Hashed & Salted | A Privacy and Data Security Update
December 2025

California Privacy Regulations Requiring Cybersecurity Audits and Risk Assessments: What To Know and What To Do

The California Privacy Protection Agency (CPPA) earlier this year succeeded in finalizing new and amended regulations under the California Consumer Privacy Act (CCPA). In addition to updated regulations governing businesses' obligations relating to consumers' privacy rights (opt-out mechanisms; right to know; data accuracy and correction; sensitive personal information; dark patterns in consumer interfaces; and transparency around data collection by mobile apps, connected devices, and augmented and virtual reality environments), the package of regulations includes new obligations requiring certain businesses to conduct cybersecurity audits and risk assessments.

These new regulations begin to take effect on Jan. 1, 2026, and some (such as the risk assessment requirements) apply to existing processing activities initiated before the effective date. While businesses that process consumers' personal information have time to comply with their new obligations, they should assess their cybersecurity programs and risk assessment processes and begin updating components and processes as needed.

Here's what covered businesses need to know.

Cybersecurity Audits

Beginning as early as 2027, businesses whose processing of personal information presents a "significant risk" to consumers' security must perform annual cybersecurity audits. A business is considered to present a "significant risk" to consumers' security if:

- It generated in the preceding calendar year annual gross revenue in excess of $25 million and processes either personal data of more than 250,000 consumers or sensitive data of more than 50,000 consumers.
- It derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Audit requirements

The regulations set out the annual audit requirements, including timing, process, scope, documentation, report content and certification.

Timing: Audit deadlines and audit periods are phased in based on revenue thresholds beginning in 2026:

- **April 1, 2028**, for businesses with annual gross revenue in 2026 exceeding $100 million, with an audit period of Jan. 1, 2027, through Jan. 1, 2028.
- **April 1, 2029**, for businesses with annual gross revenue in 2027 between $50 million and $100 million, with an audit period of Jan. 1, 2028, through Jan. 1, 2029.

Attorney Advertising

- **April 1, 2030**, for businesses with annual gross revenue in 2028 of less than $50 million, with an audit period of Jan. 1, 2029, through Jan. 1, 2030.
- **After 2030**, businesses that meet revenue thresholds must submit annual audits of the previous 12 months by April 1 of each year. In other words, a business that meets a revenue threshold on Jan. 1, 2030, must submit its audit by April 1, 2031, covering Jan. 1, 2030, through Jan. 1, 2031.

Process: Audits must be performed by qualified, objective and independent professionals, following recognized standards, such as those defined by AICPA, ISO, ISACA and PCAOB, for example. Audits may be conducted by internal or external professionals. To preserve independence, internal auditors must report to executives not responsible for cybersecurity. Internal auditors must exercise impartial judgment on all issues and refrain from participating in the business activities being assessed.

Audits must primarily rely on specific evidence, including documents, testing and interviews—not attestations from business executives. The business is required to provide all relevant materials and retain audit documentation for five years.

Scope: Audits must evaluate the business's policies and technical controls. Policies should provide written documentation of how the business's cybersecurity program protects personal information from unauthorized access, destruction, use, modification or disclosure; enforces compliance; and implements and maintains the cybersecurity system.

The audit should address how the business has implemented the following components of its cybersecurity program, as applicable:

- Authentication, such as multi-factor authentication and password management
- Encryption of personal information, both at rest and in transit
- Account management and access controls
- System inventory, including personal information inventories, and hardware and software inventories
- Secure configuration of hardware and software, including masking of sensitive information and patch management
- Vulnerability scans, penetration testing and change management
- Audit-log management, including the centralized storage, retention and monitoring of logs
- Network monitoring and data loss prevention
- Antivirus and anti-malware protection
- Segmentation of information systems via, for example, properly configured firewalls, routers and switches
- Limitation and control of ports, services and protocols
- Cybersecurity awareness and staff training
- Secure software development and coding practices
- Oversight of service providers, contractors and third parties
- Incident response and business continuity/disaster recovery planning
- Data retention/disposal policies

Report content: Audit reports must:

- Describe the business's information system and the criteria used for the audit
- Summarize the evidence reviewed, such as documents, tests and interviews
- Explain the auditor's rationale for the findings
- Evaluate the effectiveness of controls and safeguards used to prevent unauthorized activity
- Identify and detail the status of any gaps or weaknesses found that increase the risk of unauthorized access to consumers' personal information; destruction, use, modification or disclosure of consumers' personal information; or unauthorized activity resulting in the loss of availability of personal information
- Document the business's plan to address these gaps and weaknesses, including the time frame in which it will resolve them
- Be provided to executive management overseeing cybersecurity

Certification: For each calendar year that a business is required to complete a cybersecurity audit, it must submit to the CPPA a written certification that the business completed the cybersecurity audit as required. Certification must be submitted no later than April 1 of the following year. So if an audit is required in 2030, certification must be submitted to the CPPA by April 1, 2031.

Next steps: To prepare for audit obligations under the revised regulations, businesses should:

- Review the financial thresholds to determine when your audit obligations will be triggered
- Schedule annual checks to monitor whether thresholds have been triggered
- Review the revised regulation requirements and address any potential gaps
- Identify an auditor and audit process in advance of obligations being triggered

Risk Assessments

Beginning in 2026, businesses must perform risk assessments on all new and existing data processing activities that present a "significant risk" to consumer privacy. The goal of a risk assessment is to identify, and therefore limit or avoid, the processing of personal information when risks to the consumer's privacy outweigh the benefits that result from processing to the consumer, the business, other stakeholders and the public.

Activities that require a risk assessment include:

- Selling or sharing personal information
- Processing sensitive personal data (with an exception for processing sensitive personal information of employees/contractors for the purpose of administering compensation or benefits)
- Using personal information for automated decision-making technology (ADMT) that will result in a significant decision for a consumer
- Using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, location or movements, based on systematic observation of that consumer when they are acting in their capacity as an educational program applicant, job applicant, student, employee or independent contractor for the business
- Using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior or movements, based on that consumer's presence in a sensitive location
  - The definition of "sensitive location" includes health care facilities, such as hospitals, doctors' offices, urgent care facilities and community health clinics; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; educational institutions; political party offices; legal services offices; union offices; and places of worship.
- Processing personal information to train ADMT for a significant decision concerning a consumer or for facial recognition, emotion recognition or other technology that verifies a consumer's identity, or conducts physical or biological identification or profiling of a consumer
  - This includes planned uses or plans to permit others to use personal information (including advertising/marketing the use of personal information for this purpose).

Risk Assessment Requirements

The regulations outline risk assessment requirements, including stakeholder involvement, timing and retention, content, and annual submissions.

Stakeholder involvement: Business stakeholders involved in the activity being assessed must be included in the risk assessment process.

Timing and retention: For new initiatives (those started after Jan. 1, 2026), businesses must complete risk assessments before processing begins and review those assessments at least every three years. For existing processing activities—those initiated before Jan. 1, 2026, that are ongoing—businesses will need to conduct a risk assessment no later than Dec. 31, 2027.

All risk assessments must be updated within 45 days of any material change in the processing or risks. All

versions of the assessments must be retained for a minimum of five years after completion or until processing is complete.

Content of a risk assessment: Each assessment must determine whether the privacy risks outweigh the benefits to the business, consumers and the public. The written report must include:

- Purpose of processing (without using generic terms)
- Categories of data involved, including sensitive personal information and minimization practices
- Operational details, including the method of collection/processing, length of retention, method of interacting with consumers (such as via a website), purpose of the interaction, approximate number of consumers affected, and the categories of third parties involved
- If ADMT is used, the report should include:
  - The ADMT's logic, assumptions and limitations
  - Output and how the output will be used to make a significant decision
  - If the business makes ADMT available to another business for a significant decision, it must provide the facts available to allow the business to conduct its own assessment.
- Benefits to the business, the consumer, stakeholders and the public
- Potential harms, with the source and cause of the harm, which may include:
  - Unauthorized access, destruction, modification and disclosure
  - Discrimination
  - Impairing control of personal information that interferes with consumers' ability to make their own choices
  - Coercing or compelling consent
  - Economic harms that affect economic opportunities, prices and compensation
  - Physical harm
  - Reputational harm
  - Psychological harm such as emotional distress and fear

Safeguards to mitigate risks: These may include, for example, encryption, privacy-enhancing technologies, network segmentation and bias testing.

Approval by an authorized decision-maker: Names and positions of the stakeholders involved should be included.

Businesses may reuse risk assessments conducted for other jurisdictions, such as the European Union's General Data Protection Regulation (GDPR) and Data Protection Impact Assessments (DPIAs) or Virginia's and Colorado's Data Protection Assessments (DPAs), as long as they meet California's content requirements.

Annual submissions: In previous drafts of the regulations, businesses were required to submit all risk assessments to the CPPA. This filing requirement was removed from the final version and replaced by an annual certified report.

Starting on April 1, 2028, businesses must submit an annual summary to the CPPA with the following:

- Time period covered
- Number of assessments completed
- Data categories assessed
- Certification by an executive attesting to compliance under penalty of perjury

The CPPA and the California Attorney General may request a copy of any risk assessment report, which must be submitted within 30 days of the request.

Next steps: To prepare for risk assessment obligations under the revised regulations, businesses should:

- Determine whether any in-scope activities are taking place
- Review existing DPIA templates (if any) and update as needed to address the new regulatory requirements
- Consider creating a process for conducting a risk assessment and test it before 2027

Related Professional

Jessica B. Lee . . . . . jblee@loeb.com