faegre drinker

September 02, 2025

Cybersecurity Audits Under the California Consumer Privacy Act (CCPA)

Audits Must Address 18 Key Components

Authors: Peter A. Blenkinsop, Reed Abrahamson, Doriann H. Cain, Simonne Brousseau, Charles E. Westerhaus

At a Glance

- Certain California businesses that handle high revenue or large volumes of sensitive personal data must conduct and document annual cybersecurity audits, covering 18 technical and organizational areas. This requirement begins between 2028 and 2030, depending on revenue size.
- Audits may be conducted by independent internal or external auditors, and prior audits can be reused if they meet the new regulatory standards.
- These provisions were unanimously approved by the California Privacy Protection Agency in July 2025 and are pending final review and effective date confirmation by the Office of Administrative Law.

Recent rulemaking activities under the California Consumer Privacy Act (CCPA) have created a new duty to conduct and document a robust "cybersecurity audit" for certain businesses. See Cal. Code Regs. tit. 11, §§ 7120-7124. The audit requirement is the first of its kind among state data privacy laws of general applicability, and it may involve a significant compliance effort for the businesses within its scope. Although the first cybersecurity audits will not be required until 2028 (as discussed below), companies that do business in California should be mindful of this significant development in privacy and cybersecurity law.

Overview

Under the CCPA regulations, a cybersecurity audit is a comprehensive evaluation of a business's cybersecurity program and its ability to protect personal information from unauthorized access and use. See Cal. Code Regs. tit. 11, § 7123(a). The duty to conduct the audit applies to any business whose processing of personal information presents a "significant risk to consumers' security." *Id*. at § 7120(a). The regulations identify three categories of businesses whose processing meets this threshold, namely, any business that:

1. Derives 50% or more of its annual revenue from the sale or sharing of personal information.
2. Processes the personal information of more than 250,000 consumers or households.
3. Processes the sensitive personal information of more than 50,000 consumers. *Id*. at § 7120(b).

The cybersecurity audit may be conducted by an external or internal auditor, provided that the auditor is sufficiently independent and qualified. *Id*. at § 7122(a). The regulations contain relatively strict criteria for ensuring the auditor's independence and qualification. For instance, the auditor must report to a member of the business's management team who "does not have direct responsibility for the cybersecurity program," and the auditor must be able to request any information from the business that is "relevant to the cybersecurity audit." *Id*. at § 7122(a-b).

The cybersecurity audit must address 18 technical and organizational components of the business's cybersecurity program that the "auditor deems applicable to the business's information system." *Id*. at § 7123(b-c). These components include:

1. Authentication.
2. Encryption of personal information, at rest and in transit.
3. Account management and access controls.
4. Inventory and management of personal information and the business's information system.
5. Secure configuration of hardware and software.
6. Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).
7. Audit-log management, including the centralized storage, retention and monitoring of logs.
8. Network monitoring and defenses.

9. Antivirus and anti-malware protections.
10. Segmentation of an information system.
11. Limitation and control of ports, services and protocols.
12. Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.
13. Cybersecurity education and training, including training for each employee, independent contractor and any other personnel to whom the business provides access to its information system (e.g., when their employment or contract begins, annually thereafter, and after a personal information security breach).
14. Secure development and coding best practices, including code reviews and testing.
15. Oversight of service providers, contractors and third parties.
16. Retention schedules and proper disposal of personal information are no longer required to be retained, by (1) shredding, (2) erasing or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.
17. How the business manages its responses to security incidents.
18. Business-continuity and disaster-recovery plans, including data-recovery capabilities and backups. *Id*. at § 7123(c).

The results of the audit must be compiled in a cybersecurity audit report that is signed by the auditor and provided to the business's management. *Id*. at § 7123(e). The report must describe the business's cybersecurity program and "identify and describe in detail" any gaps that would increase the risk of unauthorized access or use of personal information. *Id*. The report must be based on the "specific evidence" examined by the author, rather than the assertions or attestations of the business's management. *Id*. Critically, however, a business may rely on another cybersecurity audit that it prepared for another purpose — such as NIST's Cybersecurity Framework 2.0 — provided that the other audit satisfies the same requirements under the CCPA, "either on its own or through supplementation." *Id*. at § 7123(f).

For every year that a business must complete a cybersecurity audit and report, the business must submit a signed certification of completion to the California Privacy Protection Agency (CPPA) by April 1 of the following year. *Id*. at § 7124. These requirements become effective between 2028 and 2030 in a phased approach based on annual gross revenues:

- Companies with annual gross revenues of more than $100 million in 2026 will be required to conduct

cybersecurity audits by April 1, 2028, covering the period from January 1, 2027, to January 1, 2028.

- Companies with annual gross revenues of more than $50 million and less than $100 million in 2027 will be required to conduct cybersecurity audits by April 1, 2029, covering the period from January 1, 2028, to January 1, 2029.
- Companies with annual gross revenues under $50 million in 2028 will be required to conduct cybersecurity audits by April 1, 2030, covering the period from January 1, 2029, to January 1, 2030.

Next Steps

The provisions addressed above were introduced as part of a broader set of regulatory updates to the CCPA, which the CPPA voted unanimously to approve on July 24. The vote was the culmination of a rulemaking process that began in November 2024 and featured several rounds of public feedback. As of this writing, the revised regulations have been submitted to California's Office of Administrative Law (OAL) for final review, and the OAL has 30 days from its receipt of the revised regulations to approve or deny them. Cal. Gov't Code § 11349.3. Once approved, OAL will then determine the effective date of the revised regulations.

Although the CCPA's cybersecurity audit requirement is the first of its kind among state data privacy laws of general applicability, it is not the first example of a state-level cybersecurity audit requirement. Indeed, New York's cybersecurity regulations, as amended in November 2023, require "class A" financial services companies to conduct an "independent audit" of its cybersecurity program. N.Y. Comp. Codes R. & Regs. tit. 23, § 500.2(c). The New York regulations define this term as "an audit conducted by internal or external auditors free to make decisions not influenced by the covered entity being audited or by its owners, managers or employees." *Id*. at § 500.1(h). Likewise, a company is designated as "Class A" when it has greater than $20,000,000 in gross annual revenue in each of the last two fiscal years from all business operations and:

1. "[O]ver 2,000 employees averaged over the last two fiscal years, including employees of both the covered entity and all of its affiliates no matter where located; or
2. Over $1,000,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates no matter where located." *Id*. at § 500.1(d).

Unlike the regulations to the CCPA, however, the New York financial services regulations provide little guidance concerning the scope of the audit requirement. For instance, the New York regulations do not address who may serve as the auditor, what must be included in the auditor's reports or when the audit must be completed.

Legal clerk John L. Evans contributed to the preparation of this article.

MEET THE AUTHORS

Peter A. Blenkinsop

Partner

+1 202 230 5142
Washington, D.C.

peter.blenkinsop@faegredrinker.com

Reed Abrahamson

Partner

+1 202 230 5672
Washington, D.C.

reed.abrahamson@faegredrinker.com

Doriann H. Cain

Partner

+1 317 569 4837
Indianapolis

doriann.cain@faegredrinker.com

Simonne Brousseau

Associate

+1 202 230 5260
Washington, D.C.

simonne.brousseau@faegredrinker.com

Charles E. Westerhaus

Associate

+1 312 569 1144
Chicago
Indianapolis

charles.westerhaus@faegredrinker.com

Related Legal Services

Government & Regulatory

Litigation

Labor & Employment

Privacy, Cybersecurity, Data Ethics & Strategy

Privacy Litigation

HR Compliance, Training & Transactions

Related Industries

Consumer Products & Retail