VASQUEZ
+ COMPANY LLP
Certified Public Accountants and Consultants

Internal Controls for Small Staff

Practical, Sustainable, and Right-Sized for Your District

Roger Martinez, CPA
Partner, Audit Practice Leader

Tonette Santillan, CPA, CGMA
Partner, Outsourcing Practice Leader

Michelle De Guzman
Director, Technology Services

What You'll Walk Away With

By the end of this session, you'll have practical tools to:

1

Build a stronger control environment

Learn the COSO framework and its five components

2

Strengthen oversight with a small team

Implement segregation of duties and compensating controls

3

Reduce cyber and fraud risk

Apply high-impact controls such as MFA, RBAC, and audit trails

4

Better oversee vendors and service providers

Understand SOC reports and management's oversight responsibilities

5

Put ideas into action immediately

Use practical tools and checklists designed for small districts

2026 CSDA ANNUAL CONFERENCE & EXHIBITOR SHOWCASE

The Reality Check

WHAT ACCOUNTING FRAMEWORKS OFTEN ASSUME:

- Dedicated accounting department
- Separate staff for each function
- Full-time IT support
- Internal audit team

WHAT MANY SPECIAL DISTRICTS ACTUALLY HAVE:

- **1–3 finance staff**
  sometimes the same person who also handles HR or admin
- **Shared bookkeeping support**
  part-time or shared
- **A board that wants assurance**
  needs plain and simple explanations
- **A limited budget**
  for tools or outside support

Concerns Across District Organizations

Which of these concerns you most right now?

FRAUD RISK

Fraud or misappropriation that no one catches in time.

AUDIT FINDINGS

An audit finding that requires corrective action by the board or district.

CYBERSECURITY

A cybersecurity incident that disrupts operations or exposes data.

KNOWLEDGE LOSS

A key person leaves and takes all the institutional knowledge with them.

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

A framework for designing, implementing, and evaluating internal controls.

What Is COSO and Why Should You Care?

COSO = The ***gold standard*** for internal control design

CONTROL ENVIRONMENT

The tone at the top. Does your board and management model integrity? Does staff know what is expected?

RISK ASSESSMENT

What could go wrong? How likely is it? How bad would it be? Have you talked about it?

CONTROL ACTIVITIES

The actual policies, approvals, and procedures that prevent or detect problems.

INFORMATION & COMMUNICATION

Are the right people getting the right financial information at the right time?

MONITORING

Is someone checking whether the controls are actually working?

***References:**

- **COSO Internal Control Guidance Page -** COSO Internal Control – Integrated Framework
- **COSO Internal Control Resource Center -** COSO Internal Control Resources

COSO Mapped to Your District

COSO Component	Small District Practical Application
1 CONTROL ENVIRONMENT	Board ethics policy, written delegation of authority, staff training on expectations.
2 RISK ASSESSMENT	Annual risk discussion at board meeting, documented top risks with mitigations.
3 CONTROL ACTIVITIES	Check signing limits, invoice approvals, bank reconciliations, payroll change approval.
4 INFORMATION AND COMMUNICATION	Monthly treasurer report, budget-to-actual reporting, audit findings communication.
5 MONITORING	Board finance committee review, annual audit, surprise petty cash counts, self-assessments.

SEGREGATION OF DUTIES WITH 2-6 PEOPLE

What Is Segregation of Duties (SoD)?

The four functions that must be separated:

1

AUTHORIZATION

Approving that a transaction should occur.

→

2

CUSTODY

Physical or electronic access to assets (cash, checks, bank accounts).

→

3

RECORDING

Enter it into the accounting system.

→

4

RECONCILIATION / REVIEW

Verify what was recorded matches what happened.

WHY IT MATTERS

- ✓ Reduces opportunity for undetected fraud or error.
- ✓ Creates a natural second set of eyes on every process.
- ✓ Required by auditors and the California State Controller's Office.
- ✓ Protects your staff from false accusations - control is also a defense.

The SoD Challenge: What If I Only Have Three People?

When perfect segregation is not possible, compensating controls provide additional oversight that reduces risk to an acceptable level.

THE THREE COMPENSATING CONTROLS FOR SMALL DISTRICTS:

1

INDEPENDENT MANAGEMENT REVIEW

A supervisor or board member reviews transactions completed by staff, looking for anomalies.

2

DUAL AUTHORIZATION

Two people must approve or sign off before a transaction is processed.

3

EXCEPTION REPORTING

System-generated reports that flag unusual activity for review by someone independent of the transaction.

SoD Matrix: A Quick Reference Tool

PROCESS	MINIMUM SEPARATION	IF ONLY 1 PERSON AVAILABLE
CASH RECEIPTS	Collector separate from depositor and reconciler	Lockbox + independent bank statement review
ACCOUNTS PAYABLE	Requester separate from approver and payment processor	GM approval threshold + 3-way match + Positive Pay
PAYROLL	HR authorization separate from payroll processing	Written change approvals + periodic roster review
JOURNAL ENTRIES	Preparer separate from approver	Documentation requirement + supervisory review
VENDOR SETUP	Requester separate from approver	Vendor change approval form signed by non-AP person

**See Appendix for details*

Board and Management Oversight as a Control

In a small district, the board IS the internal audit function.

Board-level controls that work:

- Monthly review of treasurer's report and budget-to-actual comparison.
- Board members reviewing bank statements directly from the bank (online access).
- Rotating board members to conduct surprise petty cash counts.
- Requiring dual signatures on checks above a defined threshold.
- Annual board review and approval of the internal control policy.
- Finance committee that meets quarterly to review controls and risk.

Small District Practical Application

- General Manager approves all payments above a defined dollar threshold.
- GM reviews bank reconciliations before they are filed.
- GM conducts an annual review of system user access.

IT CONTROLS AND CYBERSECURITY QUICK WINS

Why IT Controls Matter for Small Districts

Small districts are not small targets.

- Attackers target local governments for a reason: aging systems, thin IT staff, and publicly posted leadership contacts.
- Business email compromise (BEC) - impersonating executives to redirect payments - is the fastest-growing financial fraud in the public sector.
- One phishing email can expose your entire financial system.

The good news: the highest-impact controls cost little or nothing.

Two frameworks right-sized for your district:

1 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0

Released Feb 2024. Built for organizations of every size. Six functions: Govern, Identify, Protect, Detect, Respond, Recover.

2 Center for Internet Security (CIS) Controls v8.1, Implementation Group 1 (IG1)

The baseline every organization should implement. Your essential cybersecurity starter kit.

Quick Wins at a Glance

Four low-cost controls you can put in place this quarter:

Multi-Factor Authentication (MFA)

Blocks 99%+ of password attacks. Enable on email first, then finance, banking, and payroll.

Role-based Access control (RBAC)

Least privilege; each user gets only what the job needs. Enforce Joiner-Mover-Leaver.

Electronic approvals

Timestamped, searchable, tamper-evident records. Switch on your accounting system's routing.

Vendor change alerts

Confirm banking changes by callback; separate who edits vendors from who pays them.

Together they close the gaps attackers exploit most at little or no cost.

NIST CSF 2.0 Mini Profile for Small Districts

NIST CSF 2.0: Six functions that can be applied to your district

1 Govern

Board approves the cybersecurity policy;
GM is accountable; roles defined.

2 Identify

Inventory your systems, software, and sensitive data (resident PII, financials, utility accounts).

3 Protect

MFA enabled. RBAC configured. Backups running.
Staff trained on phishing.

4 Detect

Review system security alerts; keep an IT support number for when something looks wrong.

5 Respond

Keep a simple written plan: who to call on a suspected breach (IT, bank, legal, CISA).

6 Recover

Test backups. Know your restore time.
Document recovery steps.

CIS Controls IG1: Your Baseline Checklist

CIS Controls v8.1 - Implementation Group 1 (IG1)

The essential controls for every organization, regardless of size.

Top 10 IG1 actions for small districts:

1. Inventory all hardware connected to district systems
2. Inventory all software in use
3. Keep software and operating systems patched (enable automatic updates)
4. Enable MFA on all accounts reaching sensitive systems
5. Configure role-based access; remove unnecessary permissions
6. Require strong, unique passwords (use a password manager)
7. Enable automatic screen lock after inactivity
8. Run automatic backups and test them regularly
9. Train all staff annually on phishing and social engineering
10. Document how to report a suspected security incident

USING EXTERNAL SUPPORT WITHOUT LOSING CONTROL

Outsourcing as a Control Strategy

For small districts, external support is not a luxury - it is often the most cost-effective control available.

What you can outsource:

- ✓ Payroll processing (ADP, Paychex, MuniServices)
- ✓ Accounts payable processing
- ✓ Bank lockbox services
- ✓ IT managed services and helpdesk
- ✓ Internal audit or co-sourced audit services
- ✓ Accounting and bookkeeping (outsourced finance department)
- ✓ Shared services through your county or a JPA (Joint Powers Authority)

What you must never outsource:

- ✗ Management's responsibility for controls
- ✗ Board oversight and governance
- ✗ Review and approval of financial reports
- ✗ Oversight of vendors and service providers

Key principle: **Outsourcing transfers the execution of a task - it never transfers accountability.**

What Is a SOC Report and Why Should Districts Care?

SOC = System and Organization Controls

Reports issued by independent CPA firms about the controls in place at a service organization (e.g., your payroll provider, your utility billing system, your cloud software vendor).

SOC 1
FINANCIAL-REPORTING IMPACT

USE WHEN

Vendors process transactions or data relevant to the district's financial statements.

EXAMPLES

Payroll providers, accounts payable processors, loan servicers, utility billing processors.

REVIEW Control objectives, tests, exceptions, complementary user entity controls, and period coverage.

SOC 2
SECURITY AND DATA PROTECTION

USE WHEN

Vendors store, process, or transmit sensitive district data or host key systems.

EXAMPLES

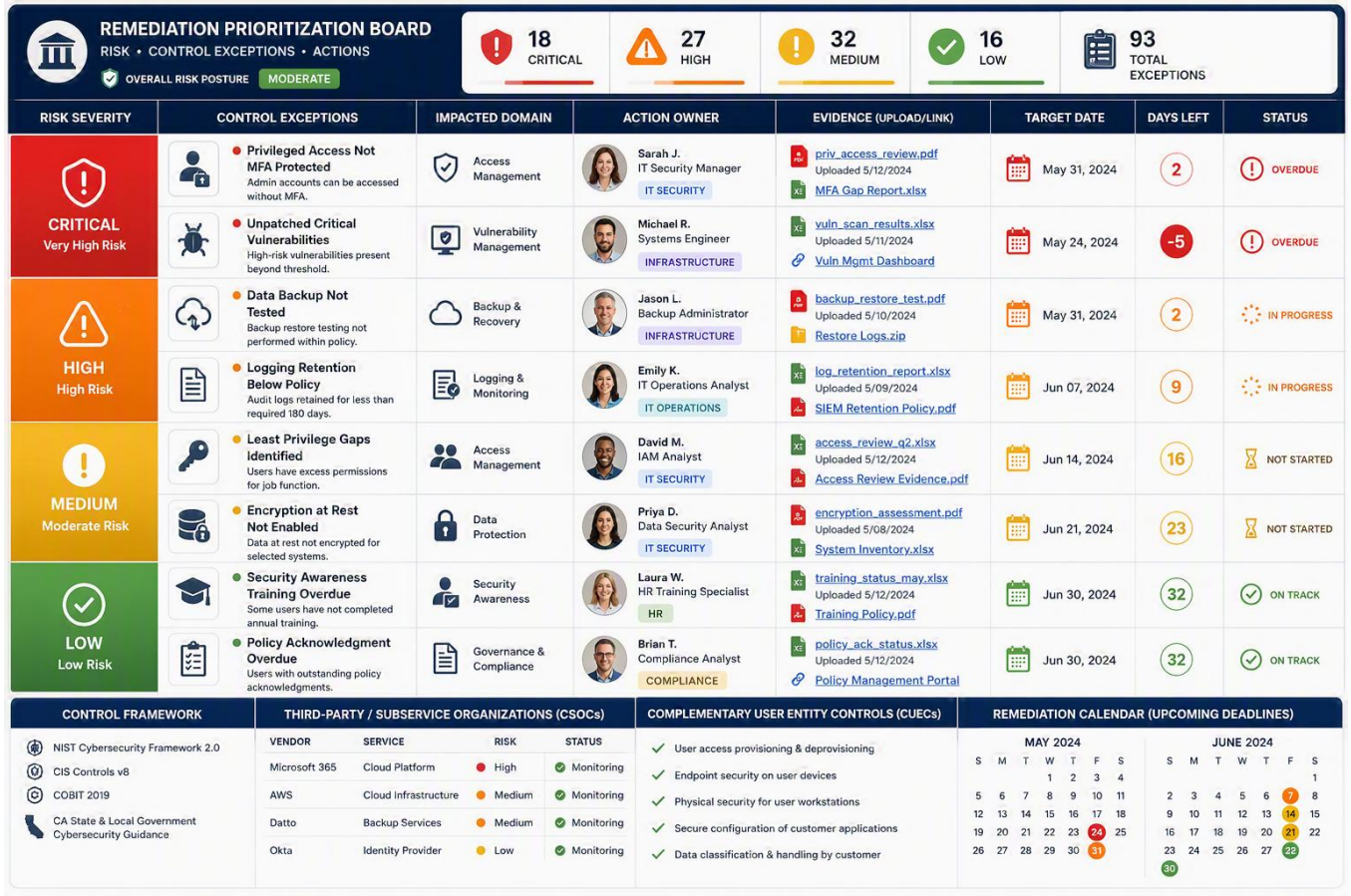
Cloud ERP, managed IT, SaaS, call centers, document platforms.

REVIEW Trust Services Criteria results, scope, subservice organizations, exceptions, and CUECs.

TIP: For critical vendors, request both if both financial-reporting and data-security risk exist.

Important SOC report sections to review

The opinion page is only the starting point — control owners should review deeply.



REMEDIATION PRIORITIZATION BOARD
RISK • CONTROL EXCEPTIONS • ACTIONS
OVERALL RISK POSTURE: MODERATE

18 CRITICAL | 27 HIGH | 32 MEDIUM | 16 LOW | 93 TOTAL EXCEPTIONS

RISK SEVERITY	CONTROL EXCEPTIONS	IMPACTED DOMAIN	ACTION OWNER	EVIDENCE (UPLOAD/LINK)	TARGET DATE	DAYS LEFT	STATUS
CRITICAL Very High Risk	Privileged Access Not MFA Protected — Admin accounts can be accessed without MFA.	Access Management	Sarah J., IT Security Manager, IT SECURITY	priv_access_review.pdf, Uploaded 5/12/2024; MFA Gap Report.xlsx	May 31, 2024	2	OVERDUE
	Unpatched Critical Vulnerabilities — High-risk vulnerabilities present beyond threshold.	Vulnerability Management	Michael R., Systems Engineer, INFRASTRUCTURE	vuln_scan_results.xlsx, Uploaded 5/11/2024; Vuln Mgmt Dashboard	May 24, 2024	-5	OVERDUE
HIGH High Risk	Data Backup Not Tested — Backup restore testing not performed within policy.	Backup & Recovery	Jason L., Backup Administrator, INFRASTRUCTURE	backup_restore_test.pdf, Uploaded 5/10/2024; Restore Logs.zip	May 31, 2024	2	IN PROGRESS
	Logging Retention Below Policy — Audit logs retained for less than required 180 days.	Logging & Monitoring	Emily K., IT Operations Analyst, IT OPERATIONS	log_retention_report.xlsx, Uploaded 5/09/2024; SIEM Retention Policy.pdf	Jun 07, 2024	9	IN PROGRESS
MEDIUM Moderate Risk	Least Privilege Gaps Identified — Users have excess permissions for job function.	Access Management	David M., IAM Analyst, IT SECURITY	access_review_q2.xlsx, Uploaded 5/12/2024; Access Review Evidence.pdf	Jun 14, 2024	16	NOT STARTED
	Encryption at Rest Not Enabled — Data at rest not encrypted for selected systems.	Data Protection	Priya D., Data Security Analyst, IT SECURITY	encryption_assessment.pdf, Uploaded 5/08/2024; System Inventory.xlsx	Jun 21, 2024	23	NOT STARTED
LOW Low Risk	Security Awareness Training Overdue — Some users have not completed annual training.	Security Awareness	Laura W., HR Training Specialist, HR	training_status_may.xlsx, Uploaded 5/12/2024; Training Policy.pdf	Jun 30, 2024	32	ON TRACK
	Policy Acknowledgment Overdue — Users with outstanding policy acknowledgments.	Governance & Compliance	Brian T., Compliance Analyst, COMPLIANCE	policy_ack_status.xlsx, Uploaded 5/12/2024; Policy Management Portal	Jun 30, 2024	32	ON TRACK

CONTROL FRAMEWORK
- NIST Cybersecurity Framework 2.0
- CIS Controls v8
- COBIT 2019
- CA State & Local Government Cybersecurity Guidance

THIRD-PARTY / SUBSERVICE ORGANIZATIONS (CSOCs)

VENDOR	SERVICE	RISK	STATUS
Microsoft 365	Cloud Platform	High	Monitoring
AWS	Cloud Infrastructure	Medium	Monitoring
Datto	Backup Services	Medium	Monitoring
Okta	Identity Provider	Low	Monitoring

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)
- User access provisioning & deprovisioning
- Endpoint security on user devices
- Physical security for user workstations
- Secure configuration of customer applications
- Data classification & handling by customer

REMEDIATION CALENDAR (UPCOMING DEADLINES)

MAY 2024

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

JUNE 2024

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	22	
30						

Opinion Type

Clean, qualified, adverse, or disclaimer—read what the auditor actually concluded.

Scope + Period

Confirm that services, systems, locations, and the report period cover the district's reliance.

Tests + Exceptions

Identify failed controls, population limits, management responses, and impact.

Complementary User Entity Controls (CUECs)

Map user-entity responsibilities and subservice assumptions to district controls.

CUECs: the most overlooked accountability gap

A clean vendor opinion does not mean your district did its part.

What CUECs are

Controls that the vendor assumes the user entity will implement so the vendor's controls can meet their objectives.

Common District CUECs

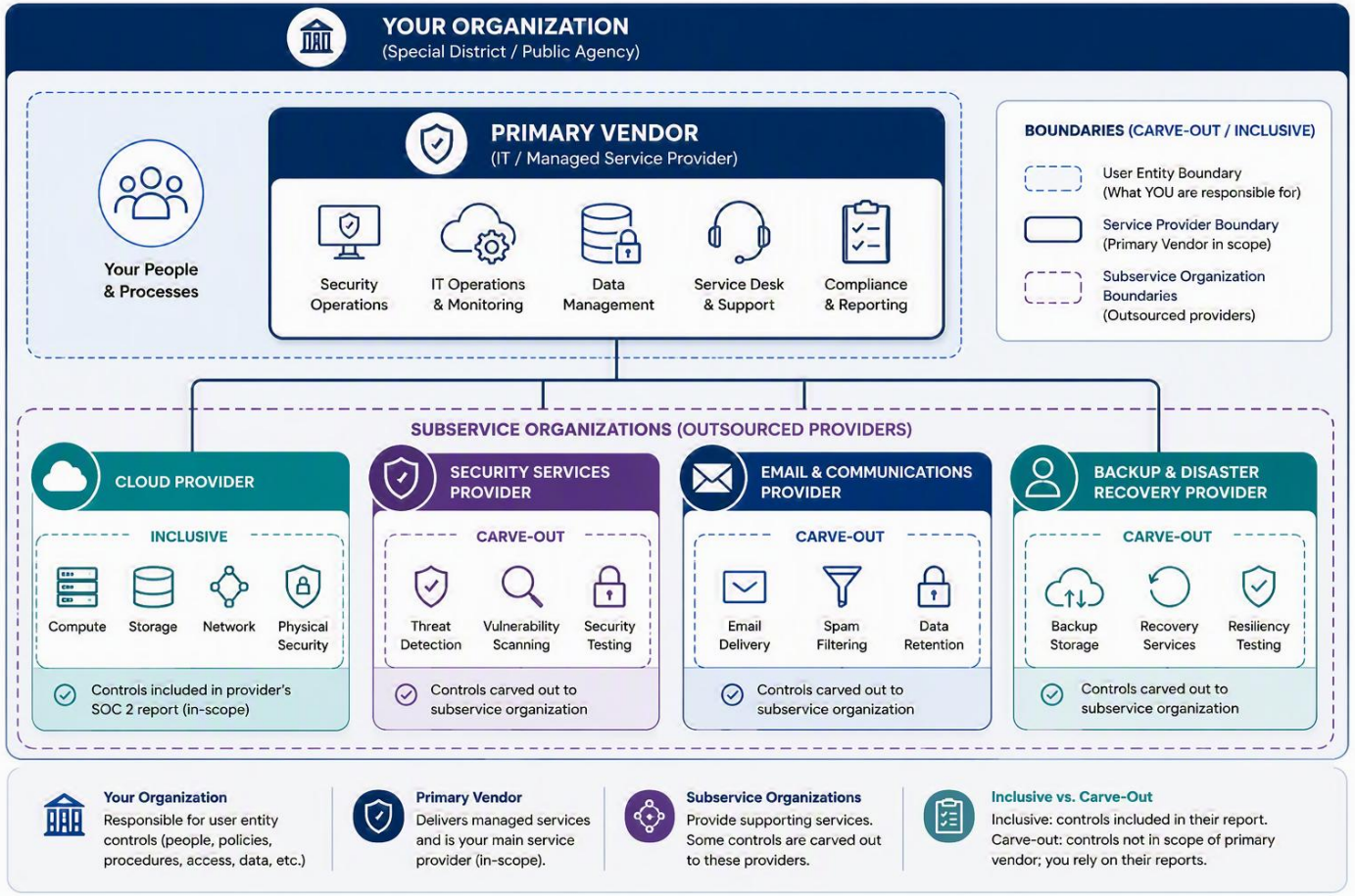
User provisioning/deprovisioning; Approval of payroll or AP data; Access reviews; Report review; Data classification; Incident notification; Secure configuration.

Control Owner Mandate

Every CUEC should have an owner, frequency, evidence, due date, and status. Unowned CUECs become control gaps.

Subservice organizations: Don’t stop at the Primary Vendor

Understand the control chain, especially carve-out vs. inclusive treatment



Carve-out Method

Subservice controls are excluded from the primary vendor’s testing. You may need the subservice SOC report or other assurance.

Inclusive Method

Subservice controls are included in the report scope. Still review related control tests and exceptions.

Complementary Subservice Controls (CSOCs)

The primary vendor may assume subservice organizations operate controls that are necessary to meet the primary vendor’s control objectives.

If a critical function is delegated twice, assurance must follow the chain.

2026 CSDA ANNUAL CONFERENCE & EXHIBITOR SHOWCASE

Annual SOC review workflow for Control Owners

A practical cadence that turns a report into oversight evidence.

1. Inventory

Identify vendors where SOC assurance is expected: Payroll, ERP, Billing, Banking, SaaS, Managed IT.

2. Request

Obtain current SOC report, bridge letter if needed, subservice reports if carved out, and NDAs if required.

3. Review

Assign finance/IT owners to review opinion, scope, period, exceptions, CUECs, and subservice organizations.

4. Map

Document each CUEC/CSOC dependency to district controls, evidence, owner, and operating frequency.

5. Remediate

Prioritize gaps, track action owners, due dates, residual risk, and retest evidence.

6. Report

Summarize status for management, audit committee/board, and external auditors.

2026 CSDA ANNUAL CONFERENCE & EXHIBITOR SHOWCASE

CALIFORNIA TRANSPARENCY

California Transparency Expectations for Special Districts

Special districts in California operate under specific transparency and reporting obligations.
Required Financial Reports (per the California Special District Uniform Accounting and Reporting Procedures):

Audited Financial Statements — 12 MONTHS

Required under Government Code 26909. Due to SCO, County Auditor, and LAFCO within 12 months of fiscal year end.

Financial Transactions Report — 7 MONTHS

Due 7 months after fiscal year end (January 31 for June 30 districts). Required by Government Code 53891.

Government Compensation Report — APRIL 30

Annual compensation data due April 30. Required by Government Code 53890-53891.

Public Retirement System Report — IF APPLICABLE

Required only for districts that maintain a public retirement system. Due within 6 months of fiscal year end (December 31 for June 30 fiscal year districts).

Building Public Trust Through Transparency

Transparency is not just a compliance requirement - it is a governance value.

Your district website transparency page should include:

- Current and prior year audited financial statements (posted within 60 days of completion)
- Approved annual budget
- Board meeting agendas and minutes
- Current board member roster and contact information
- Staff directory
- A link to the California State Controller's Office transparency portal for your district's Financial Transactions Report
- Compensation schedule for district employees
- Strategic plan or vision document (if available)

WHY IT MATTERS | **Proactive transparency reduces Public Records Act requests, builds community trust, and demonstrates governance maturity to auditors and oversight bodies.**

Your Monthly Controls Tune-Up (About 15 Minutes to Verify Key Controls)

The most sustainable control is one that becomes a routine.

Monthly (Finance Staff 10 minutes)

- Bank reconciliations completed and reviewed by supervisor
- Budget-to-actual variance review completed
- Journal entry log reviewed for unusual entries
- Vendor master file: any changes this month? If yes, were they authorized?
- Payroll register reviewed against prior period for unusual changes

Monthly (General Manager or Treasurer 5 minutes)

- Bank statements reviewed (independently, not just from staff report)
- Sign off on bank reconciliation after staff completion
- Review credit card or purchasing card statement line by line
- Check user access report if available in your system

Board Monthly

- Review and accept treasurer's report in board minutes

2026 CSDA ANNUAL CONFERENCE & EXHIBITOR SHOWCASE

Your Action Plan: Leave With Three Things

Walk out of here today with three commitments:

THIS WEEK

- ✓ Enable MFA on email and financial systems
- ✓ Review user access in your accounting system - remove anyone who should not have access

THIS MONTH

- ✓ Complete the SoD Matrix for your district - identify your gaps and document compensating controls
- ✓ Start using the Monthly Controls Tune-Up Checklist

THIS QUARTER

- ✓ Request SOC reports from your top two vendors and review using the SOC Cheat Sheet
- ✓ Present a brief internal controls update to your board

Key Takeaways

Five practical principles for stronger district controls

1	**COSO is your foundation.**	Five simple questions about environment, risk, activities, communication, and monitoring. Apply them to your district's operations, reporting, and compliance.
2	**SoD is achievable with small staff.**	When perfect separation is not possible, compensating controls - independent review, dual authorization, documentation - close the gap.
3	**IT controls are affordable and high-impact.**	MFA, RBAC, audit trails, and vendor alert controls address most cyber and fraud risk at low or no cost.
4	**Outsourcing transfers tasks, not accountability.**	Review deliverables, request SOC reports, implement CUECs, and document your oversight.
5	**Consistency beats perfection.**	A simple monthly tune-up performed reliably is worth more than a complex control framework that no one actually uses.

Questions?

Thank you for joining us!

For session questions and follow-up discussions:

Roger Martinez, CPA

O: +1.213.873.1703 | M: +1.310.721.1286
ram@vasquezcpa.com

Roger M.

Tonette Santillan, CPA, CGMA

O: +1.213.873.1754 | M: +1.213.793.6292
tsantillan@vasquezcpa.com

Tonette S.

Michelle De Guzman

O: +1.213.873.1788 | M: +1.858.828.6385
mdeguzman@vasquezcpa.com

Michelle D.

VASQUEZ
+ COMPANY LLP
Certified Public Accountants and Consultants

Scan to learn more about Vasquez + Company

APPENDIX

1. SoD in Practice: Cash Receipts

Process: Cash Receipting

Risk: Misappropriation of cash; unrecorded receipts

Ideal Structure (3+ people):

- Person A: Opens mail, prepares cash receipt log, records in system
- Person B: Makes bank deposit
- Person C (or Board): Performs/reviews bank reconciliation

Small Staff Compensating Controls (1-2 people):

- Use a bank lockbox to remove cash handling from staff entirely
- Require daily deposit with timestamped receipts
- General manager or board treasurer reviews bank statements and deposit records monthly
- Retain batch reports and deposit slips as evidence

Key Evidence to Keep: Batch reports, deposit slips, bank reconciliation with reviewer signature

2. SoD in Practice: Accounts Payable

Process: Accounts Payable

Risk: Unauthorized or duplicate payments; fictitious vendors

Ideal Structure (3+ people):

- Person A: Initiates/requests purchase
- Person B: Approves purchase
- Person C: Processes payment
- Person D: Maintains vendor master file

Small Staff Compensating Controls:

- Require three-way match: purchase order + receiving confirmation + invoice before payment
- Vendor changes (new vendors, banking changes) require written approval from someone not in AP
- General manager approves all payments above a dollar threshold before processing
- Use Positive Pay with your bank to prevent altered or fraudulent checks
- Review open vendor list quarterly and remove inactive vendors

Key Evidence to Keep: Vendor change approval log, invoices with match documentation, signed payment approvals

3. SoD in Practice: Payroll

Process: Payroll

Risk: Unauthorized pay changes; ghost employees

Ideal Structure (3+ people):

- HR/Manager: Authorizes new hires, terminations, and pay changes
- Payroll Processor: Enters changes and runs payroll
- Independent Reviewer: Compares payroll register to authorized changes

Small Staff Compensating Controls:

- General manager reviews and signs off on a payroll change report before each pay run
- Board or board subcommittee reviews payroll register at least quarterly
- Use outsourced payroll (e.g., ADP, Paychex, MuniServices) with system-enforced change logs
- Require written new-hire and termination notices signed by someone other than the payroll processor
- Periodically compare payroll records to employee roster and HR files

Key Evidence to Keep: Payroll register, signed change authorization forms, periodic roster comparison results

4. SoD in Practice: Journal Entries

Process: Journal Entries

Risk: Inaccurate financial reporting; override of controls

Small Staff Compensating Controls:

- All journal entries require a written description of purpose before posting
- Supporting documentation must be attached to every non-standard entry
- Restrict system access so staff cannot post to certain accounts (e.g., retained earnings, interfund) without supervisor approval
- Finance director or general manager reviews all non-standard journal entries monthly
- Year-end adjusting entries require specific board or auditor approval

Key Evidence to Keep: Approved journal entry forms with supporting documentation, list of approvals.

Quick Win #1: Multi-Factor Authentication (MFA)

What it is: Requiring a second form of identity verification beyond a password when logging into systems.

Why it matters: According to CISA (Cybersecurity and Infrastructure Security Agency), MFA blocks over 99% of automated password-based attacks. A stolen password alone cannot access your system.

Where to implement it immediately:

- Email accounts (this is your highest priority)
- Financial accounting system
- Banking and investment portals
- Payroll system
- Any cloud-based systems with district data

How: Most platforms (Microsoft 365, Google Workspace, QuickBooks Online, etc.) offer MFA at no extra cost. Enable it in security settings. Prefer an authenticator app over SMS text codes for stronger protection.

Cost: Free to minimal

Quick Win #2: Role-Based Access Control (RBAC)

What it is: Configuring your software systems so each user can only access the functions and data their job requires - and no more.

The principle: Least privilege. Every user gets the minimum access needed to do their job.

- Practical examples for your district:
- The accounts payable clerk can enter invoices but cannot approve payments
- The payroll processor can run payroll but cannot add new employees or change pay rates
- Read-only access for board members who need to review reports
- System administrator access limited to one person (plus one backup)
- Former employees are removed from all systems immediately upon separation

The Joiner-Mover-Leaver (JML) process:

- **Joiner:** New employee gets only the access their role requires
- **Mover:** Employee changes roles - old access is removed, new access is granted
- **Leaver:** Employee departs - all access is removed on the last day (or before)

Quick Win #3: Electronic Approvals and Audit Trails

The problem with paper approvals:

- Easy to lose or alter
- No timestamp or automatic record
- Does not integrate with your accounting system
- Cannot be easily reviewed or searched

Electronic approval tools for small districts:

- **Email approvals with timestamp** - Simple, free, and creates an automatic record. Require approval confirmation by email for all purchases above threshold.
- **Built-in accounting system workflows** - Most modern platforms (Caselle, Tyler MUNIS, QuickBooks, Sage Intacct) have built-in approval routing. Turn these features on.
- **DocuSign or Adobe Sign** - Low-cost electronic signature tools that create a tamper-evident signed record.

What a good audit trail looks like:

- Who initiated the transaction and when
- Who approved it and when
- What supporting documentation was attached
- Whether any edits were made and by whom

Quick Win #4: Vendor Change Alert Controls

One of the most common fraud schemes: Vendor banking change fraud

An attacker (or insider) changes a vendor's banking information in your system. The next payment goes to a fraudulent account.

Low-cost controls that stop this:

- Require a written vendor change form signed by someone not in accounts payable
- Call the vendor directly (using a phone number from your existing records - not from the change request) to confirm any banking change
- Set up system alerts so that any change to a vendor record triggers an email notification to the finance director or general manager
- Limit who can make changes to the vendor master file - this should be a separate role from the person who processes payments
- Conduct a quarterly vendor master file review to look for duplicates, unusual entries, or inactive vendors with new banking details