Combined SOC 2 & ISO 27001 Audits

Practical strategies to reduce audit fatigue, improve efficiency, and align two of the industry's most important assurance frameworks

Building one security program to support multiple assurance outputs

ISC2 CHAPTER | EAST BAY

Frank, Rimerman + Co. LLP
certified public accountants

Introduction

A quick background before we get started

Nelly Spieler

Nelly has nearly 20 years of auditing, consulting and management experience working with companies worldwide. She currently leads the firm's Technology Assurance and Risk Management practice which includes all service areas involving Cybersecurity, Privacy, System and Organization Controls (SOC). The team is accredited by ANAB to perform ISO/IEC 27001, 27701, 27017, 27018 and ISO 42001 audits, and frequently delivers integrated audits—either conducting both the ISO and SOC 2 engagements in-house or leading the ISO portion while another firm that is not ISO-accredited performs the SOC 2. Nelly is also an ISO Lead Auditor.
Nelly leverages her expertise in cloud security, information systems and controls into an array of topics in the Governance, Risk and Compliance field.

Nelly works with a range of clients including privately held, pre-IPO, and public companies. Nelly's experience includes serving as both an internal and external auditor for her clients. Prior to working in the professional services field, Nelly worked in both high tech start-ups and large corporations within IT and Engineering departments.

Frank, Rimerman + Co. LLP
certified public accountants

Perspective today: security-first, assurance-aware, and very practical.

Agenda & Learning Objectives

What we will cover in the next 50 minutes

Agenda

- Why Integrated Audits Matter
- Building the Foundation
- Planning for Efficiency
- Executing an Integrated Audit
- Lessons Learned & Practical Takeaways

Learning Objectives

✅ Explain how one security program can support multiple assurance frameworks.
✅ Identify key considerations for integrating SOC 2 and ISO 27001 audits
✅ Reduce audit fatigue through better planning and coordination
✅ Apply practical strategies for scope, evidence, timeline, and audit alignment
✅ Avoid common pitfalls that increase cost, complexity, and effort
✅ Select and work with auditors in a way that supports a coordinated audit experience.

Polling Question 1

How many assurance frameworks does your organization manage today?

A. SOC 2 only

B. ISO 27001 only

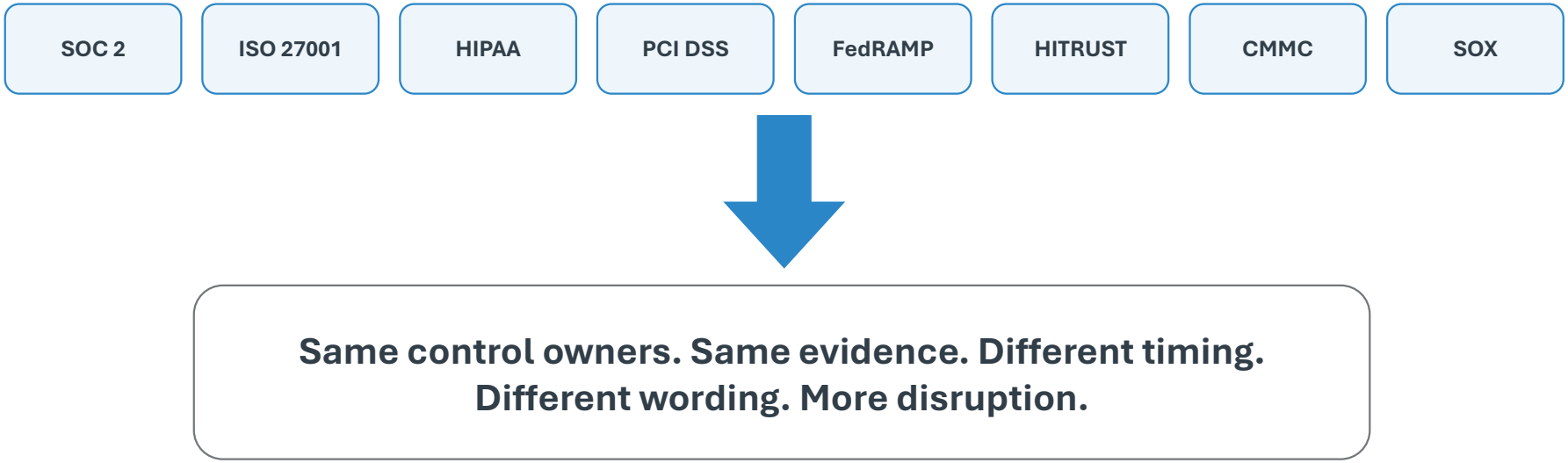
C. SOC 2 and ISO 27001

D. Three or more frameworks (SOC 2, ISO 27001, HITRUST, HIPAA, SOX, CMMC, FedRAMP, etc.)

E. Not sure / not applicable

The Real Problem: Audit Fatigue

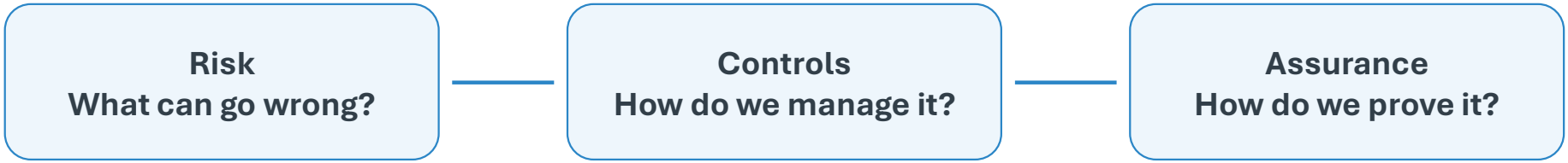
Fragmented assurance creates friction for security and engineering teams



Audit fatigue is often a symptom of fragmented governance — not necessarily weak security.

Security First, Compliance Second

Compliance should follow from a well-governed security program



Security asks: Is the system protected?

Governance asks: Can we trust the outcomes, and does management understand the impact?

Example: for user access, security enforces least privilege and MFA; governance confirms access is owned, reviewed on a schedule, and that management accepts the residual risk.

One Security Program, Multiple Assurance Outputs

The same foundation can support different customer and market needs

What Matters for Integration?

Similar security goals, different structures

1 Controls	2 Scope	3 Evidence

ISO 27001

- ✓ International management system standard
- ✓ Required clauses 4–10 for ISMS governance
- ✓ Annex A defined control set
- ✓ Statement of Applicability determines applicable controls
- ✓ Certification by accredited certification body

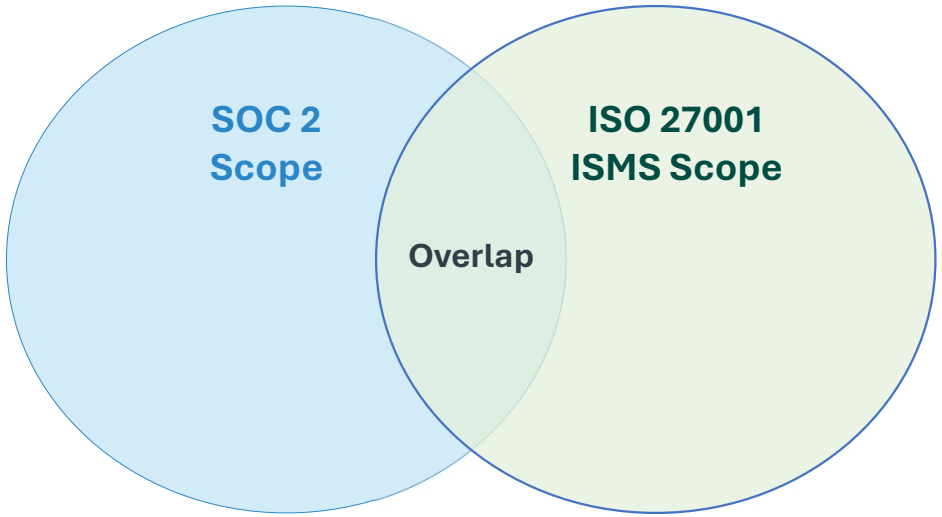
SOC 2

- ✓ AICPA attestation report
- ✓ Based on applicable Trust Services Criteria
- ✓ Points of focus guide consideration, but are not a required control list
- ✓ Company designs controls to meet commitments, system requirements, and criteria
- ✓ Report issued by CPA firm/service auditor

Integration works when the control environment is mapped carefully — not when one framework is forced into the wording of the other.

Scope Alignment Matters

Control overlap does not guarantee scope overlap



- Systems
- Products/services
- People
- Locations
- Vendors
- Business processes
- Risks

Control mapping identifies the overlap.
Scope determines how much of that overlap can actually be leveraged.

From Control Mapping to Evidence Planning

Collect once, satisfy many – when scope and requirements align

Control Mapping

Identifies where SOC 2 and ISO 27001 requirements align.

EXAMPLE AREAS

- Access management
- Vulnerability management
- Vendor/Supplier management
- Incident response
- Change management
- Security awareness
- Business continuity and disaster recovery

Evidence Planning

Determines how evidence will be collected, reviewed, and leveraged.

PLANNING QUESTIONS

- Which evidence supports both audits?
- Which evidence is unique to one framework?
- Are populations aligned?
- Is timing aligned?
- Who reviews it and when?
- How are walkthroughs coordinated?

Control mapping identifies the opportunity. Evidence planning creates the efficiency.

Frank, Rimerman + Co. LLP
certified public accountants

Timeline Alignment Matters

Integrated audits are easier when the audit calendars are aligned, not just the controls.

PLAN THE AUDIT CALENDAR EARLY

What strong teams map out before fieldwork begins

1

SOC exam period

The Type 2 window controls operate across (Jan 1 – Dec 31)

2

ISO certificate date

Annual audits — flexible, but before the certificate expires

3

Owner & auditor time

Line up control-owner and auditor availability

4

Evidence timing

Some SOC evidence is due within 3 months of period end

Risks of Misalignment

- Evidence collected too early
- Reconfirmation required
- Duplicate walkthroughs
- Certification scheduling pressure
- Lost integration opportunities

Benefits of Alignment

- Shared evidence collection
- Shared walkthroughs
- Reduced rework
- Better audit coordination

Frank, Rimerman + Co. LLP
certified public accountants

Practical Integrated Audit Approaches

ISC2 CHAPTER EAST BAY

Framework overlap creates opportunity. Planning determines whether that opportunity is realized.

Evidence-First Approach

"Upload first, discuss later"

1. Evidence uploaded
2. SOC / ISO review before fieldwork
3. Questions identified early
4. Shorter walkthroughs
5. Clarify and confirm

KEY POINTS

- Works well when evidence is easy to collect
- Reduces interview time
- Auditors review before walkthroughs
- Walkthroughs focus on clarification

Show-and-Tell Approach

"Demonstrate live, capture efficiently"

1. Pre-plan overlapping evidence
2. SOC evidence reviewed where available
3. ISO walkthrough / live demonstration
4. Auditors capture remaining evidence
5. True-up samples and questions

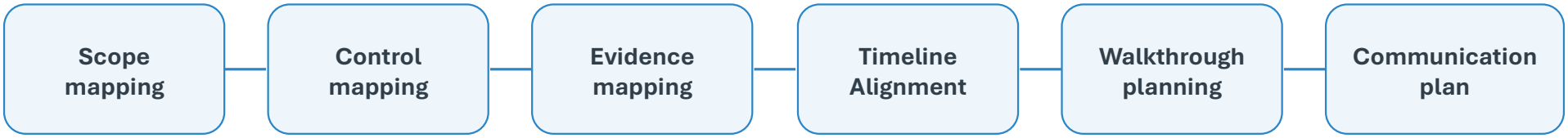
KEY POINTS

- Works well when screenshots are burdensome
- Control owners demonstrate evidence live
- Auditors capture needed support
- SOC questions cleared during ISO walkthroughs

Evidence-first or walkthrough-first — the key is deciding intentionally before fieldwork starts.

Integrated Audit Planning

Most efficiency is created before fieldwork starts



- ❑ Identify overlapping controls and process owners early
- ❑ Agree what evidence can support both frameworks
- ❑ Define what will be collected during ISO fieldwork vs. SOC testing
- ❑ Avoid duplicate walkthroughs where scope and objectives align

Executing an Integrated Audit

The goal isn't to test everything once — it's to coordinate the work wherever it makes sense while still meeting both frameworks.

COORDINATE WHEREVER IT MAKES SENSE

Walkthroughs	Evidence Review	Questions & Requests
One process discussion and demonstration can support both the SOC and ISO audits.	Shared evidence is identified once and leveraged across both frameworks.	Questions are consolidated and follow-up requests managed centrally.

WHERE TESTING DIVERGES

SOC 2

- Focused on operating effectiveness over the defined examination period
- Sample-based testing covering the full reporting period

ISO 27001

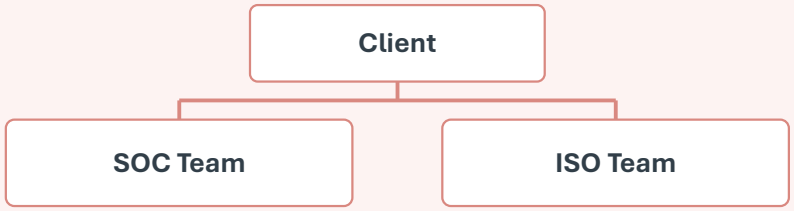
- Evaluates the information security management system
- Reviews implementation, evidence, and risk management for conformance with the standards

Similar controls may still require different testing, samples, timing, or evidence. Coordinate where the differences don't matter — the result is two audits executed efficiently, not one.

Choosing the Right Audit Team

One firm offering both services is not always one integrated team

Separate Teams
WARNING



Separate planning

Separate requests

Separate walkthroughs

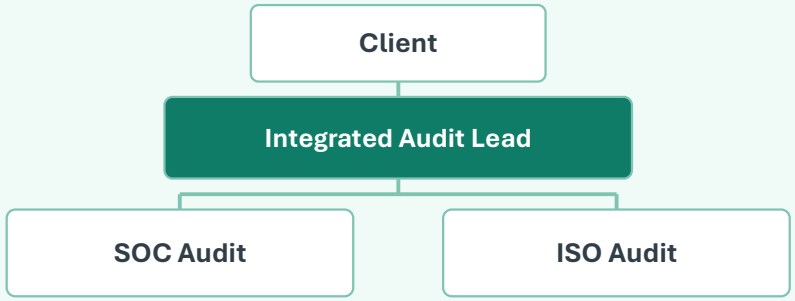
Separate follow-up

✗ **Duplicate effort**

✗ **Multiple contacts**

✗ **Conflicting requests**

Integrated Team
RECOMMENDED



✓ **Coordinated planning**

✓ **Coordinated evidence requests**

✓ **Coordinated walkthroughs**

✓ **Single point of accountability**

Ask to meet the people who will actually oversee the engagement — not just the salesperson or partner.

Frank, Rimerman + Co. LLP
certified public accountants

Polling Question 2

What is the biggest source of inefficiency in your audit process?

- A. Evidence collection and repeated document requests
- B. Duplicate walkthroughs or process interviews
- C. Misaligned audit timelines
- D. Unclear scope or evidence mapping
- E. Separate auditors or reviewers asking similar questions
- F. Not sure / not applicable

Common Pitfalls

What goes wrong when integration is treated as a shortcut

- ❌ Assuming control overlap means scope overlap
- ❌ Stopping at the control matrix instead of planning the evidence
- ❌ Waiting too long to involve auditors
- ❌ Using separate audit teams that don't coordinate
- ❌ Copying framework language into policies that don't reflect the business
- ❌ Treating ISO management system requirements as optional extras
- ❌ Over-relying on GRC tools
- ❌ Treating compliance as the objective instead of security risk management

Integration should reduce duplication — not reduce professional judgment.

Five Practical Takeaways

What I would want you to remember

1. **Objectives first** - Start with security objectives and risk — not audit wording.
2. **Scope matters -** Evaluate scope before assuming evidence can be reused.
3. **Build once -** Build controls once and reuse evidence where it truly fits.
4. **Coordinate** - Coordinate planning, walkthroughs, sampling, and communication.
5. **Right team** - Choose a team that understands both frameworks in practice.

The goal is not to pass two audits.
The goal is to operate one effective security program that supports multiple forms of assurance.

Questions

Thank you for your time. We hope you found this information valuable.

Frank, Rimerman + Co. LLP
certified public accountants

Thank you

Nelly Spieler
Assurance & Advisory Partner
nspieler@frankrimerman.com

Frank, Rimerman + Co. LLP
certified public accountants

www.frankrimerman.com

Frank, Rimerman + Co. LLP
certified public accountants