Alpha Secure LLP

Digital Trust. Delivered.

Navigating California's Updated Privacy Laws

Presented to:

ISACA Los Angeles Chapter

February 10, 2026

Alpha Secure LLP
Digital Trust. Delivered.

Navigating California's Updated Privacy Laws

Session Background

The California Privacy Protection Agency (CPPA) finalized crucial regulations in July 2025, defining mandatory compliance requirements around Automated Decision-Making Technology (ADMT), comprehensive risk assessments, and cybersecurity audits.

This session reviews these finalized rules, offering practical strategies to implement the new "Privacy Pillars" for successful outcomes. We will clarify the newly narrowed scope of ADMT compliance, which now focuses primarily on systems that substantially replace human decision-making for significant decisions.

Note: The official CPPA website is listed here: https://cppa.ca.gov/
The amended CCPA legislation leveraged for this presentation is here: Final Regulations Text

Alpha Secure LLP

Digital Trust. Delivered.

Learning Objectives

Understand the history of the CCPA and CPRA acts and review the consumer data privacy and protection rights in California.

Evaluate existing Automated Decision-Making Technology (ADMT) systems to determine whether they meet the finalized standard of substantially replacing human decision-making for significant decisions, requiring consumer opt-out mechanisms or exceptions.

Determine specific processing activities that trigger a comprehensive California risk assessment, including the processing of sensitive personal information or the use of ADMT for training that will render a significant decision.

Outline organizational strategies for engaging qualified, objective, and independent auditors and initiating cybersecurity audit readiness reviews, leveraging established standards like AICPA or ISACA, based on the required staggered timelines.

Develop a plan to modify existing Privacy Impact Assessment (PIA) programs to capture the unique requirements of the CPPA risk assessment, including detailing the risk-benefit analysis and designating appropriate internal reviewers.

Alpha Secure LLP
Digital Trust. Delivered.

About Alpha Secure LLP

We are a fully-licensed CPA firm, delivering risk advisory and audit solutions for mid-market companies.

We help transform emerging and mid-market companies into security leaders through our specialized IT audit and advisory solutions.

- As a strategic audit partner, we convert compliance requirements into real competitive advantages that facilitate business growth.

Our professionals understand finance, business operations, IT systems, and cybersecurity - not just one piece of the puzzle.

- Our comprehensive expertise means we solve actual problems, not just check compliance boxes.

We combine our deep audit and cybersecurity expertise to help mid-market companies demonstrate compliance quickly and without complexity.

- We help companies build digital trust with their stakeholders without the complexity.

Alpha Secure LLP
Digital Trust. Delivered.

Audit and Risk Advisory Solutions

Comprehensive Solutions Tailored to You

Audit

Our comprehensive audit solutions convert your compliance investment into the trusted evidence that your stakeholders can use for assurance across your enterprise technology.

SOC 1 Audit

Internal controls over financial reporting (ICFR)

SOC 2 Audit

Security + Availability/Processing Integrity/Confidentiality/Privacy

Comprehensive Cybersecurity Audits

Combined Center for Internet Security (CIS) framework AUP + SOC 2 audit

SOC 2+ Audit

A SOC 2 audit that includes controls that overlap with other key cybersecurity frameworks

Risk Advisory

Our tailored advisory solutions leverage industry-leading and accepted frameworks, demonstrating to your stakeholders that you are serious about internal controls and cybersecurity.

Strategic Risk Advisory

Inclusive of IT general controls (ITGC), business process internal controls, and SOX compliance

SOC 1 & 2, CIS, CMMC, ISO, & HITRUST Readiness

Readiness with key industry leading compliance frameworks

AI Readiness & Governance

Secure AI adoption, including policy & control design

Data Privacy (e.g., GDPR, CCPA, HIPAA) Readiness

Prepare for compliance with key data privacy frameworks

Alpha Secure LLP

Digital Trust. Delivered.

Cybersecurity Solutions

Solutions to Protect Your Sensitive Data

vCISO

- Draft and tailor security policies and procedures
- Facilitate quarterly InfoSec committee meetings
- Develop cybersecurity strategy
- Drive cybersecurity initiatives
- Ensure data protection and recovery programs with expected results are in place
- Lead compliance efforts with required frameworks and regulations

vISM

- Security Incident Response Team (SIRT) leader
  - Lead the incident response and recovery
  - Document corrective/preventative actions
- Quarterly security maturity assessment
- Annual risk assessment report for the InfoSec Committee
- Security awareness training
- Information security policy training

Security Operations Center (SOC)

- 24x7x365 Cybersecurity
- Monitoring and administration
- Security threat response and escalation
  - Discovery of insecure ports, protocols and services
  - Discovery of vulnerabilities that could lead to an incident
- Security Event Response and Escalation
  - Resetting compromised usernames and passwords
  - Triaging bad actor IP Addresses and domain names to the Firewall Team to be blocked
- Security Incident Response and Escalation to the SIRT Team Leader
  - Escalation of confidentiality, integrity or availability incident
- SIEM management
- Data Loss Prevention (DLP) system management

Professional Services (Projects)

- Hardware & software inventory controls
- SIEM installation & configuration
- Network & server hardening
- Data encryption
- Web browser & email hardening
- Deploy SSO and MFA
- Automate security policy requirements

RED Team

- Penetration Testing
- Simulated email phishing attacks/ testing
- Simulated cyber attacks/testing
- Vulnerability reporting
- Physical security procedure testing
- Wireless network, web application and desktop client attacks and testing
- Scan environment for unsecured sensitive or confidential data

Alpha Secure LLP
Digital Trust. Delivered.

Advantages of FlowGRC

Our SaaS Solution Helps Our Clients Save Money

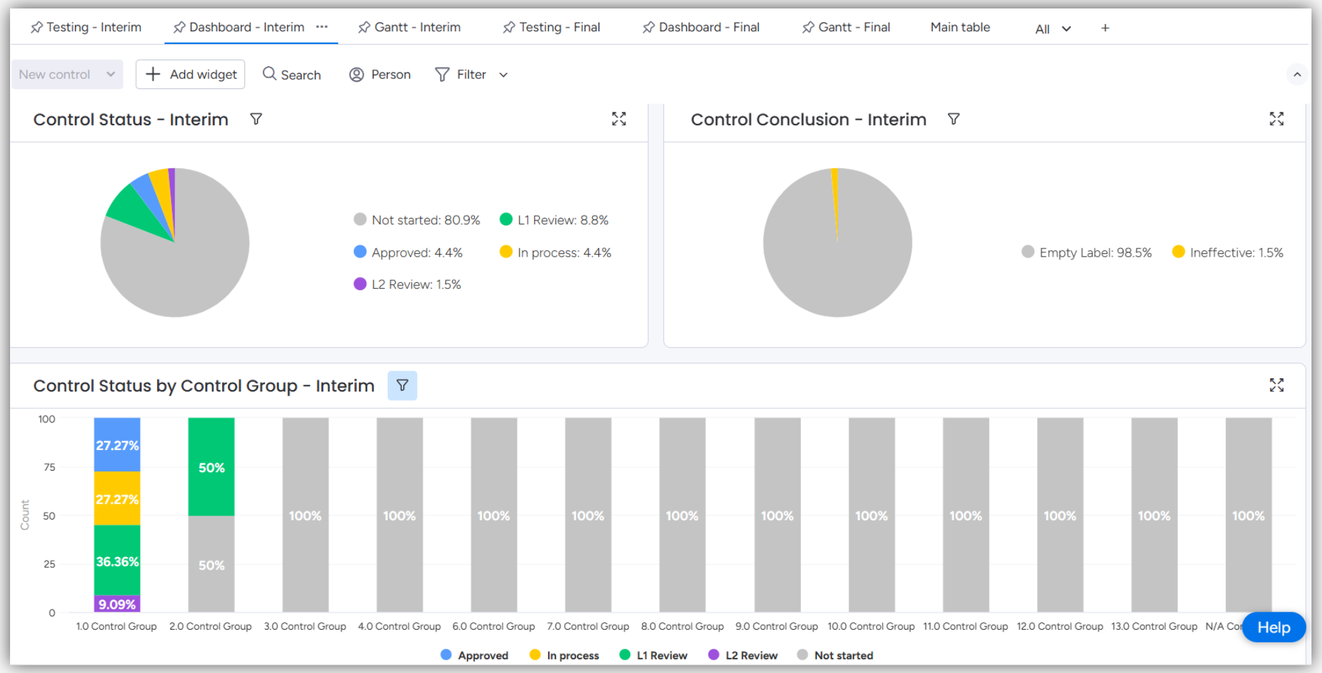
FlowGRC

How FlowGRC saves you time and money:

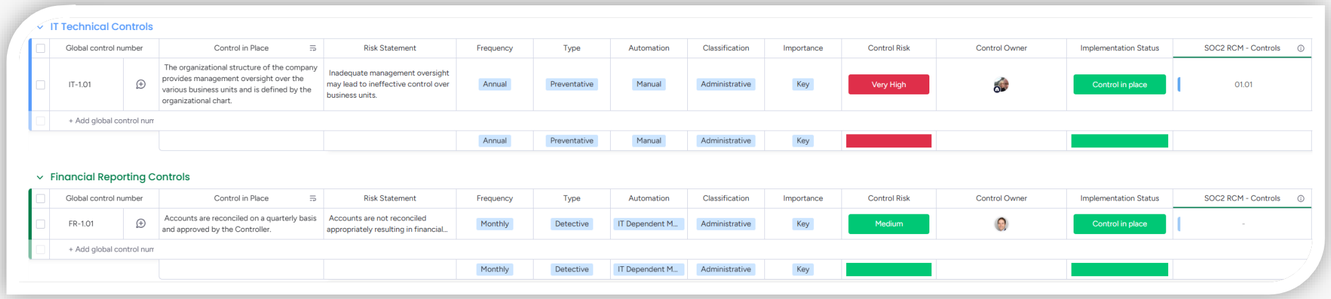
- A real-time shareable GRC, SOC, SOX, CIS, and CMMC internal controls matrix that is accessible on-demand via our SaaS FlowGRC tool
- Full automation and cloud-based access of the project workflow, document request, and issue management processes
- Best-in-class dashboarding, Gantt charts, and real-time reporting of project status and results
- Ability to manage all internal controls and related testing, mapped together by framework, in a single SaaS cloud-based repository
- Turn-key vendor management, risk assessment, and contract compliance modules are included to help you manage third-party risk

Access to our FlowGRC tool is included for clients that contract for services with Alpha Secure.

Project Dashboard



GRC Module



Alpha Secure LLP
Digital Trust. Delivered.

Your Presenters

Carl Grifka, CISSP, CISA, CISM, CDPSE, PMP

Principal

Carl serves as the internal controls function leader at Alpha Secure. Carl's practice areas include IT risk, internal audit/SOX/JSOX, cybersecurity, SOC reporting, financial process advisory, & project management.

Carl's prior work experience:

- Risk Consulting Director at RSM
- Managing Director at a top 100 CPA firm leading the cybersecurity and IT risk practice
- Global enterprise CFO and compliance officer for Cinionic (Now Barco Cinema)
- Internal Audit Lead at General Motors, including SOX and IT audit
- Revenue Agent for the Internal Revenue Service
- Frequent speaker and ISACA OC board member

Carl.Grifka@GoAlphaSec.com
+1(248)219-8533

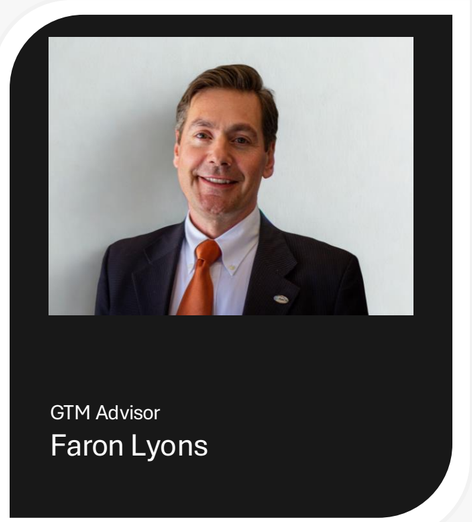
Faron Lyons

GTM Advisor

Faron serves as a sales and marketing leader at Alpha Secure. Faron's areas of expertise include Compliance, Cybersecurity, Process Automation, Information Governance, Device Management, Data Privacy, and Data Security.

Faron's prior work experience:

- Territory Manager at BlackBerry
- National Sales Director at iCompli
- Sales Executive, Legal Solutions Group, OpenText
- Sales Executive, Alfreso (Hyland)
- Sales Director, Zia Consulting Group
- Sales & Marketing Consultant
- Frequent speaker and ISACA LA board member



Faron.Lyons@GoAlphaSec.com
+1(323)333-6278

Alpha Secure LLP
Digital Trust. Delivered.

Polling Question #1

What function do you represent within your company?

a) Internal audit

b) Finance

c) IT

d) Operations

e) Other

GTM Advisor
Faron Lyons

History of CCPA & CPRA

Alpha Secure LLP
Digital Trust. Delivered.

History of CCPA

Background

History of CCPA

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States. The bill was passed by the California State Legislature and signed into law by Jerry Brown, Governor of California, on June 28, 2018, to amend Part 4 of Division 3 of the California Civil Code.

CCPA Compliance Scope

The CCPA act, at its inception, applied to any business, including any for-profit entity that collects consumers' personal data, which conducted business in California, and satisfied at least one of the following thresholds:

- Has annual gross revenues in excess of $25 million;
- Buys or sells the personal information of 50,000 or more consumers or households; or
- Earns more than half of its annual revenue from selling consumers' personal information.

Organizations were required to "implement and maintain reasonable security procedures and practices“ to protect consumer data.

Importantly, non-profit organizations and governmental entities were generally excluded from compliance with this legislation (a few circumstances can trigger compliance).

Alpha Secure LLP
Digital Trust. Delivered.

History of CCPA

Original Privacy Bill of Rights

Consumers Benefit of CCPA Passage

The CCPA created an array of consumer privacy rights and business obligations with regard to the collection and sale of personal information. The California Privacy Protection Agency (CPPA) board (now CalPrivacy) was established to enforce the CCPA on businesses. Conversely, these rights created a substantial number of requirements for employers to meet in order to comply with these regulations.

As of January 1, 2026, there are now 20+ US states with consumer data privacy laws.

CCPA Original Consumer Rights

The CCPA provided consumers with a number of rights, to increase the data privacy and providing them with more control of their personal data.

Right to Know

Consumers have the right to know what personal information is collected, used, shared, and sold.

Right to Delete

Consumers have the right to have their personal information held by businesses to be deleted.

Right to Opt-Out

Consumers have the right to prevent businesses from selling or sharing personal data for cross-context behavioral advertising (targeted ads).

Non-Discrimination

Consumers have the right that businesses cannot discriminate against consumers for exercising their rights.

Alpha Secure LLP
Digital Trust. Delivered.

CPRA History

Background

CPRA (2023 to Present)

The California Privacy Rights Act (CPRA) amended the California Consumer Privacy Act (CCPA)–modifying its scope, expanding consumer rights (e.g., and employee data), and adding additional regulations around commercial data collection and processing.

Employee Data Coverage in CPRA

CCPA (2018 through 2022)

Employee data was largely exempt. Only notice at collection and breach liability applied.

CPRA (2023 to Present)

Full coverage of employee data is included.
All consumer rights now apply to employees.

Key Changes that CRPA Brought to Consumers

The CPRA amended the CCPA to add four new rights to consumers.

1. Right to correction

Consumers have the right to correct inaccuracies in their own personal data held by third-party organization.

2. Right to limit the collection sensitive personal information (SPI)

Consumers have the right to request that a business limit collected sensitive data's use to what is "necessary to perform the services or provide the goods reasonably expected" by a consumer.

3. Right to access and opt-out of automated decision-making tools (ADMT)

Businesses must respond to consumer requests for information about the logic behind automated decision-making and the likely outcome of those processes. Consumers may opt-out of automated decision-making, including profiling, related to their "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."

4. Right to data portability

Consumers can ask a business to transmit their personal data to another business.

CPRA History

Personal Information vs Sensitive Personal Information (SPI)

Personal Information

CPRA defines personal information very broadly:

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked (directly or indirectly) with a particular consumer or household.

Sensitive Personal Information (SPI)

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(G) A consumer's neural data, which means information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information.

(2) The processing of biometric information for the purpose of uniquely identifying a consumer.

(3) Personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.

(4) Personal information of consumers that the business has actual knowledge are less than 16 years of age. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. Sensitive personal information does not include information that is "publicly available".

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Penalties

Business Case for Compliance

Civil CPRA Penalties, effective 1/1/25

Civil Code § 1798.150(a)(1)(A): ***Monetary damages range per consumer per incident***	Not less than **$107** and not greater than **$799** per consumer per incident or actual damages, **whichever is greater**.
Civil Code § 1798.155(a): ***Administrative fine amounts***	Not more than **$2,663** for each violation or **$7,988** for each intentional violation and violations involving the personal information of consumers **whom the violator has actual knowledge are under 16 years of age.**
Civil Code § 1978.199.90(a): ***Civil penalty amounts***	Not more than **$2,663** for each violation or **$7,988** for each intentional violation and violations involving the personal information of consumers **whom the violator has actual knowledge are under 16 years of age.**

Alpha Secure LLP
Digital Trust. Delivered.

Polling Question #2

What is the maximum penalty per consumer per incident as defined by CPRA?

a) $799 per incident

b) Actual damages

c) Whichever of (a) or (b) is greater

GTM Advisor
Faron Lyons

Alpha Secure LLP

Digital Trust. Delivered.

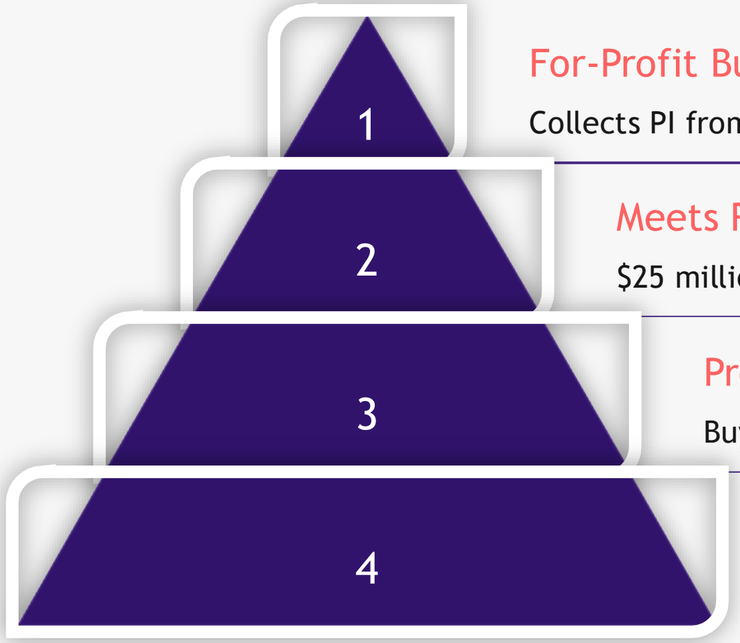
CPRA Evolution

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

Revised Business Applicability Criteria

A business is **subject to the CCPA/CPRA** if it meets **any of the following criteria:**



For-Profit Business Operates in California

Collects PI from California residents and does business in California

Meets Revenue Threshold

$25 million or more in annual gross revenues *($25.625M after 1/1/25)*

Processes Significant Data

Buys, sells, or shares PI of 100,000+ consumers/households/devices*

Revenue from Data

Derives 50%+ of annual revenue from selling/sharing PI

** Note: CPRA raised this threshold from 50,000 (under CCPA) to 100,000 to relieve smaller businesses from the steep compliance requirements.*

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

Automated Decision-Making Technology (ADMT)

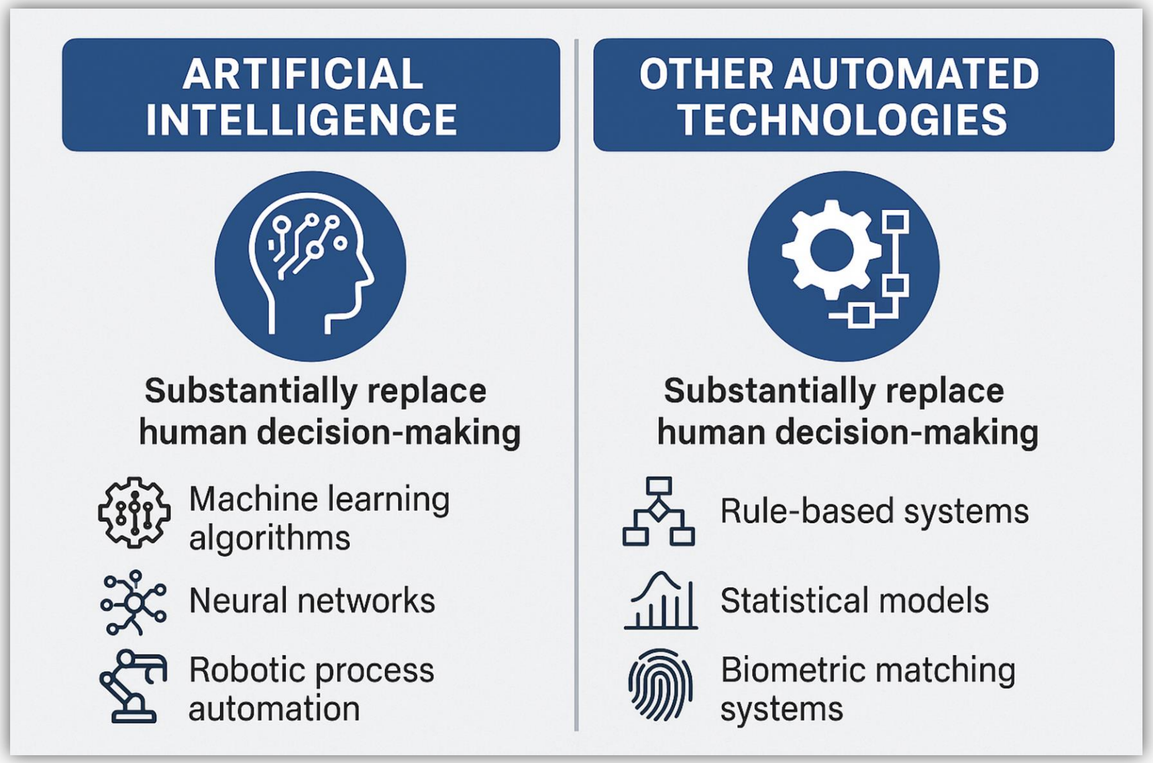
Critical Updates to CPRA in 2025 - ADMT

CPPA's finalized regulations materially tighten ADMT scope under the CPRA, limiting coverage to technologies that replace or substantially replace human decision-making, when used for "significant decisions" impacting consumers (e.g., employment screening, credit decisions, healthcare treatment, housing).

Behavioral advertising is no longer treated as a "significant decision" and the earlier proposal that could have pulled in certain first-party advertising use cases has been removed.

Net effect: compliance focus shifts toward high-stakes decisioning versus routine analytics or business support workflows.

Opt-out rights are more bounded through expanded exceptions. When a business implements a **meaningful human review** of qualified ADMT outputs and provides a consumer appeal path for ADMT-driven significant decisions, the business generally does **not** need to offer an ADMT opt-out for that process.



Note: *"Automated decision-making technology" or "ADMT" means any technology that processes personal information and uses computation to replace human decision-making or substantially replace human decision-making.*

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

CPPA Risk Assessment Lifecycle

Risk Assessment Purpose:

The company must identify and document in a risk assessment report the categories of personal information to be processed, including any categories of sensitive personal information. This must include the minimum personal information that is necessary to achieve the purpose of processing consumers' personal information.

The goal of a risk assessment is restricting or prohibiting the processing of personal information if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.

Refresh cadence:

Re-evaluate each risk assessment no less than once every 3 years and revise it as needed to keep it current.

Change-triggered updates:

If a processing activity undergoes a material change, the assessment must be updated within 45 calendar days.

Data Retention:

Maintain the original and all revisions for the full life of the processing activity, or 5 years after the assessment is completed, whichever period is longer.

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

CPPA Risk Assessment Reporting & Attestation

When do businesses need to report the risk assessments to the CPPA?

- For risk assessments conducted in 2026 and 2027, the business must submit to the Agency the information required by subsection (b) no later than April 1, 2028.
- The individual submitting the information must be a member of the business's executive management team who:
  - Is directly responsible for the business's risk-assessment compliance; and
  - Has sufficient knowledge of the business's risk assessment to provide accurate information

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

CPPA Risk Assessment Reporting & Attestation

A business must submit to the CPPA, the following risk assessment information:

- The time period covered by the submission, by month and year.
- The number of risk assessments conducted or updated by the business during the time period.
- Whether the risk assessments conducted or updated by the business during the time period covered by the submission involved the processing of each of the categories of personal information and sensitive personal information defined in the legislation.
- **Attestation to the following statement:** “I attest that the business has conducted a risk assessment for the processing activities set forth in California Code of Regulations, Title 11, section 7150, subsection (b), during the time period covered by this submission, and that I meet the requirements of section 7157, subsection (c). **Under penalty of perjury under the laws of the state of California**, I hereby declare that the risk assessment information submitted is true and correct.”

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

CPPA Annual Cybersecurity Audits

CPPA Cybersecurity Audit Requirement: Trigger Criteria

The California Privacy Protection Agency finalized rules define an annual cybersecurity audit requirement for businesses whose data practices create significant security risk to consumers.

An audit is required if any of these thresholds are met:

- Revenue concentration: 50%+ of annual revenue comes from selling or sharing consumers' personal information; or
- Scale + revenue test: prior-year gross revenue exceeded $25M and the business processed either:
  - PI of 250,000+ California Consumer Privacy Act consumers/households in the prior year; or
  - Sensitive PI of 50,000+ California consumers in the prior year
- Audit execution must be led by a qualified, objective, and independent auditor (internal or external) with proven capability in cybersecurity program assurance.

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

CPPA Annual Cybersecurity Audits

What if an Internal Auditor is used by the company to conduct the audit?

If a business uses an internal auditor for the cybersecurity audit, to maintain the auditor's independence, the highest-ranking auditor must report directly to a member of the business's executive management team who does **not** have direct responsibility for the business's cybersecurity program.

A member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program must conduct the highest-ranking auditor's performance evaluation, if any, and determine the auditor's compensation.

Also, no finding of any cybersecurity audit may rely primarily on assertions or attestations by the business's management. Cybersecurity audit findings must rely primarily upon the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) that the auditor deems appropriate.

Alpha Secure LLP
Digital Trust. Delivered.

Polling Question #3

What is a requirement for an internal auditor to perform the annual cybersecurity audit that must be reported to the CPPA?

a) The CAE must report directly to a member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program

b) The CAE must have at least one CISA certified professional on its staff to conduct the audit

c) All of the above

GTM Advisor
Faron Lyons

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

How CPPA Audits Are Measured, Phased-in, and Certified

CPPA Cybersecurity Audits: Key Scope Requirements

Audit Standards

Required audits can be completed by professionals using auditing standards from the AICPA, ISO, the PCAOB, or ISACA.

Audit Scope

The updated act provides an example that the NIST Cybersecurity Framework (NIST CSF) 2.0 is considered an acceptable audit scope for the CPPA.

Audit reuse is permitted

An existing cybersecurity audit performed for another purpose may satisfy the requirement if it aligns to the CPPA criteria, such as NIST CSF 2.0.

Phased rollout based on revenue size

The first required audits fall within April 2028-2030, with larger-revenue organizations expected to comply earlier.

Alpha Secure LLP
Digital Trust. Delivered.

Polling Question #4

Which audit standards are allowable to perform the annual CPPA mandated cybersecurity audit?

a) AICPA

b) ISO

c) PCAOB

d) ISACA

e) All of the above

GTM Advisor
Faron Lyons

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

Audit Reporting & Attestation Requirements

CPPA Cybersecurity Audits: Reporting Requirements

The business must submit the certification to the CPPA no later than April 1 following any year that the business is required to complete a cybersecurity audit.

The written certification must be completed by a member of the business's executive management team who:

1. Is directly responsible for the business's cybersecurity-audit compliance;
2. Has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and
3. Has the authority to submit the business's certification to the Agency.

Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

Audit Reporting & Attestation Requirements

CPPA Cybersecurity Audits: Required Attestation Language

An electronically signed **attestation to the following statement:**

“I attest that I meet the requirements of California Code of Regulations, Title 11, section 7124, subsection (c), to submit this certification.

Under penalty of perjury under the laws of the state of California, I hereby declare that the information contained within and submitted with this certification is true and correct and that the business has not made any attempt to influence the auditor’s decisions or assessments regarding the cybersecurity audit.”

Alpha Secure LLP
Digital Trust. Delivered.

Why Cybersecurity Controls Are Important

Value Beyond the Cyber Audit Investment

Cyber Threats In Perspective

Hackers are no longer lone wolves. They're now banding **together** to run fewer – yet much larger – attacks, similar to the traditional crime rings of the 20th century.

80% of cyber-attacks are driven by organized crime rings, in which data, tools and expertise are widely shared.

Organized cybercrime is the most profitable type of crime.

$2,300
Average **loss per individual burglary** in the U.S.

$30,000,000
The **largest bank robbery in U.S. history.**

$445 Billion
Annual cost of cybercrime to the global economy.

"60% of cyber attacks target small businesses"

Juniper Research

"85% could have been prevented by 6 Critical Security Controls!!"

Center for Internet Security CIS Report

The bottom line is that basic cybersecurity hygiene, which these audited controls represent, will reduce a Company's overall cyber risk posture and improve its business resilience.

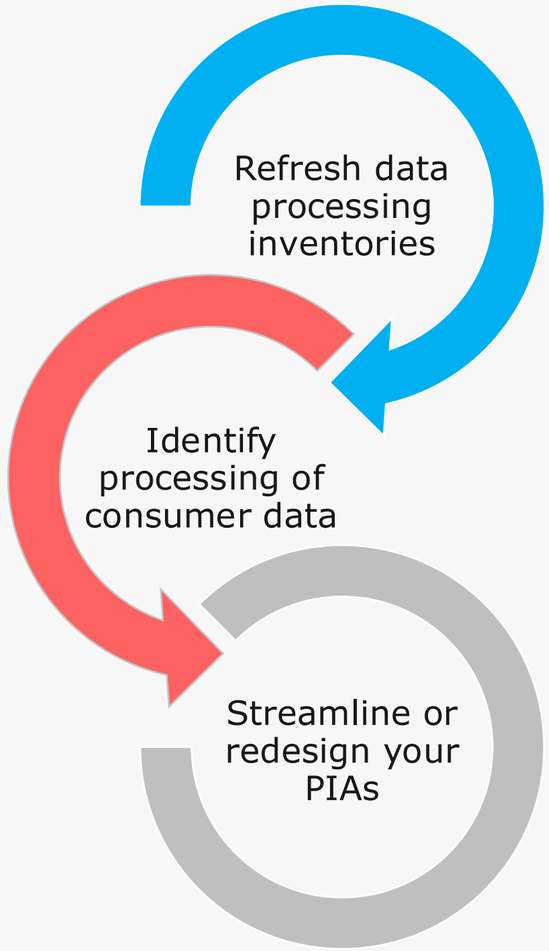
Alpha Secure LLP
Digital Trust. Delivered.

CPRA Evolution

Impact to PIAs

Possible Impact on Privacy Impact Assessments (PIA):

- **Refresh** processing activity inventories to ensure they stay current and automatically account for new PII use cases.
- **Identify** processing activities requiring risk assessments under the finalized rules, and update or redo PIAs where additional risks must be captured.
- By early 2026, **streamline or redesign** the PIA program to ensure full traceability to the new risk assessment requirements, including adding a CPPA-specific risk assessment overlay as either a standalone workflow or an enhancement to the existing process.



Alpha Secure LLP
Digital Trust. Delivered.

How to Prepare for CPRA Compliance

& Identify the Right Compliance Partner

How can you identify the right CPRA compliance or audit partner?

1. Pick the right CPRA data privacy compliance project or audit based on your needs – and make sure you pick a trusted independent CPA firm, like Alpha Secure.
2. Take the time to prepare for your CPRA compliance project or audit with a readiness approach; scope properly, identify your processing inventory and controls, and designate your internal team.
3. Determine if you can have overlapping internal controls tested; wherein you demonstrate compliance with additional frameworks within a single audit or readiness project.
4. Leverage a partner that uses a comprehensive SaaS tool (our FlowGRC SaaS tool is included with our solutions) to automate the audit process and add transparency; make sure any solution includes real-time reporting.

This approach allows you to achieve a much higher ROI on your data privacy compliance investment and will help you choose a partner that you can leverage for years to come.

Alpha Secure LLP

Digital Trust. Delivered.

Let’s Transform Compliance into Advantage

| www.goalphasec.com

| contact@goalphasec.com

| www.linkedin.com/company/alpha-secure-llp

Contact Information:
+1.949.423.6386
contact@goalphasec.com, carl.grifka@goalphasec.com, faron.lyons@goalphasec.com
515 S Flower Street, 18th Floor
Los Angeles, CA 90071