

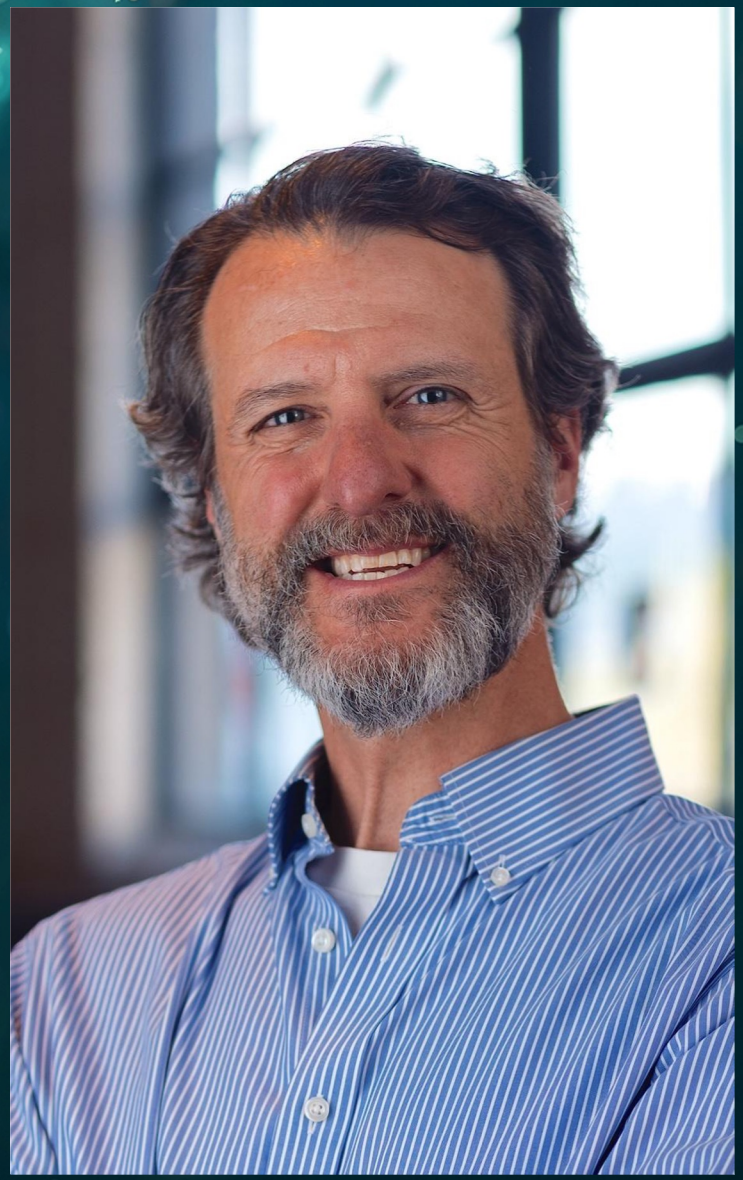
ROC'em SOC'em Robots

PCI DSS · PCI SSF · SOC 1 · SOC 2

Use of Automation for Efficiency in Consolidated Assessments

Sam Pfanstiel, PhD

Principal Analyst, Toast



Adam Bush

Managing Director, Schellman



20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council

schellman

Quality, above all.

Case Study Overview



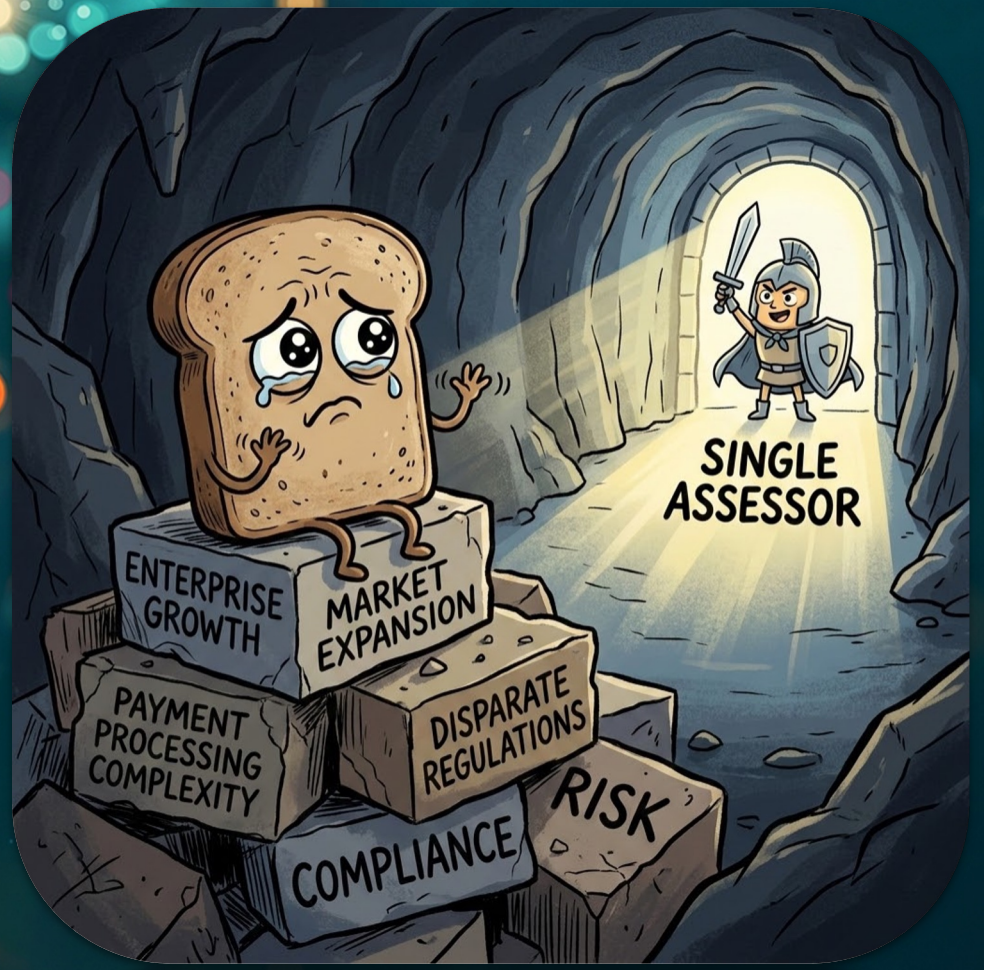
The views expressed here are our own and do not represent the official position of Toast, Inc. or Schellman & Company, LLC.

This information is intended for INFORMATIONAL PURPOSES ONLY, and not as a binding commitment. Please do not rely on this information in making any purchasing decisions. The development, release, and timing of any products, features, or functionality described in this presentation remain at the sole discretion of the company offering them and are subject to change. Each company speaks only for itself and makes no representations regarding the products, statements, or materials of any other company. No company warrants the accuracy or completeness of any information, text, graphics, links, or other items in this presentation, or guarantees that you will achieve any particular results from following any advice it contains.

Case Study Overview - Toast

Toast Business Requirements for RFP

1. Rotating Assessor (recommended practice)
2. Multiyear Contract to Maximum Partnership and Ongoing Efficiencies
3. Multi-framework:
   PCI DSS, PCI SSF SSS, PCI SSF SSLC,
   PCI PIN, SOC 1, SOC 2 (different scopes)
4. Multi-Products
   a. Toast Go 3
   b. Flex 3
   c. Core Environment
   d. Toast Capital
   e. Payroll
5. No reduction in rigor



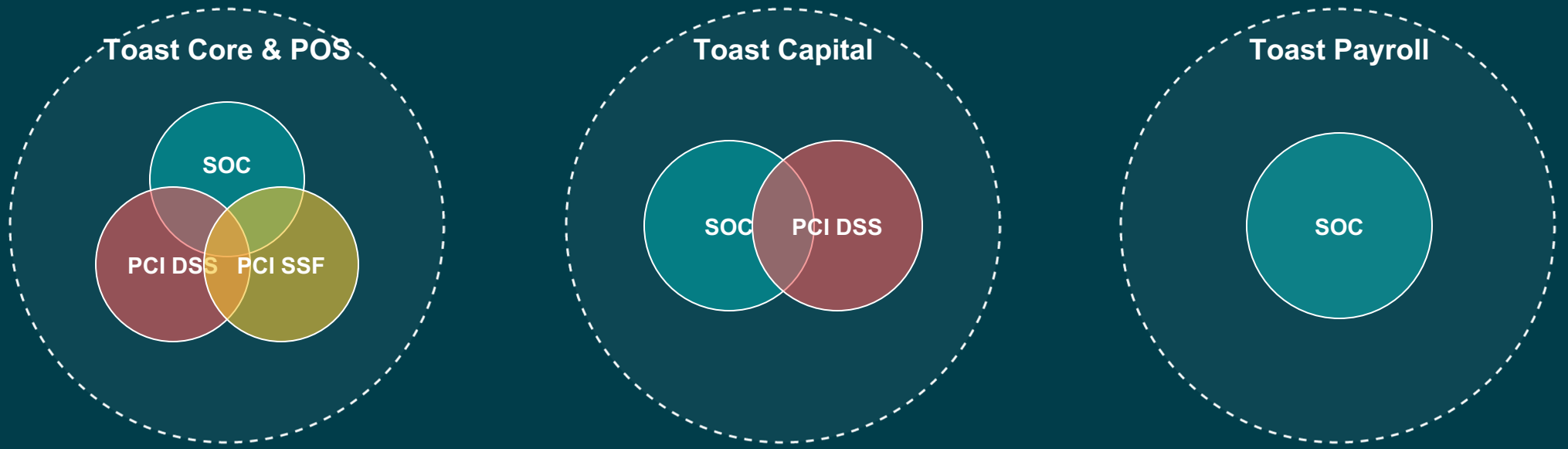
Case Study Overview

Schellman Experience

- Multi-year, multi-framework engagement
- PCI DSS + SSF + SOC
- Multiple products, shared ecosystem
- Specialized assessors required
- Common assessors where practical
- Integration by design - not magic



Case Study Overview - Scope Concept Diagram



Case Study Overview - Constraints

Integrated Scope Definition

- No Implicit Satisfaction:
  SOC controls do not implicitly fulfill PCI requirements; each standard has distinct testing mandate.
- Dual Validation:
  Evidence must be evaluated independently against the precise technical and administrative criteria of both PCI and SOC standards.

Harmonized Operational Execution

- Common Request Library:
  A unified evidence request maps to multiple underlying framework requirements.
- Cross-Trained QSAs:
  External assessment teams leverage QSAs with SOC experience to perform a consolidated review of shared artifacts.
- Synchronized Sampling Window:
  Coordinated testing timelines help streamline evidence collection across all five frameworks

Case Study Overview - Tooling

Enabling the Process: Our Technology Stack

Optro

Internal GRC

- Unified repository for managing risk registers
- Establishes clear control ownership across teams
- Automates operational evidence collection

Fieldguide

Assessor Platform

- Primary interface used by Schellman assessors
- Facilitates seamless external collaboration
- Tracks real-time review status and validation

Middleware

Custom Integration

- Custom APIs built using AI coding assistants
- Bridges data flow between GRC and assessor portals
- Supports ongoing bi-directional syncing

LLM Scripts

Semantic Analysis

- Standalone Python scripts utilizing LLMs
- Automates cross-framework control mapping between PCI DSS, SOC, and PCI SSF
- Human review

Outcomes & Metrics



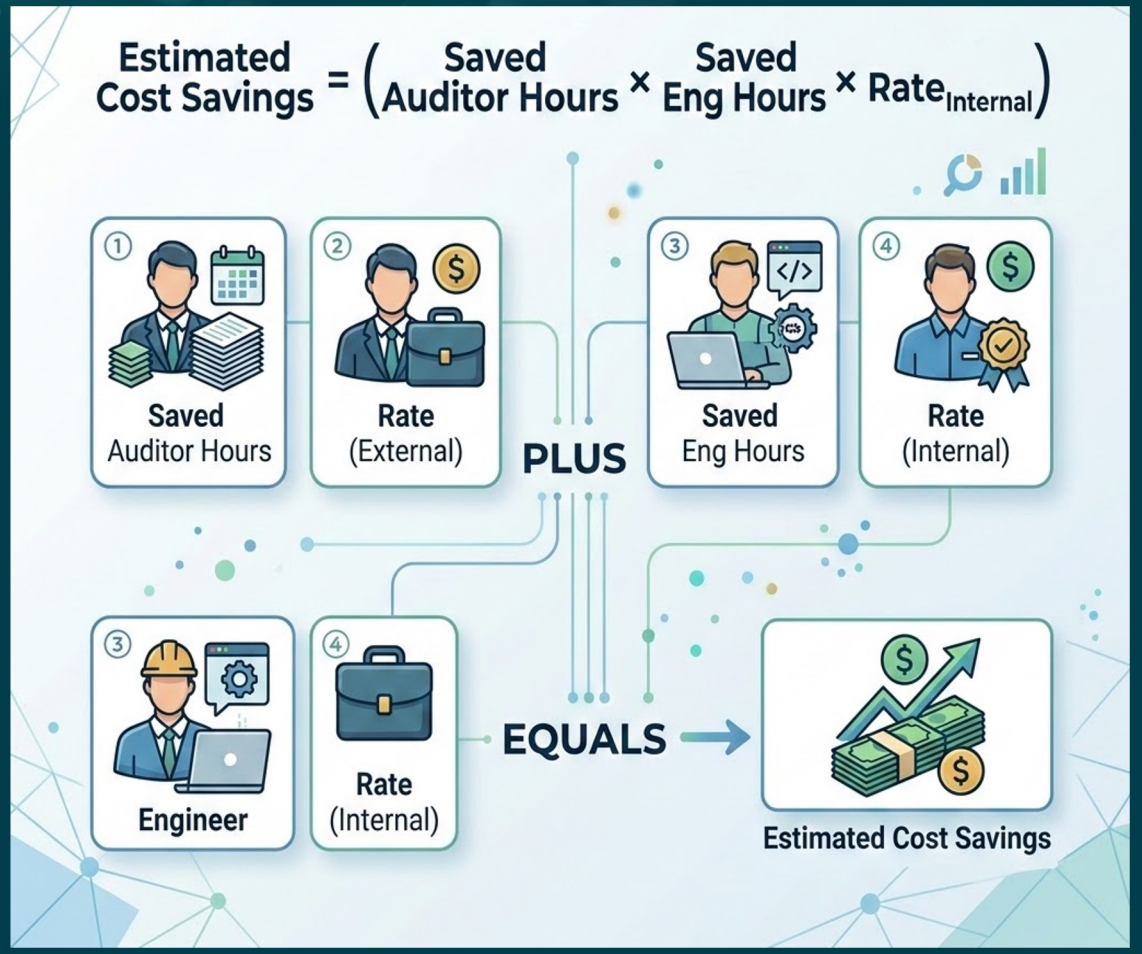
Outcomes - Toast

Operational Value

- Evidence Once: Artifacts uploaded to Optro populate to Fieldguide, designed to significantly reduce duplicate evidence uploads.
- Reduced Assessor Touchpoints: Automated API, status syncing significantly decreases recurring status meetings and email chasing
- Continuous Posture: Shifting from an annual 'audit scramble' toward ongoing, audit-ready evidence streams.

Measurable ROI

- Cost Optimization: Streamlined reviews reduce billable external auditor hours and total engagement expense.
- Reclaimed Resource Capacity: Minimizing duplicate interviews helps free engineering and product teams to focus on core roadmap delivery.



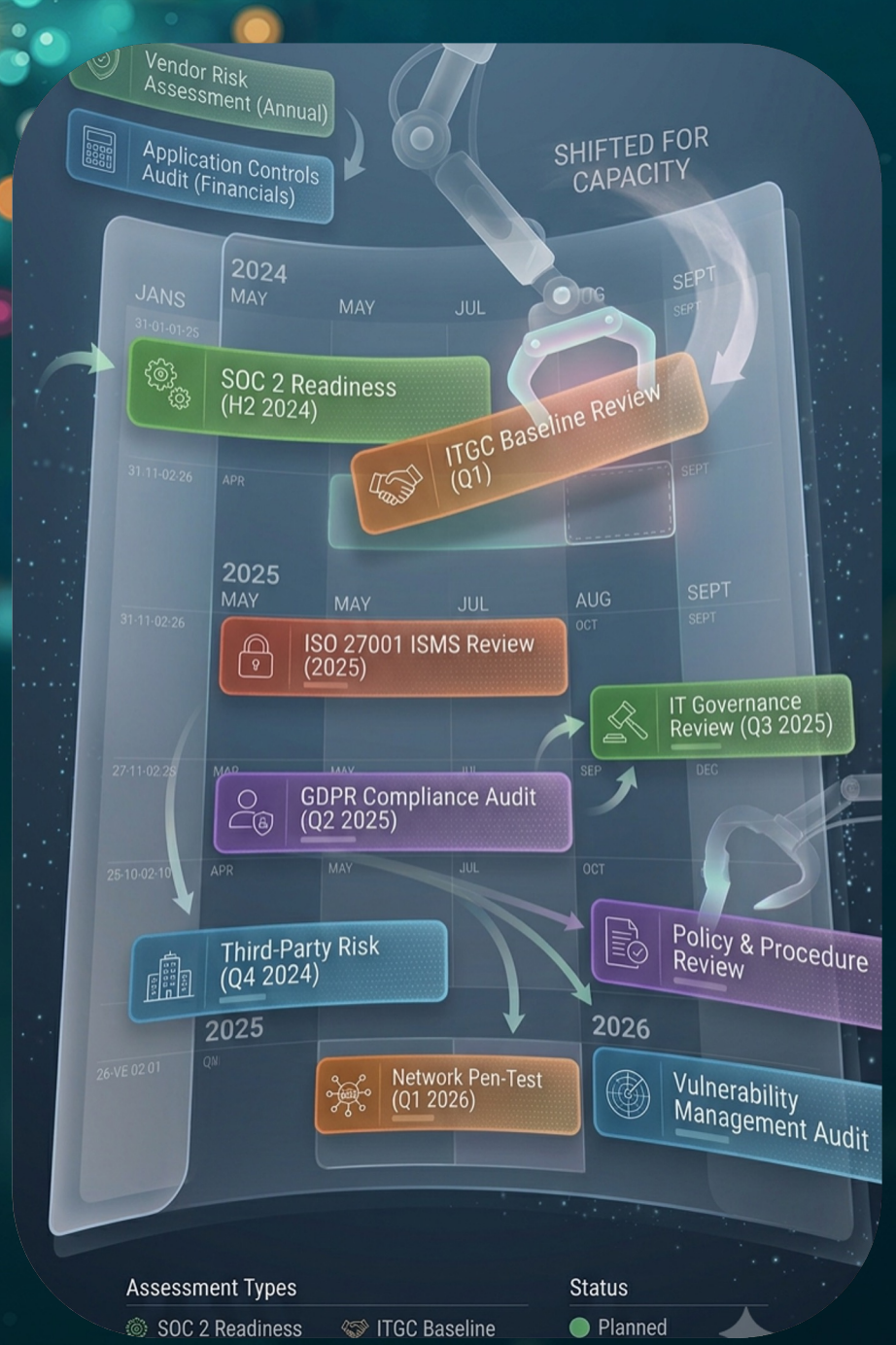
Outcomes - Schellman

Timing Optimization

- Map every engagement
- Respect reporting deadlines
- Align compatible assessments
- Create breathing room where needed
- Stage work for maximum reuse

Quantifiable Impact

- 1,339 standalone requests
- 871 consolidated requests
- 468 requests eliminated
- 35% fewer client requests
- Less noise, more value



Outcomes - Other Clients

Does this approach generalize?

Cross-Framework Opportunities

- SOC + ISO: natural alignment
- PCI joins the conversation
- NIST as common language
- Shared controls, shared evidence
- Purposeful control mapping

The Tradeoff

- Consolidate where it counts
- Some requests become broader
- Fewer asks, richer responses
- Less churn for stakeholders
- Optimize the overall experience



Learnings


20
YEARS OF SECURING
PAYMENT DATA
PCI
Security
Standards Council

Learnings - Toast

What we'd tell ourselves at the RFP

Collaboration is front-loaded

- We budgeted for tooling. We spent calendar.

1 Control → 1 Owner → 1 Description

- Shared controls fail if the wording isn't shared too.

AI drafts; Humans decide

- Every mapping was reviewed by a human. Budget for the QA.

What we'd do differently

- Taxonomy first, plumbing second.
- Involve control owners early.

Learnings - Schellman

Key Takeaways

- Collaboration is the multiplier
- Invest heavily up front
- Security first, compliance follows
- AI accelerates - not replaces - judgment
- Automation demands expert QA
- Shared controls require consistency
- Coordination prevents duplicate effort
- Think like one audit team



Community Collaboration



Community Collaboration - BoA

Sam is a member of the PCI SSC Board of Advisors

Participation & Standards Evolution

- Valuable opportunities to share operational insights across the payment landscape.
- Real-World Feedback: PCI SSC actively seeks direct input from participating organizations and BoA members regarding practical implementation challenges.
- Harmonization & Automation Focus: Real-world feedback on multi-framework harmonization, modern engineering practices, and automated compliance technologies.
- Continuous Dialogue to Ensure security standards evolve dynamically alongside modern cloud architecture and CD pipelines.
- PCI DSS alignment with DORA



Community Collaboration - GEAR

Adam Bush is a member of the PCI SSC Global Executive Assessor Roundtable

GEAR Initiatives

- Machine-readable standards (Standards computers can understand)
- Enable AI-ready frameworks
- Advance control crosswalks like PCI DSS 4.0.1↔ NIST CSF mapping
- Better framework interoperability
- Smarter tools, better assessments
- Preparing for what's next

Summary

- A Consolidated Assessment approach isn't right for everyone: it requires communication, collaboration, tech enablement, and willingness to get "into the weeds" to navigate scope and framework complexities.
- Examples of crosswalked requests, requirements and controls between SOC, PCI DSS and other PCI standards.
- Tech- and AI-enabled processes can streamline evidence collection and consolidated-audit collaboration.
- Updates on how the Board of Advisors and GEAR are supporting PCI SSC's activities to improve efficiency

PCI Security Standards Council®

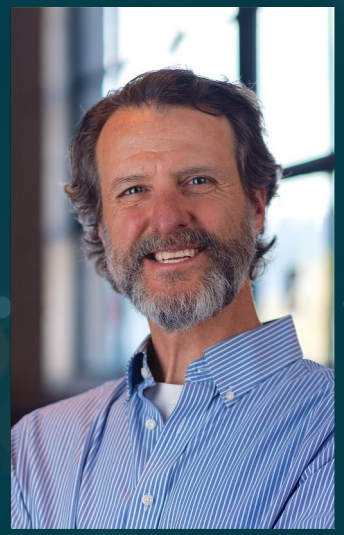
toast

schellman
Quality, above all.

Thank You!



Adam Bush
Managing Director, Schellman
/adamdbush



Sam Pfanstiel, PhD
Principal Analyst, Toast
/diverge