SOC & Audit: Using Third-Party Assurance Together

July 2026

forvis mazars

SOC & Audit: Using Third-Party Assurance Together

Meet the Presenters

Karen Cardillo
Managing Director, SOC & HITRUST

336.259.6611
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal, SOC & HITRUST

828.989.3176
ryan.boggs@us.forvismazars.com

Today’s Focus

1 Identify

Recognize the inefficiencies. Identify the inefficiencies that arise when SOC reporting and the financial statement audit are managed separately by different firms.

2 Weigh

Consider the benefits. Weigh the operational and cost benefits of coordinating assurance activities under a unified approach.

3 Recognize

Address blind spots. Recognize common blind spots in third-party assurance programs and apply practical frameworks for addressing them.

forvis mazars

Agenda

1. **Setting the stage**: The modern assurance environment and executive pressures driving change
2. **Understanding the problem**: How financial audits and SOC examinations intersect and duplicate work
3. **Why fragmented assurance creates inefficiencies**: Operational, cost, and governance consequences
4. **The power of an integrated approach**: What changes when one provider performs both engagements
5. **Practical frameworks and leading practices**: Implementation roadmap, maturity model, and executive action checklist

forvis mazars

Setting the Stage

Today’s Assurance Environment

The volume and complexity of assurance demands facing organizations and their audit committees have grown substantially.

- Service organizations routinely carry multiple concurrent assurance obligations: financial statement audits, SOC 1 examinations, SOC 2 examinations, regulatory examinations, and internal audit reviews
- Customers, regulators, and rating agencies increasingly treat SOC reports as baseline procurement and contracting requirements — not optional differentiators
- IT environments have expanded through cloud adoption, third-party dependencies, and hybrid infrastructure, broadening the scope of every assurance engagement
- The result: more evidence requests, more auditor relationships, more coordination burden — often without proportional increases in assurance quality

The organizations that manage assurance most efficiently are those with the most deliberate coordination model.

forvis mazars

Rising Assurance Demands

Customers & Prospects

Require current SOC 2 Type 2 as baseline procurement; some require SOC 1 for financial reliance. Requests arrive year-round with tight turnaround, and supplemental questionnaires follow when reports are late.

Auditors & Committees

User-entity auditors rely on SOC 1 Type 2 and CUEC evaluation to reduce substantive testing; audit committees expect consolidated reporting consistent with internal audit findings.

Regulators & Examiners

Financial regulators, banking supervisors, and data-protection authorities reference SOC Reports as evidence of control adequacy and expect active CUEC compliance and exception remediation.

Investors & Boards

Investors and lenders depend on assurance status to support reliance; boards and executive leadership expect real-time visibility into assurance posture, not year-end summaries.

forvis mazars

The Executive Burden of Fragmented Assurance

Key Friction Points

When separate providers manage separate engagements without coordination, the administrative and operational burden falls disproportionately on internal teams, and executives are beginning to question it.

- Managing multiple audit-firm relationships with separate scheduling, scoping, and logistics
- Responding to overlapping evidence requests covering the same control populations at different times
- Explaining the same control narratives and exception histories to different audit teams
- Reconciling inconsistent conclusions when two firms evaluate the same control differently

Executives are asking: “Why give the same evidence to two firms in one month?” “Two auditors judged one control differently—which is right?” “Our SOC period ends in October, fiscal year in December—who owns the gap?”

Real-world example: A mid-sized payments processor found its access-control team spending 150+ hours a year on audit requests, most of those duplicates from separate providers.

forvis mazars

Setting the Stage
Summary

Key Takeaways

1 **Obligation**

Service organizations now operate under a multi-stakeholder assurance obligation that cannot be efficiently managed as a collection of independent, uncoordinated engagements.

2 **Duplication**

The same underlying control environment is evaluated repeatedly by different providers, creating duplicative work that adds cost without adding assurance value.

3 **Fragmentation**

Executives are asking the right questions; the frameworks to answer them exist and will be presented later in this presentation.

forvis mazars

Understanding the Problem

Financial Statement Audits
What They Are & What They Require

Overview

A financial statement audit is a rigorous, standards-based examination of an organization's financial controls and reporting, requiring substantial evidence from IT and operational teams.

Purpose: Provide independent assurance that financial statements are free from material misstatement, whether due to error or fraud.

Standards: Conducted under AICPA auditing standards (or PCAOB for public companies); governed by GAAS and GAAP.

Scope: Entity-level controls, IT general controls (ITGCs), application controls, process-level controls, and automated controls within financially relevant systems.

Key evidence demands:

- User access listings
- Change management records
- Interface reconciliations
- Exception monitoring logs
- IPE (system-generated reports)

Timing: Fieldwork typically spans 3–6 months; year-end procedures concentrated in Q4 and Q1.

Real-world example: For a technology company with a December 31 fiscal year-end, the financial auditor will request user access listings, change management ticket populations, and ITGC evidence beginning as early as September—coinciding directly with SOC Examination fieldwork for many service organizations.

forvis mazars

SOC Examinations
What They Are & What They Require

SOC 1

Focus: Controls relevant to user entities' internal control over financial reporting (ICFR). Used when the service organization's systems process or affect the user entity's financial statements.

Report types: Type I — Design; Type 2 — Operating effectiveness

Primary audience: User entities, their financial auditors, and regulators evaluating ICFR reliance

SOC 2

Focus: Controls against the AICPA Trust Services Criteria — Security, Availability, Processing Integrity, Confidentiality, and Privacy. Security is required; others are optional.

Report types: Type I — Design; Type 2 — Operating effectiveness

Primary audience: Customer procurement teams, information security leaders, regulators, and prospective clients

SOC 3

Focus: A summary report of SOC 2 conclusions designed for broad, public distribution, without detailed control descriptions or auditor testing results.

Report types: Single report type

Primary audience: Public audiences — website visitors, general market stakeholders, and prospects who do not require detailed control-level evidence

Examination period: Typically 9–12 months; examination end date often precedes the fiscal year-end, creating a gap period requiring bridge letters or roll forward procedures.

forvis mazars

Multiple Stakeholders, Overlapping Objectives

Financial Statement Audit

- External investors and lenders
- Financial regulators
- Audit committees
- Board of directors
- Management (internal control reporting)

Shared evidence: ITGCs, Application Controls, IPE Validation, Vendor/ Subservice Assurance, Change Management; same systems, same people, same processes.

SOC Examination

- User entity external auditors
- User entity management
- Customer procurement and security teams
- Regulators of user entities
- Prospective customers

Executive insight: When stakeholders are different but evidence sources are shared, the organization bears the coordination burden. The question is whether that burden is designed to be efficient or accumulated over time.

forvis mazars

Where the Two Engagements Can Overlap

Financial Audit Only

Unique to financial audit:

- Substantive financial testing
- Transaction sampling
- Financial statement assertions
- Disclosure controls

Shared Overlap

- **ITGCs**: User access management, change management, logical access configurations, privileged access controls
- **Application controls**: Automated reconciliations, interface controls, system-calculated totals
- **IPE**: Reports, data extracts, dashboards used to operate or evidence controls
- **Vendor/subservice assurance**: SOC reports from third-party providers relevant to both engagements
- **Change management**: Records of system changes affecting financially relevant and security-relevant controls

SOC Examination Only

Unique to SOC:

- Trust Services Criteria (Availability, Confidentiality, Privacy where not financially relevant)
- System description
- Subservice organization disclosures

Key insight: The same risks — access, change, data integrity, third-party reliance, and monitoring — are evaluated twice, drawing on the same systems, people, and processes.

forvis mazars

What Two Separate Providers Request

Financial Auditor

- **User Access**: Active, privileged, and service accounts in financially relevant systems
- **Change Mgmt**.: Ticket populations for the audit period; authorization, testing, and approval evidence
- **IPE & Reports**: Report logic, query parameters, source reconciliation for financial assertion purposes
- **Vendor & Walkthroughs**: Vendor SOC Reports, bridge letters for gap periods, CUEC evidence; ITGC walkthrough

SOC Examiner

- **User Access**: Dormant accounts, temporary admin – in-scope systems per SOC criteria
- **Change Mgmt**.: Ticket populations for the examination period; production change prevention controls
- **IPE & Reports**: Same reports, potentially different parameters; accuracy & completeness focus
- **Vendor & Walkthroughs**: Subservice SOC Reports, carve-out analysis; walkthrough of all in-scope control domains

Management Response

- **User Access**: Two separate reports with different filters; scope mismatch requires reconciliation
- **Change Mgmt**.: Same population re-pulled with different date ranges; version conflicts emerge
- **IPE & Reports**: Multiple IPE versions generated; IT staff re-validates the same source data twice
- **Vendor & Walkthroughs**: Same process owners explain identical controls in separate interviews—months apart

What to Watch: The requests differ, but the sources are identical; the same walkthrough, sample, and IPE get tested 2–3 times over.

Illustrative: A cloud ERP access review runs 8–12 hrs. separately vs. 3–4 hrs. coordinated.

forvis mazars

The Burden on Internal Teams

Burden Intensity by Function & Engagement Type

The cumulative impact of fragmented assurance falls hardest on the internal teams who must respond—the teams simultaneously responsible for running the business.

- **IT & Security – Highest burden**: Primary responders for ITGC evidence, access reviews, change management, and IPE. Often respond to 3–4 separate audit requests per year for the same controls.
- **Control owners across functions**: Absorb walkthrough interviews, evidence preparation, and follow-up responses across multiple audit cycles, without a shared calendar or evidence library.
- **Real-world example**: A mid-market SaaS company estimated its IT team spent over 200 hours annually supporting audit activities across two assurance providers, internal audit, and one regulatory examination. Less than 40% of that effort was considered non-duplicative.

Visible Costs

- Professional service fees for multiple audit providers
- Dedicated audit liaison staff time
- Audit committee and board reporting preparation
- Repeated procurement and contracting cycles

Hidden Costs

- Control owner hours on duplicate evidence requests
- IT time regenerating the same reports in different formats
- Management time in repeated walkthrough interviews
- Escalations when providers reach inconsistent conclusions
- Delayed financial close from unresolved audit questions

forvis mazars

Understanding the Problem
Summary

Key Takeaways

1 **Isolation**

The two engagements are not as separate as they appear. The same ITGCs, IPE, and vendor assurance information are required by both; but, requested independently, prepared redundantly, and reviewed in isolation.

2 **Burden**

The burden is distributed and often invisible: IT teams, control owners, finance staff, and compliance functions absorb the duplicate work as overhead.

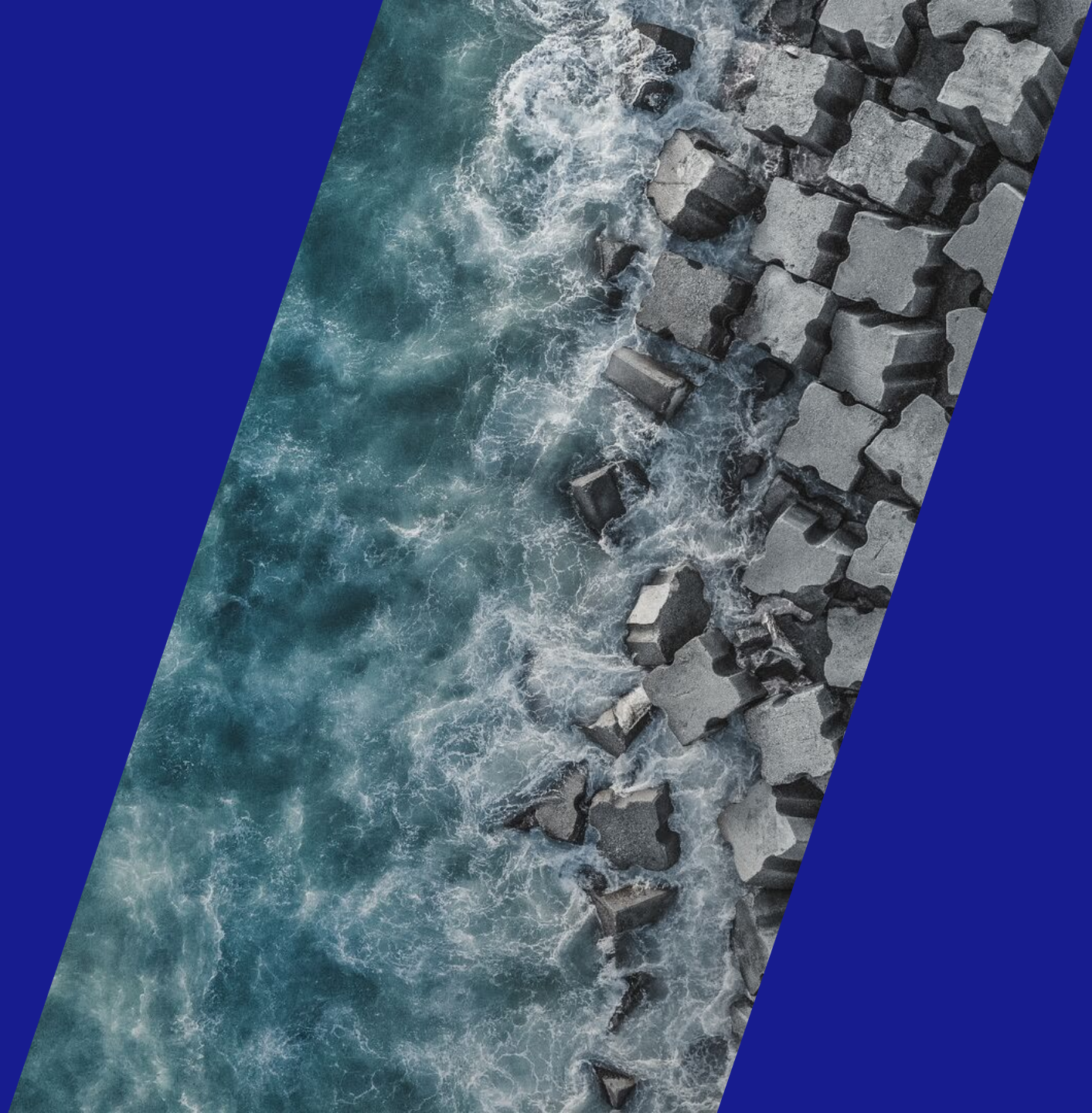
3 **Hidden Costs**

The hidden costs—in time, escalation, and rework—typically equal or exceed the visible professional service fees paid to external audit providers.

Next: We'll examine the specific operational, governance, and strategic inefficiencies created by a fragmented model and begin to build the case for integration.

forvis mazars

Why Fragmented Assurance Creates Inefficiencies



The Timing Problem

Engagement Timeline

When SOC Examination fieldwork and financial audit procedures run on separate schedules, management faces overlapping demands that compete for the same internal resources at highly inopportune times.

- **SOC Type 2 Examination Period**: Jan–Dec (full year)
- **Financial Audit – Interim Procedures**: Q3 Interim (Jul–Sep)
- **Financial Audit – Year-End Procedures**: Q4–Q1 Year-End
- **Overlap Zone**: Peak Demand Q3–Q4
- **Bridge Period Gap**: 60–90 Day Gap (Oct–Nov)

Consequence: IT teams and control owners respond to evidence requests from two providers simultaneously during a typically high-pressure operational period—Q3 and Q4.

What to Watch: Bridge letter requests arrive in Q4, when year-end activities are often competing for attention. They require vendor cooperation, management review, and auditor sign-off and sometimes are treated as administrative afterthoughts.

forvis mazars

The Evidence Treadmill
Collecting the Same Data Repeatedly

Cycles + a Root Cause & Example

1 SOC Examination (Q1/Q2)

- IT generates user access listing, change management population, IPE validation package for SOC examiner
- Stored in SOC workpaper repository

2 Financial Audit Interim (Q3)

- Financial auditor requests user access listing; IT re-runs report with different parameters
- New population generated and stored in financial audit evidence folder

3 Financial Audit Year-End (Q4/Q1)

- Financial auditor requests year-end population; IT runs report again
- Version discrepancies from Q1 and Q3 discovered; reconciliation required

Root cause: Absence of a canonical evidence design forces re-creation at each request point

Example: A technology services company generated 14 separate versions of its privileged access listing over 18 months—all based on the same underlying data

forvis mazars

When Two Providers Reach Different Conclusions

Why it occurs: Different risk thresholds, sampling, timing, and definitions of “operating effectively,” not flawed controls

SOC Examiner Conclusion

- **Finding**: Control is operating effectively. One exception noted; root cause addressed; no modification to opinion
- **Action**: Exception documented; remediation evidence accepted; period closed without qualification

Financial Auditor Conclusion

- **Finding**: Control requires incremental testing; requests additional remediation evidence; extends scope to prior-period changes
- **Action**: Expanded sample selection; additional management testing required; timeline extended pending resolution

What to watch: Inconsistent conclusions signal an uncoordinated assurance framework; audit committees may lose confidence in both.

forvis mazars

The Full Cost of Fragmented Assurance
Costs & Consequences

Direct Costs

- Professional fees for two separate audit providers is often higher in aggregate than a single integrated provider
- Additional engagement management overhead may include multiple contracts, separate billing, separate status reporting

Internal Labor Costs

- Control owner hours for duplicate evidence preparation (~50–200+ hours annually)
- IT time for repeated report generation and IPE validation; management time for walkthrough interviews

Escalation & Remediation Costs

- Reconciling inconsistent conclusions; late-year bridge letter and gap period management
- Remediation rework when duplicate findings are raised independently
- **Example**: For every $1 of external audit fee, $0.50–$1.50 in internal labor is incurred—disproportionately higher under a fragmented model
- **Illustrative cost composition (fragmented vs. integrated)**: Direct Fees 100 vs. 80; Internal Labor 130 vs. 70; Escalation & Remediation 50 vs. 15; Strategic Opportunity Cost 60 vs. 20

Executive impact: Delayed financial close, IT fatigue and deferred control improvements, customer-facing SOC Report gaps, and divergent conclusions requiring board-level explanation.

forvis mazars

Assurance Fatigue
An Illustrative Scenario

Quarterly Demand Cycle

Assurance fatigue is a measurable deterioration in evidence quality, stakeholder responsiveness, and audit outcomes from sustained, uncoordinated audit demand.

Illustrative example: SaaS Co. | Dec. 31 fiscal year | SOC 2 Type 2 Oct–Sep | annual financial audit

- **Q1 (Jan–Mar)**: SOC Readiness begins; IT supports prior-year SOC evidence; financial audit close ongoing
- **Q2 (Apr–Jun)**: SOC fieldwork begins; access review walkthroughs and change management evidence
- **Q3 (Jul–Sep)**: SOC fieldwork peak and financial audit interim—dual demand, highest concurrent period
- **Q4 (Oct–Dec)**: SOC closes; bridge letters; financial audit year-end accelerates; IT at maximum capacity
- **Q1+ (Next Year)**: Audit completes; SOC Readiness restarts; no meaningful recovery period
- **Result**: Continuous audit support mode; evidence quality degrades; response times lengthen; auditors expand procedures
- **What to watch**: Assurance fatigue is self-reinforcing, but structural coordination can help

forvis mazars

Why Fragmented Assurance Creates Inefficiencies
Summary

The Self-Defeating Cycle & What's Next

1 **Inefficiency**

- Operational inefficiencies, like duplicate requests, repeated walkthroughs, parallel evidence cycles, misaligned timing, are predictable consequences of the separate provider model, not random events

2 **Inconsistency**

- Inconsistent conclusions, escalation costs, and strategic opportunity costs multiply the impact beyond what any single line item captures

3 **Fatigue**

- Assurance fatigue is a structural outcome of uncoordinated demand, degrading evidence quality, stakeholder responsiveness, and audit outcomes over time

The cycle: Poor coordination increases burden → reduces improvement capacity → perpetuates findings → repeat

Next: The Power of an Integrated Approach

forvis mazars

The Power of an Integrated Approach

What Changes With an Integrated Model

Separate Provider Model

- Two firms, two engagement teams, two scoping processes, two evidence request cycles
- No shared knowledge of the control environment before fieldwork begins
- Parallel walkthroughs, independent IPE validation, separate vendor assurance conclusions
- Inconsistency risk whenever the same control is evaluated through different lenses

Integrated Provider Model

- One firm, one unified engagement team, one coordinated scoping and planning process
- Shared understanding of the control environment built through a unified risk assessment
- Single walkthrough series serving both engagements; evidence designed once for dual use
- Consistent conclusions anchored in a unified view of control design and effectiveness
- **Independence maintained**: Professional standards permit coordinated execution by a single qualified firm; teams remain separate where required

forvis mazars

Five Guiding Principles of Integrated Assurance

Integrated Assurance Model

Five principles balance operational efficiency with professional integrity. Coordination does not compromise independence or assurance quality.

1. **Coordinate inputs, not opinions.** Evidence, timelines, and walkthroughs are coordinated; each team forms its own conclusions.
2. **Design evidence once.** Canonical packages satisfy both engagements; evidence not duplicated, not merged; each provider evaluates independently.
3. **Build a unified risk assessment.** Shared understanding focuses resources on highest-risk areas rather than evaluating low-risk areas twice.
4. **Provide consistent communication.** One coordinated calendar: one set of status meetings, one open items log, one escalation path.
5. **Maintain professional standards.** Independence, skepticism, and quality standards rigorously maintained. Coordination is not consolidation of opinion.

forvis mazars

Planning, Assessment, Evidence, & Testing

Integrated Planning: One Calendar

- Single kickoff and unified evidence request list across both scopes
- Canonical evidence definitions: scope, parameters, owner, retention
- Coordinated fieldwork calendar precludes timeline collisions
- Walkthroughs and IPE validation performed once, shared by both teams

One Risk Assessment, Two Engagements

- Financial audit focuses ITGCs and IPE on financially relevant systems
- SOC Examination scopes systems by Trust Services Criteria; covers subservice controls and CUECs
- Joint review targets high-risk areas; low-risk areas not evaluated twice

Leading practice: Shared understanding, not shared working papers or merged conclusions

Evidence Reuse: Designed In

- **Fully reusable**: Access listings, change tickets, IPE packages, vendor SOC reports
- **Partially reusable**: Shared populations; samples differ by scope or materiality lens
- **Engagement-specific**: Financial substantive procedures, planned in advance

Design once; each team evaluates independently.

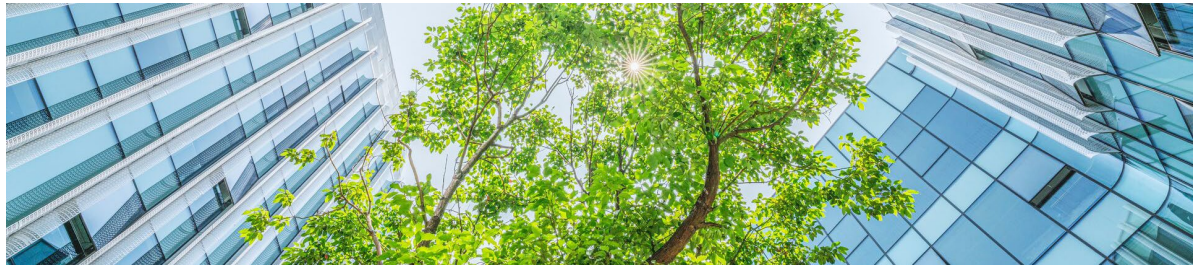
Aligned Testing, Without Losing Rigor

- SOC testing sequenced first or concurrently for shared controls; sample periods aligned where possible
- Financial auditors still perform their own independent procedures

Leading practice: Coordinate the populations, not the samples; each provider draws independent samples from one canonical population.

forvis mazars

One Communication Framework & Issue Log



One Communication Framework

- One kickoff and unified evidence request calendar, distributed once
- One consolidated status rhythm covering both engagements
- One open items log with owner, due date, and engagement relevance
- Audit committee receives a single consolidated assurance briefing

One Issue Log: Unified Governance

- Every finding enters one log with consistent taxonomy; root cause analyzed once
- One owner, one timeline; repeat findings visible across audit periods
- **Real-world example**: One organization found 40% of open issues traced to only three root causes—tracked separately for two years

forvis mazars

Operational Efficiency
Measurable Outcomes

Time

- **~2–4 weeks shorter** financial audit close through coordinated procedures
- Fewer bridge period escalations through proactive planning
- **Walkthrough hours reduced** through consolidated interviews

Cost

- Internal labor costs potentially reduced **30–45%** through evidence reuse and walkthrough consolidation
- Single provider coordination typically more cost-effective than two separate engagement fees
- Escalation and remediation costs reduced through unified issue management
- **340+ hrs. before → 190–230 hrs. after** across IT, Finance, and Compliance

Quality

- **Evidence quality improvements**: Canonical packages may be better designed and more reliably documented
- Fewer IPE and population questions; fewer incremental evidence requests
- Consistent control narratives across both reports; fewer divergent conclusions

Predictability

- Management can **plan audit support activities in advance**; no surprise request collisions
- Audit timelines can be more reliable; year-end close can be less disrupted
- Single coordinated assurance calendar replaces parallel, collision-prone schedules

forvis mazars

What Integration Means at the Executive Level
Strategic Benefits

CFO & Controller

- Faster, more predictable financial close supported by coordinated audit evidence
- Reduced total compliance cost; more efficient budget allocation
- Single audit relationship for both financial reporting and SOC obligations

CIO & IT Director

- IT team capacity restored from audit support to strategic control improvement
- Reduced IPE and ITGCs deficiency risk through coordinated evidence design
- Single provider for IT control assurance across both frameworks

CISO & Security

- SOC conclusions consistent with financial audit ITGCs conclusions; precludes explaining contradictions
- Single coordinated security control narrative across all assurance deliverables
- Earlier identification of security control gaps through integrated risk assessment

Audit Committee

- Consolidated assurance posture reporting; one provider, one accountability structure
- Consistent conclusions from a provider with a holistic view of the control environment
- Higher confidence in the organization's assurance program maturity
- **Beyond efficiency**: Earlier issue identification and reduced regulatory risk can strengthen governance and board confidence.

forvis mazars

The Power of an Integrated Assurance Approach
Summary

Structural Drivers

A single provider for both the financial statement audit and the SOC examination reduces separate planning, evidence design, walkthroughs, and issue tracking.

Measurable Impact

30–45% reduction in internal audit support burden; ~2–4 weeks shorter audit cycles; significant reduction in escalation and remediation costs.

Governance

Consistent conclusions, earlier issue identification, consolidated audit committee reporting, and faster control maturity advancement.

Independence

Coordination occurs at the planning, evidence, and communication levels—not at the conclusion level. Each team reaches independent conclusions.

Next: Practical frameworks, maturity model, implementation roadmap, leading practices

forvis mazars

Practical Frameworks & Leading Practices

The Integrated Assurance Operating Model

- Internal audit coordinator: Single point of coordination for both engagements
- Financial audit provider: Scope, independence, and conclusions
- SOC engagement provider: Attestation standards and conclusions
- Control owners: Evidence preparation within the canonical framework

- Pre-engagement kickoff (Q4 prior year): Unified scope, evidence design, calendar alignment
- Quarterly status checkpoints: Coordinated progress reporting to management
- Post-engagement governance: Consolidated findings reporting to audit committee

- Centralized repository with defined evidence owners, retention rules, and version control
- Evidence packages designed to satisfy both engagements from a single preparation
- IT leadership accountable for IPE validation and ITGCs evidence quality

- Single assurance status report to audit committee covering both workstreams
- One consolidated escalation path; no parallel board reporting tracks
- Consistent assurance posture narrative across executive and board communications

Leading practice: Components 1 and 2 can be implemented within a single audit cycle, capturing most efficiency gains before a provider transition.

forvis mazars

From Fragmented to Integrated
A Practical Roadmap

Cycle 1: Coordinate (Level 1–3)

- Conduct an assurance burden inventory: document evidence requests, walkthrough hours, and coordination overhead by function
- Identify high-overlap control areas: ITGCs, application controls, vendor assurance
- Establish canonical evidence definitions for top 10–15 high-frequency controls
- Align engagement calendars to preclude timeline collisions
- Establish a unified issue log with consistent taxonomy

Quick win: Consolidated vendor assurance review framework; fewer bridge letter surprises.

Cycle 2: Integrate (Level 4)

- Transition to single provider for both engagements (if not already in place)
- Implement coordinated walkthrough program, *i.e.*, single walkthrough serving both engagements
- Expand canonical evidence library to full control population
- Launch integrated governance reporting to audit committee

Cycle 3: Optimize (Level 5)

- **Continuous improvement cycle**: Measure burden reduction, evidence quality, and audit cycle time
- **Advance to Maturity Level 4–5**: Integrated assurance embedded in annual governance calendar
- **Expand coordination** to internal audit and regulatory examination activities

Goal: Assurance maturity at Level 4–5; efficiency gains quantified and sustained year over year.

forvis mazars

Anticipating & Addressing Common Integration Challenges

Challenges & Solutions

Organizations implementing integrated assurance may encounter predictable challenges, each with a practical, tested solution.

- **Challenge 1**: “We’ve always used separate providers and change is disruptive.”
  - Solution: Start with the coordination model (Maturity Level 3) before transitioning providers. Demonstrate efficiency gains from evidence design and calendar alignment first. Use those results to build the case for provider consolidation.
- **Challenge 2**: “We’re concerned about independence and conflicts of interest.”
  - Solution: Professional standards explicitly address this. AICPA standards permit a single firm to perform both a financial audit and a SOC Examination for the same organization, subject to standard independence and AICPA conceptual-framework safeguards.
- **Challenge 3**: “Our control owners won’t maintain a canonical evidence library.”
  - Solution: Start with 10–15 high-frequency controls; demonstrate time savings to the control owners themselves; build the library incrementally. Compliance follows demonstrated value.
- **Challenge 4**: “Our SOC and financial audit timelines don’t align.”
  - Solution: Calendar alignment is a planning decision, not a constraint. Work with the provider to design examination periods that reduce overlap—even a 30-day shift in start date can meaningfully reduce Q3/Q4 collision(s).

What to Watch

The most common failure mode is attempting too much in Cycle 1. A targeted pilot (one high-risk process, one evidence package, one vendor class) can demonstrate value quickly and build momentum.

forvis mazars

Critical Success Factors & Leading Practices

What High-Maturity Organizations Do

Sustainable integration depends on organizational commitments, not technology – each observable, measurable, and replicable.

- **Executive sponsorship**: The CFO, CIO, or CAE champions integration as a priority rather than delegating it as an IT coordination task
- **Clear accountability**: A named coordinator owns the assurance calendar, canonical evidence library, and single issue log
- **Live assurance calendar**: Providers, internal audit, and regulatory exams mapped on one calendar, updated quarterly with clear evidence windows
- **Evidence design discipline**: A canonical library for high-frequency controls with owners named and parameters and retention enforced before requests arrive
- **Unified walkthroughs and proactive vendor management**: Control narratives documented once as living documents; CUEC mapping matrix and bridge letters managed ahead of deadlines
- **Single issue log**: Consistent root-cause taxonomy, named remediation owners, reported to the audit committee quarterly
- **Continuous measurement**: Burden/fatigue reduction, evidence quality, and audit-cycle time tracked annually against the five-level maturity model

forvis mazars

Executive Action Checklist
Where to Start

For All Executives

- Estimate your organization's total annual audit support burden in hours across IT, finance, and compliance functions
- Map your current assurance calendar: identify all active engagements, their timing, and where overlap occurs
- Ask your current audit provider(s) whether they perform both financial audits and SOC Examinations—and whether they coordinate between teams
- **Assess fit**: Overlapping control domains, colliding fieldwork windows, dual governance tracks, and a provider capable of both engagements all signal a strong integration opportunity

For CFOs & Controllers

- **Quantify internal audit labor costs**: How much of your team's time is absorbed in audit coordination vs. core finance activities?
- **Review your vendor assurance program**: Are bridge letters managed proactively or reactively?
- **Assess** whether your financial audit and SOC providers have been asked to coordinate, and whether they have a framework for doing so

For CIOs & CISOs

- **Audit your canonical evidence posture**: For your top 10 most-audited controls, is there a defined scope, parameters, and owner for each evidence package?
- **Identify the three controls** that generate the most duplicate evidence requests and prioritize them for canonical evidence design
- **Review your CUEC compliance matrix**: Do you have documented evidence that each CUEC was operated during the most recent examination period?

Executive insight: Start with the burden inventory; organizations that measure their total audit support cost are well-positioned to build the business case for integration.

forvis mazars

Summary
Q&A

Five Key Takeaways

Organizations that coordinate financial statement audit and SOC Examination activities under a single integrated provider model consistently achieve lower costs, reduced burden, higher-quality assurance, and stronger governance outcomes.

1. **The problem is structural.** Fragmented assurance creates duplicate evidence requests, redundant testing, inconsistent timelines, and increased burden. This is a predictable consequence of the separate provider model.
2. **The solution is integration.** A single provider performing both the financial statement audit and the SOC Examination enables coordinated planning, integrated risk assessment, aligned testing, and efficient evidence sharing—while fully maintaining independence.
3. **The benefits are measurable.** Integrated assurance can reduce internal audit support costs by 30–45%, shorten audit cycles by 2–4 weeks, and significantly reduce escalation and remediation overhead.
4. **Quality and governance improve.** One provider yields consistent conclusions, earlier issue identification, consolidated governance reporting, and improved audit committee confidence.
5. **The path forward is clear.** Start with evidence design and calendar alignment; advance to provider integration; measure and report efficiency gains; mature toward Levels 4–5.

forvis mazars

Q&A

SOC & HITRUST® Solutions

Questions?

forvis mazars

Contact

Forvis Mazars

Karen Cardillo
Managing Director
SOC & HITRUST Practice
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal
SOC & HITRUST Practice
ryan.boggs@us.forvismazars.com

Scan to learn more about our SOC & HITRUST® Services

forvis mazars