RELISH

Modernizing Audit & Finance Workflows

Best practices for managing supplier data and payment controls

YOUR PRESENTERS

Meet the Presenters

DOUG CARLSON

Head of Regulated Industries, Relish

- Former CPO, University of Nebraska
- Former CPO, State of Nebraska
- 10+ years in public sector procurement leadership
- Deep expertise in audit compliance, Accounts Payable, and supplier management

DAN PARK

Head of Sales – Workday, Relish

- 20+ years in high-tech sales leadership
- Deep expertise in the Workday ecosystem — drove growth in Workday's sales organization and partner network
- Leads Relish's Workday go-to-market strategy, helping procurement and AP teams automate supplier compliance and fraud controls

What We'll Cover Today

01 **About Your Presenters**
CPO experience meets Workday expertise

02 **The Public Sector Challenge**
Pressure, risk, and regulatory expectations

03 **Key Takeaway 1: Audit-Ready Supplier Validation**
Continuous validation & CFR 200 compliance

04 **Key Takeaway 2: Bank Account Validation**
Preventing fraud and improper payments

05 **Key Takeaway 3: Security Practices**
SOC 2, GDPR, HIPAA – staying audit-ready

06 **Introducing Relish Data Assure + Q&A**
Automated, defensible controls for your ERP

QUICK POLL

What's your biggest supplier management challenge right now?

A	Manual processes — too much time on data entry, W-9s, and follow-up
B	Audit risk — we've had findings or are worried about the next review
C	Fraud concerns — bank account changes, duplicate vendors, improper payments
D	Security & compliance — PII exposure, SOC 2, HIPAA, or GDPR obligations
E	All of the above

A WORD FROM EXPERIENCE

I've Sat in Your Chair

> *When I was CPO at the University of Nebraska, our supplier onboarding process was a glorified spreadsheet, a stack of W-9s in someone's inbox, and a manual SAM.gov lookup that we hoped someone remembered to run.*
>
> *We had good people. We had solid intent. But we were one audit away from findings we couldn't defend — because our controls were invisible.*
>
> **— Doug Carlson, Former CPO, University of Nebraska & State of Nebraska**

Doug's Background

- Managed $700M+ in annual public procurement spend
- Led supplier compliance for a Big Ten university system
- Navigated federal grant audits under CFR 200
- Oversaw procurement and invoice system implementation

The Public Sector Challenge

Agencies face increasing pressure — with limited time, staff, and resources

Regulatory Exposure

CFR 200, state funding requirements, and audit standards demand continuous compliance — not just annual reviews.

Staff Burden

Manual supplier onboarding, data checks, and payment approvals pull teams away from strategic work.

Audit Findings

Incomplete or outdated supplier records are among the top drivers of audit findings and compliance risk.

Fraud Risk

Improper payments, duplicate vendors, and unvalidated bank accounts remain persistent threats to public funds.

Supplier Fraud in Higher Education: By the Numbers

$68K–$75K

median loss per fraud case in higher education — per occurrence

$107K+

per occurrence in large-scale vendor impersonation and wire transfer fraud targeting university payments

$5.75

in total costs incurred for every $1 directly lost to fraud — including recovery, legal fees, and remediation

9.8%

of equivalent annual revenue lost to fraud by U.S. organizations — up from 6.7% in prior years

Source: Higher Ed Fraud Impact Report, 2026

THE COST OF INACTION

The Numbers Don't Lie

$162B

in improper payments reported by U.S. federal agencies in FY 2024 — $2.8T cumulative since 2003 Source: U.S. GAO, March 2025

79%

of organizations experienced attempted or actual payment fraud in 2024, most via manipulation of approval and payment workflows Source: AFP Payments Fraud & Control Survey, 2025

~89%

of occupational fraud cases involve asset misappropriation — phantom vendors, falsified payments, unauthorized approvals Source: ACFE Report to the Nations, 2024

68%

of businesses still manually enter AP data into their ERP or accounting platform — a key source of errors and fraud exposure Source: BILL.com Procurement Audit Research

BEST PRACTICES COMPARISON

Common Pitfalls — and What Best Practice Looks Like

✗ MANUAL PROCESS (TODAY)	✓ BEST PRACTICE APPROACH
Email W-9 requests; wait days for replies; chase vendors manually	Best practice: suppliers self-serve their data through a secure portal — reducing staff burden and data entry errors
Manual SAM.gov lookups — if staff has time to run them	Best practice: schedule recurring SAM.gov and OFAC checks, not just at onboarding — status changes between reviews
Bank account changes confirmed via email or phone call — easily spoofed	Best practice: verify bank account ownership through a separate channel before processing any new or changed account
Audit prep means pulling files, emailing colleagues, scrambling for proof	Best practice: log every validation action with a timestamp — if you can't show the verification and when you did it, it might as well not exist
PII (SSNs, bank details) emailed across staff inboxes and shared drives	Best practice: sensitive data (SSNs, bank info) should never travel through email — use encrypted portals with role-based access

KEY TAKEAWAY 01

Audit-Ready Supplier Validation

Reduces Compliance Risk

Knowing your suppliers is a regulatory requirement for public funds.

KEY TAKEAWAY 1 • THE AUDITOR'S LENS

What Auditors Are Actually Looking For

Insight from someone who has prepared for — and passed — public sector audits.

What triggers a finding

- No documentation that vendor was verified before first payment
- Compliance checks not performed — or performed once at onboarding but never again
- W-9 on file is expired, unsigned, or doesn't match ERP data
- No evidence of who approved the vendor or when

What auditors want to see

- A timestamped record of every validation check performed
- Evidence of continuous monitoring — not just point-in-time
- Clear segregation of duties in the approval workflow
- Ability to produce any supplier's full validation history on demand

What "defensible" really means

- A system-generated log is evidence. An email chain is better than nothing
- Auditors want to see the process, not just the outcome
- If you can’t replicate it, it might as well not exist

QUICK POLL

When it comes to your vendor/supplier records right now, which statement is most true?

A	We validate vendors at onboarding but don't re-check them after that
B	We have had a bank account change request come through — and it made us uncomfortable
C	Our W-9s and sensitive vendor data are stored in shared drives or email inboxes
D	Honestly, we're not sure our current process would hold up to a detailed audit
E	All of the above

KEY TAKEAWAY 1 • SUPPLIER VALIDATION BEST PRACTICES

Best Practices for Audit-Ready Supplier Validation

- Verify supplier identity, tax status, and licensure at onboarding — and document exactly what was checked and when
- Screen against SAM.gov debarment lists and state exclusion databases on a recurring schedule — not just at onboarding
- Collect and validate W-9s and W-8s before a vendor is activated — treat an incomplete tax form as a hard stop, not a follow-up item
- Periodically review your vendor master for duplicates, dormant records, and high-risk entries — a clean vendor list is a compliance asset
- Maintain a dated, written record of every validation step — who checked, what they checked, and the result. Verbal confirmation is not a control.
- Build a standing cadence for re-validating active vendors — annual at minimum, quarterly for high-spend or high-risk suppliers

Why These Practices Matter

- CFR 200 requires documented due diligence — the process must be visible, not assumed
- State funding requirements often mirror federal standards — one framework should cover both
- The most common audit finding isn't fraud — it's missing documentation
- A consistent, repeatable process is defensible — an inconsistent one is a liability

KEY TAKEAWAY 1 • REGULATORY CONTEXT

Understanding Your Compliance Obligations

2 CFR Part 200

Uniform Grant Guidance

Federal recipients must verify supplier eligibility, maintain documentation of due diligence, and demonstrate ongoing vendor oversight — not just at onboarding.

SAM.gov Debarment Checks

System for Award Management

All entities receiving federal funds must screen suppliers against SAM.gov exclusion lists before any payment is made. Recurring, scheduled checks are far more reliable than one-time lookups.

State Funding Requirements

Varies by Jurisdiction

State-funded agencies may have additional vendor verification obligations that often mirror federal standards.

KEY TAKEAWAY 02

Bank Account Validation

A Powerful & Often Overlooked Control

Validate ownership before every payment.

KEY TAKEAWAY 2 • BANK ACCOUNT VALIDATION BEST PRACTICES

Validating Bank Ownership Before Payment

The Problem

- Fraudulent bank account changes are among the most common ACH fraud vectors against government entities
- Manual approval processes rely on email confirmations — easily spoofed
- Delayed detection means funds are often unrecoverable once wired
- Duplicate vendor accounts enable split-payment fraud schemes
- Staff don't have tools to verify account ownership in real time

Best Practice Controls

- Verify bank account ownership through an independent channel — micro-deposit, instant verification, or third-party confirmation — before any payment is issued
- Build a reconciliation step that flags mismatches between ERP records and verified account ownership
- Replace manual call-back verification with a documented, repeatable process that doesn’t rely on individual staff judgment
- Controls should live inside your existing ERP workflow — not require staff to use a separate system or bypass established processes
- Every bank account verification action should be timestamped and retained — your audit trail is only as strong as your documentation

KEY TAKEAWAY 2 • FRAUD LANDSCAPE

How Fraud Happens — And How to Stop It

Ghost Vendor Scheme HIGH RISK	A fictitious vendor is entered into the ERP. Invoices are submitted and paid without any corresponding goods or services.	Best practice: verify supplier identity through independent data sources at onboarding — EIN validation, business registration, and identity checks — before any account is activated.
Account Takeover / ACH Fraud HIGH RISK	An attacker changes a legitimate vendor's bank account via a spoofed email. Payments are redirected before anyone notices.	Best practice: any bank account change should require independent ownership verification and a cooling period before payments are processed — never rely on email confirmation alone.
Duplicate Payment Fraud MEDIUM RISK	Invoices are submitted twice — intentionally or accidentally — resulting in double payment.	Best practice: run duplicate vendor and invoice checks as a pre-payment control, not a post-payment reconciliation — catching issues after the fact is too late.

KEY TAKEAWAY 03

Strong Security Practices

Protect Data & Your Team

Strong security standards protect your agency, your vendors, and your team.

GDPR

SOC 2

HIPAA

KEY TAKEAWAY 3 • SECURITY & COMPLIANCE

Security Practices That Keep You Audit-Ready

SOC 2 Type II	SOC 2 Type II certification means a vendor's security controls have been independently verified over time — not just assessed once. When evaluating any supplier management solution, require SOC 2 Type II as a minimum standard.	**Impact:** Reduces audit risk and satisfies security review requirements from your own IT and legal teams.
GDPR Alignment	Data minimization, right-to-erasure workflows, and consent management are built in — critical for institutions managing international supplier relationships or EU-based vendors.	**Impact:** Protects against regulatory fines and reputational damage from mishandled PII.
HIPAA Considerations	For healthcare-adjacent agencies and university medical centers, any platform handling supplier records with PHI must support HIPAA-compliant data handling — confirm this explicitly before onboarding any vendor management tool.	**Impact:** Allows procurement teams to onboard healthcare vendors without creating compliance gaps.

KEY TAKEAWAY 3 • PII PROTECTION

Protecting PII Without Slowing Down Operations

The PII Risk in Procurement

- W-9 forms contain SSNs — emailed, stored in shared drives
- Supplier contacts include personal email, home addresses
- Manual processes mean sensitive data handled by multiple staff
- No centralized audit log of who accessed what, when
- Breaches result in regulatory penalties AND reputational damage

Best Practice Controls for PII

- Suppliers enter sensitive data directly — never passes through staff hands
- Encrypted at rest and in transit; no email handling of W-9s
- Role-based access controls limit who can see what
- Full audit trail of every data access and validation event
- Automated retention and purge workflows reduce long-term storage risk

About Relish

AI-Powered Procurement Intelligence for the Public Sector

What We Do

Relish extends existing ERP systems (Workday, SAP, Coupa & ServiceNow) with AI-powered supplier data management and payment controls. We don't replace your system — we make it smarter.

Data Assure Supplier

Our flagship product automates supplier onboarding, continuous validation, bank account verification, and compliance monitoring — all within your existing ERP workflow.

Invoice AI

AI-powered invoice processing that reads invoices from any source, in any format — eliminating manual data entry, reducing errors, and integrating directly into your existing AP workflow.

Data Assure HR

Extends Data Assure into Workday HR — validating worker banking details, tax forms, and identity during onboarding and job changes to prevent payroll fraud and improper payments.

Data Assure: How It Works

1

Supplier Invited

Procurement sends an automated invite through your ERP — no manual email required.

2

Data Collected

Supplier enters their information directly — tax IDs, W-9s, banking details, certifications.

3

Validation Runs

AI engines verify identity, check debarment lists, validate bank accounts, and screen for risk.

4

Results in ERP

Validated supplier record is written back into Workday/SAP/Coupa — fully documented and audit-ready.

5

Continuous Monitoring

Ongoing re-validation alerts you to changes in status, ownership, or risk indicators.

Relish SOLUTION • INTEGRATIONS

Works Inside Your Existing ERP

No rip-and-replace. Relish extends your current system with AI-powered controls.

Workday

Primary focus — Workday Financials & Sourcing (SRM)

SAP / Ariba

Full integration with SAP procurement workflows

Coupa

Supplier portal and payment control extension

ServiceNow

Embedded in Supply Lifecycle Operations (SLO) — Key partner

LET'S ADDRESS THE ELEPHANT IN THE ROOM

Questions We Hear — And Our Honest Answers

"We already do manual checks — isn't that enough?"

Manual checks are a single point-in-time snapshot. A vendor cleared in January can be debarred in March. Automated continuous monitoring catches what a one-time check misses — and gives you a paper trail that manual processes never can.

"Our ERP already handles supplier management."

ERPs are great transaction engines — but they weren't designed to validate bank account ownership, screen against verifications in real time, or auto-collect W-9s. Data Assure is the missing compliance layer your ERP vendor never built.

"We don't have budget for new software right now."

One improper payment, one audit finding, or one fraud incident typically costs far more than the annual licensing fee. Through Carahsoft, there are contract vehicles that streamline approval and often fit within existing IT or audit budgets.

"Implementation sounds like a big project."

Most implementations go live in 8 weeks. There's no rip-and-replace — Data Assure connects directly to your existing ERP. The system adds a defensible compliance layer underneath it.

NEXT STEPS

The Time to Act Is Before Your Next Audit

Why Act Now?

- Audit cycles don't wait — compliance gaps identified during reviews are costly and public
- Manual processes become more fragile as staff turnover increases
- Fraud tactics are evolving faster than manual detection can respond
- Carahsoft contract vehicles make procurement fast and compliant
- Implementation timeline is weeks, not months

Your Next Steps

01 Request a personalized demo with the Relish team

02 Review available Carahsoft contract vehicles for quick procurement

03 Identify 2–3 pain points from today's session to explore further

04 Connect with Doug Carlson directly — he knows your world

RESOURCES

Learn More About Relish

Carahsoft Relish Page

carahsoft.com/relishiq

Browse Relish resources, contract vehicles, and contact information through our Carahsoft partnership page.

Data Assure Product Overview

Relishiq.com/data-assure

Detailed product information, feature breakdowns, and integration guides for Workday, SAP, Coupa, and ServiceNow.

Book a Demo

https://relishiq.com/get-started/

Schedule a personalized walkthrough with the Relish team. See Data Assure in action for your use case.

Webinar Recording

https://relishiq.com/webinars

This recording and slides will be available on our website following today's session.

Why Carahsoft Makes This Easy

Carahsoft is The Trusted Government IT Solutions Provider® — serving 15,000+ public sector agencies since 2004 through pre-competed contract vehicles.

No Lengthy RFP Process

Relish is available through Carahsoft's existing contract vehicles. That means no sole-source justification needed, and a dramatically faster procurement cycle.

Contract Vehicles

Available via GSA, NASPO ValuePoint and state-level cooperative contracts.

Procurement Support

Carahsoft's team handles the procurement logistics — order processing, licensing, invoicing — so your team focuses on implementation, not paperwork.

Education & SLED Specialist

Carahsoft's education and state/local government team has deep experience navigating the unique procurement rules for universities and public agencies.

Q&A

Thank you for joining us today!

DOUG CARLSON

Head of Regulated Industries

doug@Relishiq.com

DAN PARK

Head of Sales – Workday

dan@Relishiq.com