POLSINELLI

Publications

August 5, 2025 • Updates

What You Need to Know About California's Finalized CCPA Amendments: Part Two

On July 24, 2025, the California Privacy Protection Agency (CPPA) approved final regulations (the Rule) under the California Consumer Privacy Act of 2018 (CCPA), introducing new obligations related to automated decision-making (ADMT), mandatory risk assessments for high-risk data processing and cybersecurity. While Part One of our coverage on the Rule focused on the ADMT requirements, this section turns to the Rule's cybersecurity and risk assessment provisions. Assuming the Office of Administrative Law (OAL) approves these regulations (expected by late August 2025 based on its 30-day review period and past practices), certain provisions of the Rule could take effect on January 1, 2026. Key cybersecurity obligations are to be implemented in phases between 2027 and 2029, based on a business's gross revenue, with the CCPA determining that businesses with higher gross annual revenues are better able to bear the significant cost and complexity of compliance. Risk assessment reporting likely begins **April 1, 2028**, with businesses required to submit details for assessments completed in 2026 and 2027.

Key Highlights of the Rule

Cybersecurity:

- Requires annual cybersecurity audits for businesses meeting specific revenue and data processing thresholds.
- Mandates audits be conducted by qualified, independent auditors, with strict requirements for internal auditors.
- Specifies a set of 18 rigorous cybersecurity controls to be assessed in the annual audit, as applicable.
- Implements a phased timeline for businesses to complete their first audit based on revenue. For example, large organizations (i.e., with annual gross revenues exceeding $100 million in 2026) must complete their first audit report by **April 1, 2028**, covering the 2027 calendar year.

Risk Assessments:

- Imposes risk assessments before use of high-risk processing of personal information, such as processing sensitive data, use for training artificial intelligence (AI) systems,

Related People

- Laila Paszti
- Noor K. Kalkat
- Ashleigh Bickford

Related Capabilities

- Privacy & Cybersecurity
- US State Privacy Laws
- Artificial Intelligence & Machine Learning

use of ADMT for significant decisions, or selling or sharing of personal information.
- Requires that a senior executive certify the assessment, update every three years or after material changes and retain records for at least five years.
- Requires prescribed annual reporting to the CPPA starting **April 1, 2028**, summarizing completed assessments and certifying compliance.

Mandatory Annual Cybersecurity Audits for Businesses with "Significant Risk"

An annual cybersecurity audit requirement applies to companies that present "significant risk" to personal information security based on their size and the type of data processing. Specifically, this applies to any business with annual gross revenue over $25 million that processes personal information of 250,000 or more consumers or households or the sensitive information of 50,000 or more consumers, or any business that derives 50% or more of its annual revenue from selling or sharing consumer personal information.

The Rule establishes a phased timeline for when covered businesses must complete and submit their first audit report. The timeline is based on the business's annual gross revenue, giving smaller businesses more time to prepare. The current version of the Rule sets the following deadlines for the first audit:

- **April 1, 2028** for a business with an annual gross revenue for 2026 of $100 million or more.
- **April 1, 2029** for a business with an annual gross revenue for 2027 between $50 million and $100 million.
- **April 1, 2030** for a business with an annual gross revenue for 2028 of less than $50 million.

After April 1, 2030, the cybersecurity audit becomes an annual obligation for any business that meets the criteria at the start of each year.

Evaluating the Effectiveness of a Cybersecurity Program

The Rule prescribes a detailed set of requirements for annual cybersecurity audits to evaluate the effectiveness of a business's cybersecurity program. Each audit must assess the establishment, maintenance and implementation of the program over a 12-month period beginning January 1 of each year and must be conducted by an independent auditor using a recognized audit framework. Businesses do not submit the full audit report to the CPPA. Instead, they must file an annual certificate of completion, signed by management, confirming that the audit was conducted. This certificate is due by April 1 of the year following the audit.

Audits may be conducted internally or externally by qualified professionals with knowledge of cybersecurity and auditing practices, so long as they maintain independence and objectivity. The Rule stipulates that internal auditors cannot participate in any business activities they may assess in current or future audits (e.g., implementing or maintaining a cybersecurity program) nor can they report to an executive who is directly responsible for the cybersecurity program. Companies that have traditionally relied on their IT or cybersecurity teams for cybersecurity audits will need to engage independent personnel or external auditors to meet the Rule's independence requirements.

Although assessing the "effectiveness" of a cybersecurity program involves auditor judgment, such evaluation must reflect the business's size, complexity and processing activities and take into account both state-of-the-art practices and the cost of implementation. Auditors must evaluate a defined set of 18 core controls, as applicable, against a business's cybersecurity program. Certain controls listed in the Rule, such as

access control and authentication, encryption in transit, incident response and vulnerability patching, are commonly found in mature cybersecurity programs. Other controls, such as phishing-resistant multi-factor authentication or comprehensive secure software development, may not be fully implemented by businesses, even in well-established cybersecurity programs, given their complexity, cost and skill requirements. If a business wants to rely on an existing cybersecurity assessment (e.g., one based on the NIST Cybersecurity Framework or HIPAA Security Rule), it cannot treat that assessment as an automatic substitute for the CCPA-mandated audit. Most of those frameworks are risk-based, allowing businesses flexibility in implementing safeguards, while the Rule is more prescriptive. An auditor wanting to rely on such previous assessments will need to evaluate them against the 18 specific components identified in the Rule, determine whether supplementation is needed, and ensure compliance with reporting standards and independence (which may limit the ability to use prior internal assessments prepared by IT teams).

Risk Assessments for Processing Activities with "Significant Risk"

The Rule requires businesses to complete a risk assessment before initiating any personal information processing activity that includes "significant risk" and to review or update each assessment at least once every three years or within 45 days of any material change. Activities with significant risk include processing sensitive information, using personal data to train an ADMT or biometric system, profiling individuals in sensitive contexts, deploying ADMT for a significant decision (as discussed in Part 1), or selling or sharing personal data. Once approved by the OAL, the risk assessment provisions will likely take effect on January 1, 2026. However, the Rule includes a lookback requirement: businesses must complete risk assessments for activities already in progress prior to the effective date by December 31, 2027. Rather than submitting full assessments, the Rule requires businesses to provide the CPPA with an annual certified report beginning April 1, 2028 with prescribed information. Businesses must also maintain complete documentation for each assessment, as the CPPA or California Attorney General may request copies at any time, with 30 days' notice.

Scope of a Risk Assessment

Risk assessments must describe the activity in detail, including data categories, collection methods, retention periods and consumer disclosures; evaluate the benefits and potential harms such as discrimination or loss of control; and outline safeguards to mitigate those risks. While the CPPA dropped a ban on high-risk activities, the Rule intends to limit processing where risks to the consumer are disproportionate to benefits.

Businesses must also develop internal processes to identify activities that pose heightened privacy risks, perform structured risk assessments and maintain evidence of compliance. This marks a clear move toward preventative privacy governance, shifting away from reactive measures. Businesses that fail to complete required assessments before engaging in high-risk processing could face regulatory consequences.

What to Do Now

With the Rule introducing complex, phased compliance obligations that may require significant allocation of financial and human resources, especially for businesses that may not have a mature cybersecurity program, businesses will want to get head start on understanding their obligations under the Rule.

Key steps include:

- Review the business's current cybersecurity program against the 18 required controls

and identify gaps.

- Decide whether audits will be conducted internally or by external firms and confirm that internal auditors meet independence requirements.
- If relying on NIST, HIPAA or other frameworks, map them to the 18 controls and plan for supplementation as needed.
- In light of the lookback requirement for significant-risk activities predating the Rule's effective date for risk assessments, establish procedures to identify such activities and implement necessary practices and procedures (e.g., strong documentation practices to ensure information required for assessments is available and complete).
- Ensure executive buy-in, as certifications for both audits and risk assessments will require sign-off from senior leadership.
- Budget for additional resources, especially for advanced cybersecurity controls (e.g., phishing-resistant MFA, penetration testing, zero trust).