX Outputs Into Risk Intelligence

Use exceptions, deficiencies, process data, and control themes to inform operational and strategic audits.

3 Protect Audit Capacity for the Risks That Matter

Avoid SOX-ification and rebalance the audit plan toward cyber, technology, transformation, fraud, third parties, AI, and emerging risks.

Discussion Prompts

Where is SOX consuming the most capacity today?
Which SOX insights are not being used in audit planning?
What rationalization or automation lever is most feasible next quarter?

© 2026 Crowe LLP

Crowe

Thank You

Adam Pajakowski

Internal Audit – Partner

Adam.Pajakowski@crowe.com

Justin Mahoney

Internal Audit – Senior Manager

Justin.Mahoney@crowe.com

DISCLAIMER

This proposal is for informational and discussion purposes only and does not constitute a binding offer or commitment by Crowe LLP. All projections, estimates, and timelines are based on current assumptions and subject to change without notice.

The content herein is general in nature and not intended as audit, tax, accounting, legal, or other professional advice and should not be relied upon as such. You should consult a qualified adviser before making decisions based on this information. Some services may be unavailable to attest clients.

“Crowe” is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. “Crowe” may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. [illegible] of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

“Crowe” refers to the global network of independent firms operating under the Crowe brand. Each firm is a separate legal entity and not responsible for the acts of others. Crowe LLP is the U.S. member firm of Crowe Global, an entity that does not provide services to clients. For more details, visit www.crowe.com/disclosure. © 2026 Crowe LLP

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. © 2024 Crowe LLP.