

[Blogs](#)

March 28, 2019

CCPA 12-Month Compliance Series Part 3: Conduct a Gap Analysis

After conducting a data inventory (*see* [Part 2](#) of our CCPA series), a business should assess its risks by benchmarking its policies and practices with applicable privacy laws and regulations. Conducting a gap analysis is a critical tool in identifying compliance gaps and developing a plan to bridge those gaps. *See e.g.*, [Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission & Others v. Vizio, Inc.](#), No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), Document 1-3 at 5 (privacy program includes addressing privacy risks related to the development and management of new and existing products and services) and CNIL (the French Data Protection Authority) Guidance on [Six Steps for GDPR Compliance](#) (step three to identify actions to comply with current/future obligations and to prioritize such actions based on risks).

A typical gap analysis does the following: (1) lays out the applicable legal requirements/standards; (2) identifies the business's relevant policies and practices; (3) analyzes the ways in which the business is or is not compliant as to each legal requirement/standard; and (4) provides detailed recommendations on the steps it can take to establish substantial compliance. A gap analysis for CCPA implementation should take into consideration any steps a business has already taken for GDPR compliance and provide strategic guidance on how it can leverage prior GDPR compliance efforts in implementing CCPA requirements.

Conducting a gap analysis as part of developing a comprehensive privacy program allows a business to proactively identify the privacy and data security risks and mitigate them. With a comprehensive understanding of its risks, a business can properly allocate resources to the gaps of varying risk levels and can make sure its policies and procedures are in compliance with the law. Finally, by implementing the recommendations set forth in a reliable gap analysis, a business can demonstrate substantial compliance to stakeholders as well as in response to enforcement actions.

Authors

Explore more in

[Privacy & Security](#)