troutman pepper locke

Privacy+ Security Forum

Cracking the CCPA Cybersecurity Audit Code

18 Reasons to Panic (But Don't)

10 Practical Implementation Tips Privacy and Cyber Professionals Need to Know Now

May 6, 2026

Agenda

01

PANEL OVERVIEW + PANELISTS

Who's in the room and why CCPA cybersecurity audits matter — now

02

REQUIREMENTS, FRAMEWORKS + MAPPING

Coverage, timing, five-framework comparison, auditor independence, and CCPA's 18 components

03

INDUSTRY ROUNDTABLE: 10 PRACTICAL TIPS

The implementation playbook from privacy, cyber, and audit leaders

04

KEY TAKEAWAYS + Q+A

What to do Monday morning

Panel Overview + Panelists

Who's in the room and why CCPA cybersecurity audits matter — *now*

troutman pepper locke

Meet the Panel

Panelists

Kyle Levine

Senior Lead
Privacy and Data Protection Office

Google

Hershel S. Eisenberger

Senior Director, Legal Counsel
Head of Privacy + Data Protection

The Coca-Cola Company

Dean Forbes

VP, Associate General Counsel
+ Chief Privacy Officer

DaVita

Moderator

Jim Koenig

Partner + Global Co-Leader
Privacy + Cyber + AI Practice

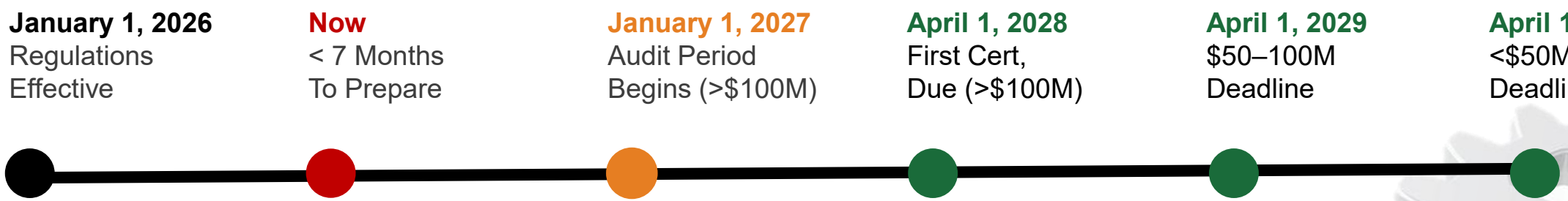
Troutman Pepper Locke LLP

Requirements, Frameworks + Mapping

Coverage, timing, five-framework comparison, and CCPA's 18 components

The Clock Is Ticking — Key Milestones

Audit period begins January 1, 2027 • Less than 7 months to have controls operational



⚠ **CRITICAL:** CalPrivacy and AG enforcement does **not** depend on certification submission dates.

Controls must be operational from January 1, 2027.
(11 Cal. Code Regs. § 7125; Cal. Civ. Code § 1798.185(a)(15))

Private Right of Action

$100–$750 per consumer per breach. Audit reports are DISCOVERABLE. A deficient audit = plaintiff's roadmap.
(Cal. Civ. Code § 1798.150(a)(1))

~30% Cost Reduction Available

CPPA Regulatory Impact Assessment: organizations with existing framework certifications can reduce costs by ~30%. (*CPPA Reg. Impact Assessment;* ***11 Cal. Code Regs. § 7121)***

The Five Frameworks Security Organizations Run On

CCPA explicitly permits leveraging existing audits — supplement, don't reinvent **(11 Cal. Code Regs. § 7121)**

CIS Controls v8.1

Closest to CCPA

18 prioritized controls by Implementation Groups (IG1–IG3). Closest analog to CCPA's 18 components. Requires 3 critical supplements: PI inventories, VDP, and phishing-resistant MFA scope for service providers.

NIST CSF 2.0

Explicitly Named

Explicitly named in CCPA regulations as an acceptable foundation. Risk-based structure across 6 functions (Govern, Identify, Protect, Detect, Respond, Recover). Requires PI classification and VDP supplement.

ISO/IEC 27001:2022

Strong Governance

Comprehensive ISMS; 93 controls in 4 themes. Third-party certification body required — which may satisfy CCPA independence requirements if audit scope alignment is confirmed.

NYDFS Part 500

Regulatory Model

Most prescriptive framework; sector-limited to NY financial services. Class A companies (>$20M revenue AND either more than 2,000 employees or more than $1 billion in total revenue (both counting affiliates)) require annual external audit. Strong MFA mandate (Nov 2025). Useful enforcement benchmark for CCPA.

SOC 2 Type II + PCI DSS

Widely Held

SOC 2 Type II is the most widely-used third-party attestation and can satisfy most CCPA evidence and independence requirements with supplementation. PCI data maps are directly reusable for PI scoping. PCI annual ROC for Level 1 or SA for lower (quarterly pen testing); SOC 2 recertification every 3 years with annual surveillance audit.

Who Is Covered — Applicability Thresholds

CCPA applies to ANY business meeting the thresholds — unlike sector-specific laws. From bakeries to banks.

§ CCPA Reg. Cite: 11 Cal. Code Regs. § 7101 — "A business shall conduct a cybersecurity audit if it has annual gross revenues exceeding $26,625,000, and either: processes the personal information of 250,000 or more consumers or households; processes the sensitive personal information of 50,000 or more consumers; or derives 50% or more of annual revenues from selling or sharing consumers' personal information."

CCPA (California)	NIST CSF 2.0	NYDFS Part 500	CIS Controls v8.1	ISO 27001:2022
• (i) $26.625M+ revenue AND either: - 250K+ consumers' PI OR - 50K+ sensitive PI • (ii) 50%+ revenue from selling PI	• Voluntary framework • No mandatory thresholds • Applicable to all organizations	• Entities under NY DFS license • Banks, insurers, money transmitters, • licensed lenders only	• Voluntary framework • Scalable via Implementation Groups • IG1–IG3 by org risk profile	• Voluntary international standard • Any org seeking ISMS certification • 93 controls in 4 themes

Three Critical Gaps — Even Mature Programs Must Address:

1. **PI Inventories + Classification:** CCPA-specific PI/SPI definitions require more than standard asset inventory. Map by CCPA category, location and third-party flow.
2. **VDP / Bug Bounty:** Not required by CIS-18, NIST, or NYDFS. CCPA mandates a formal vulnerability disclosure processes with safe harbor, submission mechanism, and 48-hr SLA. A public VDP or bug bounty program are examples of how to comply.
3. **Phishing-Resistant MFA Scope:** Must cover employees, contractors, AND service providers using FIDO2/WebAuthn or hardware tokens.

troutman pepper locke

Auditor Independence Requirements

§ CCPA Reg. Cite: 11 Cal. Code Regs. § 7122 — "The cybersecurity audit shall be conducted by a qualified, objective, and independent professional who is familiar with both cybersecurity and how to audit a cybersecurity program, and who uses procedures and standards generally accepted in the auditing profession. The auditor shall not have participated in the design, implementation, or operation of the cybersecurity program being audited during the audit period."

CCPA	NIST CSF 2.0	NYDFS Part 500	CIS Controls v8.1	ISO 27001:2022
INTERNAL OR EXTERNAL auditor permitted. • Must be 'qualified, objective, independent. • Cannot have developed or maintained the program being audited.	**SELF-ASSESSMENT PERMITTED.** • Third-party assessment optional — • No mandate. • Recommended for credibility only.	• **EXTERNAL INDEPENDENT AUDIT ANNUALLY FOR CLASS A companies** • (>$20M NY revenue + either >2,000 employees or >$1B) require an audit. • Others: internal with independence permitted.	**NO MANDATORY EXTERNAL AUDIT requirement.** • Third-party validation via CIS benchmarks available. • Self-assessment Typical.	**ACCREDITED THIRD-PARTY CERTIFICATION BODY REQUIRED.** • Stage 1 + 2 audits mandatory. • Annual surveillance audits; **Recertification Every 3 Years**.

Three Points That Matter Most:

1. **Reporting Line**: Internal auditors MUST report to an executive WITHOUT direct cybersecurity program responsibility. That executive — not the CISO — controls auditor performance reviews and compensation.
2. **Dress Rehearsal Model**: Large organizations use BOTH. Internal audit (often co-sourced with accounting firms) builds the evidence repository; third-party auditors perform the formal audit.
3. **Familiar Territory**: Independent audit requirements already exist under FTC consent decrees, NYDFS Part 500, HIPAA, and the DOJ Data Security Program. CCPA's standard is familiar — not novel.

CCPA's 18 Components: Five-Framework Mapping

= Net-new gap = CCPA stricter

Underline / CAPS = key word difference between this framework and CCPA | No underline = substantially similar

#	CCPA Component	NIST CSF 2.0	NYDFS Part 500	CIS Controls v8.1	ISO 27001:2022
1	**Multi-Factor Auth (§7123(c)(1))** Phishing-resistant MFA required for employees, contractors, and SERVICE PROVIDERS Strong passwords required unless business uses password-less auth	PR.AA-3: Authentication & access mgmt. MFA supported. NO SPECIFIC TECHNOLOGY OR SCOPE MANDATE — details left to organization.	§500.12: Universal MFA mandated Nov 2025. Strongest existing framework MFA requirement. [Does not explicitly extend to service providers.]	CIS 6 (6.3–6.5): MFA for privileged accounts. SERVICE PROVIDER SCOPE MAY NOT BE REQUIRED.	A.8.5 / A.5.15: Secure authentication. METHOD AND SCOPE LEFT TO INDIVIDUAL RISK ASSESSMENT.
2	**Encryption (§7123(c)(2))** Both at-rest and in-transit required. No specific encryption standard mandated.	PR.DS-1, PR.DS-2: Data security controls. Encryption supported; flexible technology standards.	§500.15: Encryption of nonpublic information; covers both at-rest and in-transit.	CIS 3 (3.6, 3.9–11): Data protection; encryption and key management practices.	A.8.24: Use of cryptography; A.5.14: Info transfer controls. Standard-agnostic.
3	**Account Management & Access Controls (§7123(c)(3))** Least-privilege access, limiting and monitoring privileged accounts, restricting PI access to those who need it. Explicitly includes restriction and monitoring of PHYSICAL ACCESS to personal information — often overlooked in traditional IAM programs.	PR.AA-1 through PR.AA-6: Identity & access management. Strong IAM coverage.	§500.7: Access privileges and management. Privileged access controls required.	CIS 5 & 6: Account & Access Control Management. PHYSICAL ACCESS TO PI NOT SEPARATELY ADDRESSED as a distinct access control requirement.	A.5.15–18, A.8.2–5: Access control & user access management.
4 ★	**PI Inventories (§7123(c)(4))** — NET-NEW Must inventory ALL CA PI/SPI by CCPA-defined categories. Map storage, data flows, and all third-party access.	ID.AM-1/2: General asset inventory only. SUPPLEMENT: Add CCPA PI/SPI category tagging and California-specific data flow mapping.	§500.13: General asset inventory. SUPPLEMENT: Add PI classification using CCPA PI/SPI definitions.	CIS 1,2,3: Hardware, software & data inventory (general). SUPPLEMENT: Build CCPA PI data map with category tagging and cross-border flow tracking.	A.5.9/A.5.12-13: Info classification (general). SUPPLEMENT: Add CCPA PI/SPI category classification and third-party flow documentation.

CCPA's 18 Components: Five-Framework Mapping

= Net-new gap = CCPA stricter

Underline / CAPS = key word difference between this framework and CCPA | No underline = substantially similar

#	CCPA Component	NIST CSF 2.0	NYDFS Part 500	CIS Controls v8.1	ISO 27001:2022
5	**Secure Configuration (§7123(c)(5))** Hardening, patch management, change management, and masking of sensitive PI where appropriate. Covers on-premises and cloud environments.	PR.PS-1: Configuration management processes. Hardening and change control well-covered.	§500.2(b): Cybersecurity program requirements include configuration standards and patching.	CIS 4 (4.1–4.12): Secure configuration for enterprise assets and software. Strong alignment.	A.8.9: Configuration mgmt; A.8.8: Technical vulnerability mgmt. Patch management.
6 ★	**Vulnerability Scanning, Penetration Testing & Disclosure (§7123(c)(6))** — NET-NEW Internal and external vulnerability scans, penetration testing; covers all third-party and cloud environments. Vulnerability disclosure programs (including bug bounty and ethical hacking) are explicitly listed as implementation examples within this component. NO OTHER FRAMEWORK INDEPENDENTLY REQUIRES a formal disclosure program.	ID.RA-1: Asset vulnerabilities identified; DE.CM: Continuous monitoring for threats. NOT REQUIRED: No vulnerability disclosure or VDP requirement.	§500.5: Penetration testing & vulnerability assessments mandated annually. NOT REQUIRED: No vulnerability disclosure or VDP requirement.	CIS 7: Continuous Vulnerability Management — scan, prioritize, remediate. NOT REQUIRED: No vulnerability disclosure or VDP requirement.	A.8.8: Technical vulnerability management; A.5.7: Threat intelligence (PARTIAL ONLY). NOT SUFFICIENT — no stand-alone vulnerability disclosure requirement.
7	**Audit Logging (§7123(c)(7))** Centralized storage, retention & monitoring. Logs must support detection & investigation.	DE.CM: Continuous monitoring; PR.PS: Security logging. Log aggregation and review.	§500.14(a): Audit trail systems required. Maintain and review logs regularly.	CIS 8 (8.1–8.12): Audit Log Management — centralized logs, retention schedules, and analysis.	A.8.15: Logging activities; A.8.16: Monitoring activities. Retain logs per retention schedule.
8	**Network Monitoring (§7123(c)(8))** Detect unauthorized access, modification, or disclosure of PI. Bot-detection, IDS/IPS listed as examples — not mandates.	DE.CM-1: Network monitoring; PR.DS-2: Data in transit protection. Detection and response.	§500.14(b): Monitor activity of authorized users. Detect unauthorized access.	CIS 13: Network Monitoring and Defense — IDS/IPS, bot detection, traffic analysis.	A.8.20: Network security; A.8.21: Web services security. Monitoring and intrusion detection.
9	**Malware Defense (§7123(c)(9))** Deploy and maintain antivirus and anti-malware solutions across information systems.	PR.PS: Platform security; DE.CM: Detection processes. AV/anti-malware deployment covered.	IMPLIED under cybersecurity program requirements. NO DEDICATED SECTION — assumed baseline only.	CIS 10 (10.1–10.7): Malware Defenses — endpoint protection, AV, sandboxing, scanning.	A.8.7: Protection against malware. Anti-malware tools, updates, and user awareness.

CCPA's 18 Components: Five-Framework Mapping

= Net-new gap = CCPA stricter

Underline / CAPS = key word difference between this framework and CCPA | No underline = substantially similar

#	CCPA Component	NIST CSF 2.0	NYDFS Part 500	CIS Controls v8.1	ISO 27001:2022
10	**Segmentation (§7123(c)(10))** Segmentation via properly configured firewalls, routers, and switches. Reduces attack surface and limits lateral movement.	PR.DS: Data security; DE.CM: network configuration monitoring. Segmentation covered.	§500.2(b): Cybersecurity program controls. No specific segmentation mandate.	CIS 12: Network Infrastructure Management — network segmentation and architecture controls.	A.8.20: Network security — network segregation and perimeter controls.
11	**Port & Protocol Management (§7123(c)(11))** Limitation and control of ports, services, and protocols to reduce attack surface.	PR.PS: Platform security; DE.CM: network monitoring. Port/protocol management implied.	§500.2(b): Implied under infrastructure hardening requirements.	CIS 4 (4.4–4.5): Secure Configuration — disable unused ports, protocols, and services.	A.8.9: Configuration management; A.8.8: Technical vulnerability management.
12	**Cybersecurity Awareness (§7123(c)(12))** How business maintains CURRENT knowledge of evolving threats. CalPrivacy split awareness and training into [[TWO SEPARATE COMPONENTS]] — training alone DOES NOT satisfy this component.	PR.AT: Awareness programs. CCPA SPLIT AWARENESS AND TRAINING — MUST BE ASSESSED AS SEPARATE COMPONENTS.	§500.14(a)(3): AWARENESS AND TRAINING TREATED AS COMBINED. Annual cadence.	CIS 14: Security Awareness Training. CCPA REQUIRES AWARENESS AND TRAINING AS TWO INDEPENDENT COMPONENTS.	A.6.3: AWARENESS AND TRAINING COMBINED. Must track and assess separately for CCPA.
13	**Cybersecurity Education & Training (§7123(c)(13))** Second of TWO DISTINCT components under CCPA. Training for employees, contractors, and all persons with system access. Onboarding, annual, and post-breach training required.	PR.AT: Awareness and training programs. Comprehensive training coverage — good alignment.	§500.14(a)(3): Security awareness training required for relevant personnel annually.	CIS 14: Security Awareness Training — role-based training and awareness program requirements.	A.6.3: Information security awareness and training. Onboarding and periodic training required.
14	**Secure Software Development (§7123(c)(14))** Secure coding standards, code reviews, security testing in SDLC. Applies to internally developed and procured software.	PR.PS: Platform security; SSDF integration. Secure development lifecycle and code practices.	§500.8: Application security requirements and testing. SDLC security mandate.	CIS 16: Application Software Security — secure dev practices, code reviews, SAST/DAST testing.	A.8.25–31: Secure development lifecycle — design, coding, security testing, and deployment.

CCPA's 18 Components: Five-Framework Mapping

= Net-new gap = CCPA stricter

Underline / CAPS = key word difference between this framework and CCPA | No underline = substantially similar

#	CCPA Component	NIST CSF 2.0	NYDFS Part 500	CIS Controls v8.1	ISO 27001:2022
15	**Third-Party Risk (§7123(c)(15))** Oversight of service providers, contractors, and third parties. Vendors processing CA PI are WITHIN the audit's reach. CONTRACTUAL AUDIT COOPERATION with the business's cybersecurity audit required.	GV.SC: Supply chain risk management. Third-party security governance. NO AUDIT COOPERATION REQUIREMENT.	§500.11: Third-party service provider security and contract provisions. NO AUDIT COOPERATION REQUIREMENT.	CIS 15: Service Provider Management. Third-party risk assessment. NO AUDIT COOPERATION REQUIREMENT.	A.5.19–23: Supplier security and cloud services. Contractual requirements. NO AUDIT COOPERATION REQUIREMENT.
16	**Retention Schedules & Proper Disposal of Personal Information (§7123(c)(16))** Retention schedules and secure disposal of PI no longer needed. Existing schedules should be reviewed to confirm coverage of CCPA PI/SPI definitions specifically.	PR.DS: Data security; PR.IP: Information protection. Data lifecycle management.	§500.13(a)(2): Data retention & destruction policy. Secure disposal required.	CIS 3 (3.1, 3.4): Data protection — secure disposal and data retention controls.	A.8.10: Info deletion; A.7.14: Secure disposal of equipment and media.
17	**Security-Incident Response Management (§7123(c)(17))** Incident response program, documented procedures, response capabilities, and testing. Review of actual security incidents during the audit period. Audit report MUST SEPARATELY INCLUDE NOTIFICATION SAMPLES issued during the audit period (§7124(a)(9)) — a UNIQUE CCPA AUDIT REPORT REQUIREMENT not found in any comparison framework.	RS: Respond function (RS.MA, RS.AN, RS.CO, RS.MI). Comprehensive IR planning and capabilities. NO AUDIT-SPECIFIC NOTIFICATION SAMPLE REQUIREMENT.	§500.16: Incident response plan required with documented procedures and annual testing. NO AUDIT SAMPLE REQUIREMENT equivalent to CCPA.	CIS 17: Incident Response Management — IR plan, roles, communication, and testing.	A.5.24–28: Incident management & evidence collection. Forensic evidence handling.
18	**Business Continuity & DR (§7123(c)(18))** BC/DR plans, data-recovery capabilities, backups, and regular testing to ensure availability of PI during disruptions.	RC function: RC.RP, RC.CO. Recover function — plans, communications, and improvements.	§500.16(b)(6): Business continuity planning required as component of incident response plan.	CIS 11 (11.1–11.5): Data Recovery — backup processes, testing, and documented recovery plans.	A.5.29–30: ICT continuity; A.8.13–14: Backup and redundancy. Full BC/DR scope.

Industry Roundtable: 10 Practical Tips

The implementation playbook from privacy, cyber, and audit leaders

troutman pepper locke

1 Compliance Timeline + Audit Readiness

PRACTICAL PRACTITIONER TIP:

Start Your Gap Assessment Now — Not Later.

Waiting for certification deadlines is the most common and costly mistake.

- **Map all 18 CCPA components against current controls — confirm protection from unauthorized access, use, modification, destruction, disclosure, AND loss of availability.**
- Prioritize the 3 critical gaps: PI Inventories, VDP/Bug Bounty, and phishing-resistant MFA scope.
- Document existing controls with audit-ready evidence now — don't rely on memory before an audit.
- Conduct a gap assessment under attorney-client privilege before the formal audit creates a discoverable record of vulnerabilities.

REGULATORY REQUIREMENT

CCPA cybersecurity audits phase in over three years beginning with the largest organizations (>$100M revenue, audit period beginning Jan 1, 2027).

11 Cal. Code Regs. § 7125 — "A business with annual gross revenues exceeding $100,000,000 shall conduct its first cybersecurity audit for the audit period commencing January 1, 2027, and shall submit a written certification of completion to the Agency by April 1, 2028. A business subject to this article shall maintain a cybersecurity program consistent with the requirements of this article regardless of when the business's first audit certification is due."

Roundtable Discussion: With audit requirements coming into effect in 2028 for the largest companies, when should organizations start preparing?

troutman pepper locke

2

Leveraging Existing Security Frameworks

PRACTICAL PRACTITIONER TIP:

Leverage Existing Frameworks — Don't Reinvent

CCPA explicitly allows using existing audits. Supplement, don't replace.

- **NIST CSF 2.0 is explicitly named in CCPA regulations — use it as your primary foundation.**
- ISO 27001 and SOC 2 Type II audits can satisfy most CCPA requirements with targeted supplementation.
- PCI DSS data maps and GDPR transfer maps are directly reusable for CCPA PI scoping.
- Align audit schedules to minimize duplication and cost. CPPA estimates ~30% cost reduction with existing certifications.

REGULATORY REQUIREMENT

CCPA regulations explicitly permit using audits prepared under other frameworks (NIST CSF, ISO 27001, or CIS Controls) as the foundation for CCPA compliance. The key is demonstrating that scope, independence, and documentation requirements are fully satisfied.

11 Cal. Code Regs. § 7121 — "A business may use a cybersecurity audit, assessment, or evaluation prepared for another purpose — such as an audit based on NIST CSF, ISO/IEC 27001, or CIS Controls — to satisfy the requirements of this article, provided scope, independence, and documentation requirements are met".

Roundtable Discussion: Which framework(s) do you use? How Can Organizations Leverage Existing Frameworks?

troutman pepper locke

3

Personal Information (PI) Data Mapping

PRACTICAL PRACTITIONER TIP:

Prioritize PI Data Mapping — More Than Asset Inventory

The most underestimated requirement. CCPA demands PI-specific granularity.

- **Document all PI categories — general vs. sensitive per CCPA definitions. Apply CCPA exemptions (GLBA-regulated data, FCRA-regulated data) carefully.**
- Map ALL storage locations: on-premises, cloud, SaaS, third-party systems, end-user devices, and backups.
- Track data flows including cross-border transfers — leverage existing GDPR transfer maps.
- Implement data classification and tagging within systems. Review quarterly or upon material system changes

REGULATORY REQUIREMENT

The cybersecurity audit must assess how the business inventories and manages California PI and sensitive PI — including data flows — across all systems, including cloud and third-party environments the business does not own or operate.

11 Cal. Code Regs. § 7123(c)(4) — "Maintaining an inventory of the business's personal information and the information system, including data flows of personal information into, through, and out of the information system, and an inventory of the hardware and software components of the information system."

Roundtable Discussion: How is data mapping done at your company (and reasons? What Are the Emerging Best Practices on Data Mapping?

troutman pepper locke

4

Multi-factor Authentication (MFA) Scope

PRACTICAL PRACTITIONER TIP:

Expand MFA to ALL User Populations

CCPA requires phishing-resistant MFA for employees, contractors, AND service providers.

- **Inventory every user population with system access — the requirement explicitly extends to service providers. Most programs stop at employees.**
- Prefer phishing-resistant methods: FIDO2/WebAuthn, hardware tokens. Avoid SMS/push-based MFA where feasible.
- Prioritize rollout for privileged access and high-risk roles. Document compensating controls with CISO approval where complete rollout is not yet done.
- Vendor contracts must require phishing-resistant MFA for any service provider accessing systems that touch CA PI.

REGULATORY REQUIREMENT

Phishing-resistant multi-factor authentication (MFA) for employees and contractors is a core CCPA audit component. The regulations also require appropriate authentication measures for service providers — a scope broader than most existing MFA programs.

11 Cal. Code Regs. § 7123(c)(1) — "Authentication of users and devices accessing the information system, including multifactor authentication for all users, with phishing-resistant multifactor authentication for employees and contractors with access to the business's information system, and appropriate authentication measures for service providers."

Roundtable Discussion: How is MFA handled currently – is it "phishing-resistant"? How will you handle service provider requirements contractually?

troutman pepper locke

5 Vulnerability Disclosure Program (VDP)

PRACTICAL PRACTITIONER TIP:

Implement a Vulnerability Disclosure Process

CCPA explicitly requires such a process — often completely absent even in mature programs. Three examples:

- Publish a formal VDP on your website with clear scope and safe harbor language protecting good-faith security researchers.
- Establish a submission mechanism (HackerOne, Bugcrowd, or email). Define SLAs: 48-hour acknowledgment; severity-based remediation timelines.
- Consider a bug bounty program for high-risk applications. Document ALL reports received and remediation actions taken.
- Not required by CIS-18, NIST CSF, or NYDFS — one of three net-new capabilities most organizations must build from scratch.

REGULATORY REQUIREMENT

Vulnerability disclosure and reporting process — including bug bounty and ethical hacking programs as examples — are listed among the 18 components auditors must evaluate. This is not required by CIS-18, NIST CSF, or NYDFS and must be built net-new for most organizations.

11 Cal. Code Regs. § 7123(c)(6) — "Processes for internal and external vulnerability discovery, including vulnerability scanning, penetration testing, and vulnerability disclosure and reporting programs, such as bug bounty programs and ethical hacking programs, and processes for tracking and addressing known vulnerabilities."

Roundtable Discussion: Did you have a VDP or similar already? If not, how will you build the business case for VDP internally?

troutman pepper locke

6

Auditor Selection + Independence

PRACTICAL PRACTITIONER TIP:

Engage Auditors Early — Capacity Will Be Constrained

Start vetting auditors in 2026 for 2028 certifications. Qualified auditors will be scarce.

- **Verify independence: auditors cannot have developed or maintained the program being audited. Document this if using an advisory firm that also does audit work.**
- Document the auditor's cybersecurity expertise AND auditing methodology credentials (AICPA, ISACA, ISO-related standards).
- Internal audit is permitted if reporting to an executive without direct cybersecurity program responsibility. Consider co-sourcing with a Big 4 firm.
- Conduct a privilege-protected pre-audit assessment to identify gaps before the formal audit creates a discoverable record.

REGULATORY REQUIREMENT

The auditor must be qualified, objective, and independent — and must not have participated in designing or operating the program being audited. Organizations should begin vetting auditors now; qualified cybersecurity auditors will be in high demand as deadlines approach.

11 Cal. Code Regs. § 7122 — "The cybersecurity audit shall be conducted by a qualified, objective, and independent professional who is familiar with both cybersecurity and how to audit a cybersecurity program. The auditor shall not have participated in the design, implementation, or operation of the cybersecurity program being audited during the audit period."

Roundtable Discussion: How are you approaching auditor selection? How are you managing independence with firms that do both advisory and audit work?

troutman pepper locke

7

Executive Accountability + Certification

PRACTICAL PRACTITIONER TIP:

Secure Executive and Board Buy-In

CCPA certification creates personal accountability — the signing executive attests under penalty of perjury.

- **The signatory must attest NOT ONLY that the audit was completed — but also that no attempt was made to influence the auditor's decisions. Personal perjury exposure.**
- Identify the certification signatory and brief them on the full scope of personal exposure — this is not just organizational compliance.
- Brief the board on obligations, timeline, and litigation exposure. Audit reports are discoverable — the board's oversight record matters.
- Incorporate milestones into strategic planning and budgets; document all oversight activities (board minutes, management reports, budget approvals).

REGULATORY REQUIREMENT

An executive management team member directly responsible for cybersecurity audit compliance must certify, under penalty of perjury, that the audit was conducted AND that no attempt was made to influence the auditor's decisions or assessments — creating direct personal liability.

11 Cal. Code Regs. § 7125 — "A member of the business's executive management team who is directly responsible for the business's cybersecurity audit compliance shall certify, under penalty of perjury, that the business has conducted a cybersecurity audit and that the business has not attempted to influence the decisions or assessments of the auditor."

Roundtable Discussion: What Are Best Practices for Securing Executive and Board Buy-In?

troutman pepper locke

8

Breach Notification Documentation

PRACTICAL PRACTITIONER TIP:

Enhance Breach Documentation — Notification Samples Required

CCPA audits must include breach notification samples. Unique requirement — often missed in planning.

- **Maintain copies of ALL breach notifications issued during the audit period (to consumers AND regulators). Keep drafts showing revision history.**
- Document timelines proving deadline compliance; record scope determinations (who you notified, when, and why) with supporting analysis.
- Retain all incident remediation evidence for 5 years — aligns with CalPrivacy's 5-year enforcement window.
- Update Incident Response plan templates NOW to build evidence collection into incident workflows before an incident occurs.

REGULATORY REQUIREMENT

The CCPA cybersecurity audit report must include actual breach notification samples issued during the audit period — including the nature of the breach, types of PI involved, and date of notification. This is a unique CCPA requirement not found in any of the comparison frameworks.

11 Cal. Code Regs. § 7124(a)(9) — "A sample or brief description of any notifications provided to individuals, the California Attorney General, or other state or federal agencies during the audit period regarding personal information security breaches, including the nature of the breach, the types of personal information involved, and the date of notification."

Roundtable Discussion: What documentation gaps will companies potentially find when they first look at their breach notification records through the audit lens?

troutman pepper locke

9

Service Provider Management

PRACTICAL PRACTITIONER TIP:

Strengthen Third-Party Risk Management

Your vendors are within CCPA's audit scope. Update contracts now — don't wait.

- **CCPA's scope explicitly includes third-party environments. Vendors and service providers processing CA PI are within the audit's reach.**
- Add audit cooperation and access provisions to vendor contracts; require evidence production (SOC 2 Type II, ISO 27001, pen test summaries).
- Include incident response collaboration and breach notification obligations; validate flow-down requirements to sub-processors.
- Formally risk-assess all third parties accessing, processing, or storing PI. Implement ongoing monitoring — not just point-in-time assessments.

REGULATORY REQUIREMENT

The cybersecurity audit scope explicitly encompasses third-party environments. Service providers and vendors processing California PI must cooperate with the business's cybersecurity audit — a contractual audit cooperation requirement not found in other frameworks.

11 Cal. Code Regs. § 7123(c)(15) — "Oversight of service providers, contractors, and other third parties that have access to the business's information system or that process personal information on the business's behalf, including contractual provisions requiring them to implement and maintain appropriate security measures and to cooperate with the business's cybersecurity audit."

Roundtable Discussion: How will you approach the conversation with vendors about audit cooperation rights? Which contract updates will be most contested?

troutman pepper locke

10

Audit Evidence Repository

PRACTICAL PRACTITIONER TIP:

Build Your Audit-Ready Evidence Repository Now

Don't scramble before audits. Centralize documentation — organized by all 18 CCPA components.

- **Strongest evidence is system-generated, current, and clearly tied to the specific control: logs, telemetry, configuration exports, scan results, and remediation tickets.**
- Organize by all 18 CCPA components: policies and standards, system configurations and screenshots, access logs, vulnerability scan reports, training records, third-party certifications.
- Archive network diagrams, data flow diagrams, IAM architecture, role definitions, and security org chart. Keep pen test reports, incident documentation, and lessons learned.
- Implement version control aligned with the 5-year retention requirement. Consider GRC platforms. Build collaboratively with outside counsel and advisory firms — under privilege where possible.

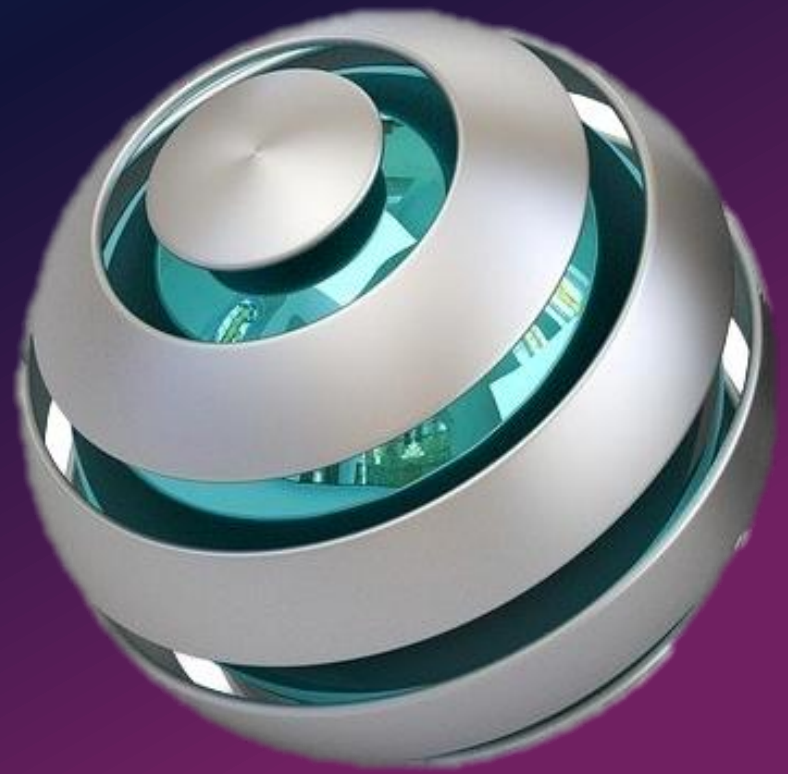
REGULATORY REQUIREMENT

The cybersecurity audit report must describe the specific types of evidence examined and why that evidence justifies the auditor's findings. Gaps, weaknesses, and remediation plans must all be documented — making evidence quality and organization critical to audit success.

11 Cal. Code Regs. § 7124(a) — "The cybersecurity audit report shall contain: a description of the information systems and cybersecurity program assessed; the criteria used for the audit; the specific types of evidence examined and why they justify the auditor's findings; the status of any gaps or weaknesses; the business's plan and timeframe to address identified gaps; and the auditor's signed certification of independence."

Roundtable Discussion: What Are the Emerging Best Practices on Building an Audit-Ready Evidence Repository? Who Is Responsible for Building and/or Maintaining?

Key Takeaways



Key Takeaways

1. The audit PERIOD begins January 1, 2027. Controls must be operational in less than 8 months — certifications come later, but enforcement is live now.
(11 Cal. Code Regs. § 7125)

2. Don't reinvent. Build on NIST CSF, ISO 27001, CIS-18, SOC 2. Then supplement the three critical gaps: PI inventories, VDP, and phishing-resistant MFA scope.
(11 Cal. Code Regs. § 7121)

3. Privacy and security leaders must work together. The CPO cannot operationalize this audit without the CISO's active involvement. Use the requirement as the catalyst.

4. Audit reports are discoverable. A clean audit is your defense; a gap-filled audit is a plaintiff's roadmap. Conduct gap assessments under privilege before the formal audit.
(Cal. Civ. Code § 1798.150)

5. Start Monday: identify your audit foundation, map to 18 components, engage auditors early, and get executive buy-in on personal certification accountability.

troutman pepper locke

Questions?

troutman pepper locke

Contact Information

Jim Koenig
TROUTMAN PEPPER LOCKE LLP
Partner + Global Co-Leader, Privacy + Cyber + AI Practice
New York
610.246.4426 | jim.koenig@troutman.com

For the full five-framework comparison article and CCPA cybersecurity audit resources:
troutman.com/services/practices/privacy-cyber

Thank You

troutman pepper locke