Davis Wright Tremaine LLP

CCPA Cyber Audit Regulations: Is Your Organization Ready?

Michael T. Borgia
Partner, DWT

Andrew M. Lewis
Counsel, DWT

Andrew Belsick
Director, BDO USA

Today’s Speakers

Michael T. Borgia

Partner, DWT

Washington, D.C.

michaelborgia@dwt.com

Andrew M. Lewis

Counsel, DWT

San Francisco, CA

andrewlewis@dwt.com

Andrew Belsick

Director, BDO USA

Pittsburgh, PA

abelsick@bdo.com

CCPA Overview

- California Consumer Privacy Act (CCPA):
  - Enacted in 2018, first went into effect in 2020.
  - "Comprehensive" state privacy law: disclosures, consumer rights, opt out of "sale," etc.
  - "Personal information" defined broadly: includes info 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."
  - "Consumers" include employees, consultants, job applicants, as well as consumers.

- Amended by the California Privacy Rights Act (CPRA) in 2020:
  - Created the California Privacy Protection Agency (CPPA or CalPrivacy).
  - Granted CalPrivacy enforcement powers and rulemaking authority on numerous topics—including cyber audits (CA AG originally had more limited rulemaking authority).

KEY POINT: The cyber audit regs are cybersecurity provisions *built into a privacy law*. Coordination between privacy and security on key terms and concepts is essential.

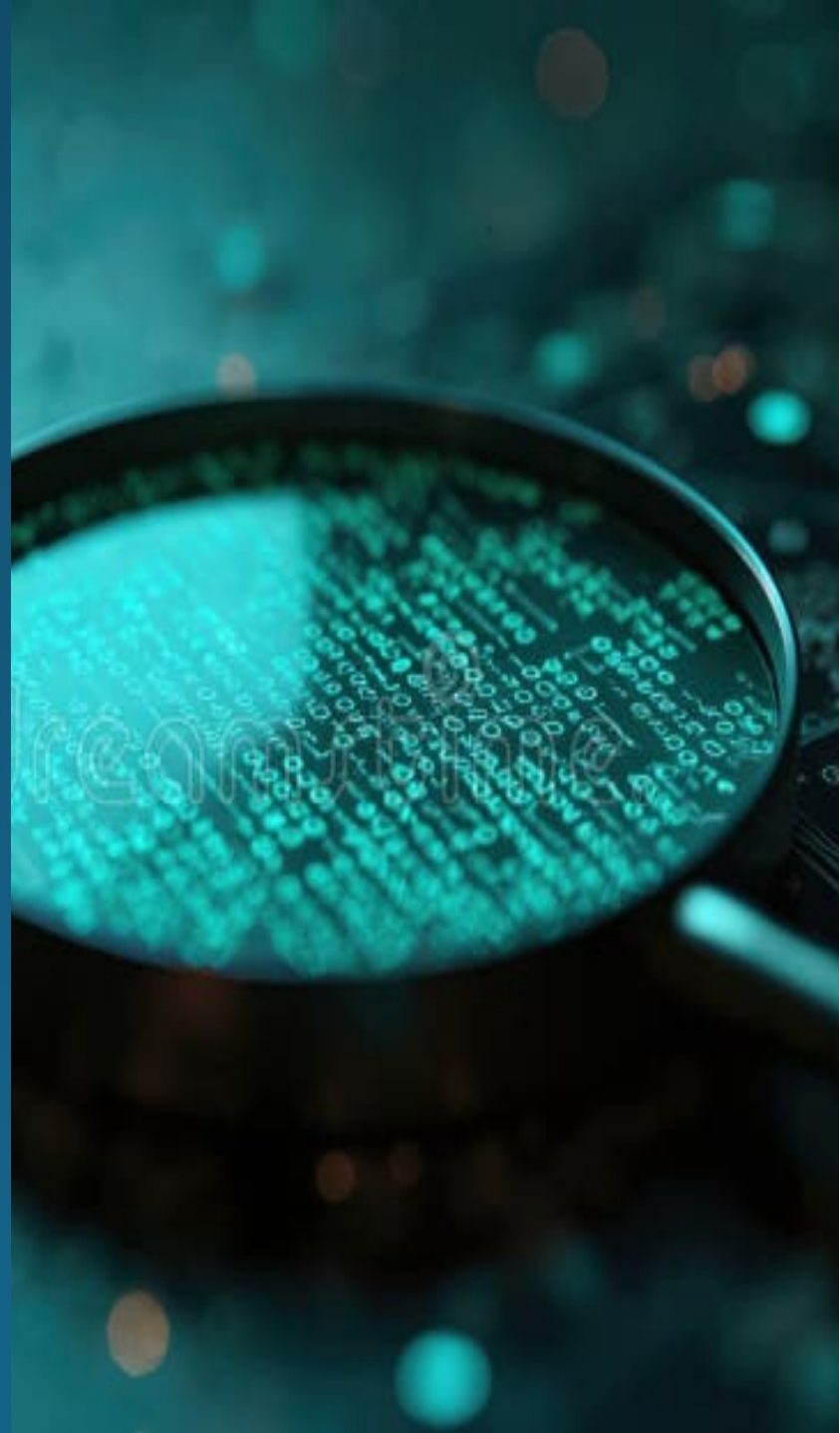
Development of the Cyber Audit Regulations

Requirement to Conduct Cybersecurity Audits

Every business whose processing of consumers' personal information presents significant risk to consumers' security … must complete a cybersecurity audit.

The cybersecurity audit must assess ("audit scope"):

- How a cybersecurity program protects personal info from unauthorized access, destruction, use, modification, disclosure and loss of availability.
- Establishment of a written cybersecurity program appropriate to business's size, complexity, nature and scope of processing activities, taking into account state of the art and costs of implementation.
- Implementation of 18 control areas that the auditor deems applicable.
- How the business implements and enforces compliance with its cybersecurity program.



Covered Businesses and Compliance Dates

Businesses that must perform cybersecurity audits (processing presents "significant risk"):

- Derives 50% or more of its annual revenues from selling or sharing consumers' personal information, OR
- Gross annual revenue of $25M ($26.6M adjusted) AND
  - Processed personal info of 250,000 or more consumers/households, OR
  - Processed sensitive personal info of 50,000 or more consumers.

Date for first audit staggered by revenue:

- Over $100M: first certification due April 1, 2028 (audit covers 2027 based on 2026 triggers).
- $50M–$100M: due April 1, 2029 (audit covers 2028 based on 2027 triggers).
- Under $50M: due April 1, 2030 (audit covers 2029 based on 2028 triggers).

Annual audit required thereafter (by April 1 for prior year).

Business v. Service Provider

- Only **businesses** are required to conduct cybersecurity audits.
- **Service providers** are required to "cooperate with *the business* … [i]n *the business's completion* of *its* cybersecurity audit."
- Where appropriate, businesses must obligate service providers by contract to provide such assistance.

FAQs:

- **What if your company is a "business" but only meets the "significant risk" thresholds for conducting cyber audits as a "service provider"?**
- **How do I know if my company "processes" personal info?**

Audit Controls

The audit must evaluate the effectiveness of the cybersecurity program across 18 control areas, including:

- Authentication
- Encryption at rest and in transit
- Account management and access controls
- Data inventory and asset management
- Secure hardware and software configuration
- Penetration testing and vulnerability scans/disclosure
- Audit-log management
- Network monitoring and defenses
- Antivirus and antimalware protection
- Segmentation of an information system (firewalls)
- Limitation and control of ports, services, and protocols
- Secure development and coding best practices
- Service providers, contractors, and third parties
- Retention schedules and personal information disposal
- Security incident response management
- Business continuity and disaster recovery plans
- Cybersecurity awareness
- Cybersecurity training

Audit Scope—What Systems are Covered?

- A CCPA cybersecurity audit must cover **all information systems that process, enable or provide access to, or are relied upon to protect personal information.**
- Information system includes systems **"regardless of whether the business owns those resources."**
- **Personal information is broad under the CCPA** and means 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.

Audit Mechanics: An Example
Access Controls

The cybersecurity audit must assess a business' "account management and access controls," including:

> Restricting each person's, account's, or application's privileges and access to personal information to what is necessary for that person, account, or application to perform their duties.

Audit Mechanics: An Example
Data Mapping

The cybersecurity audit must assess a business' "[i]nventory and management of personal information and the business's information system," including:

- Personal information inventories (e.g., maps and flows identifying where personal information is stored and how it can be accessed) and the classification and tagging of personal information (e.g., how personal information is tagged and how those tags are used to control the use and disclosure of personal information)

Audit Mechanics: An Example

	Access Control	Data Mapping
Evidence/Testing	• Sample new hires and appropriateness of granted access • Sample terminations and verify access is removed • Inspect system administrators for appropriateness	• Sample systems that contain personal information and inspect data mapping/tagging • Inspect data loss prevention/scanning results to identify unknown personal information locations
Timeframe	• Sampling and inspection during “interim” and “year-end”	

Auditor Independence & Qualifications

- Audits must be conducted by a "qualified, objective, and independent professional" (internal or external).
- Independence means decision-making free from influence by the business being audited.
- Audit must use "procedures and standards accepted in the profession of auditing" (e.g., ISACA).
- The auditor must document qualifications and the work performed.
- Highest-ranking auditor must provide signed certification with audit report that they completed the audit, exercised "objective and impartial judgment," and did not rely on management assertions.
- If an internal auditor is used:
  - The auditor must report directly to member of executive management that does not oversee the cybersecurity program (e.g., Audit Committee).
  - 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.

Required Contents of Audit Report

Audit report must:

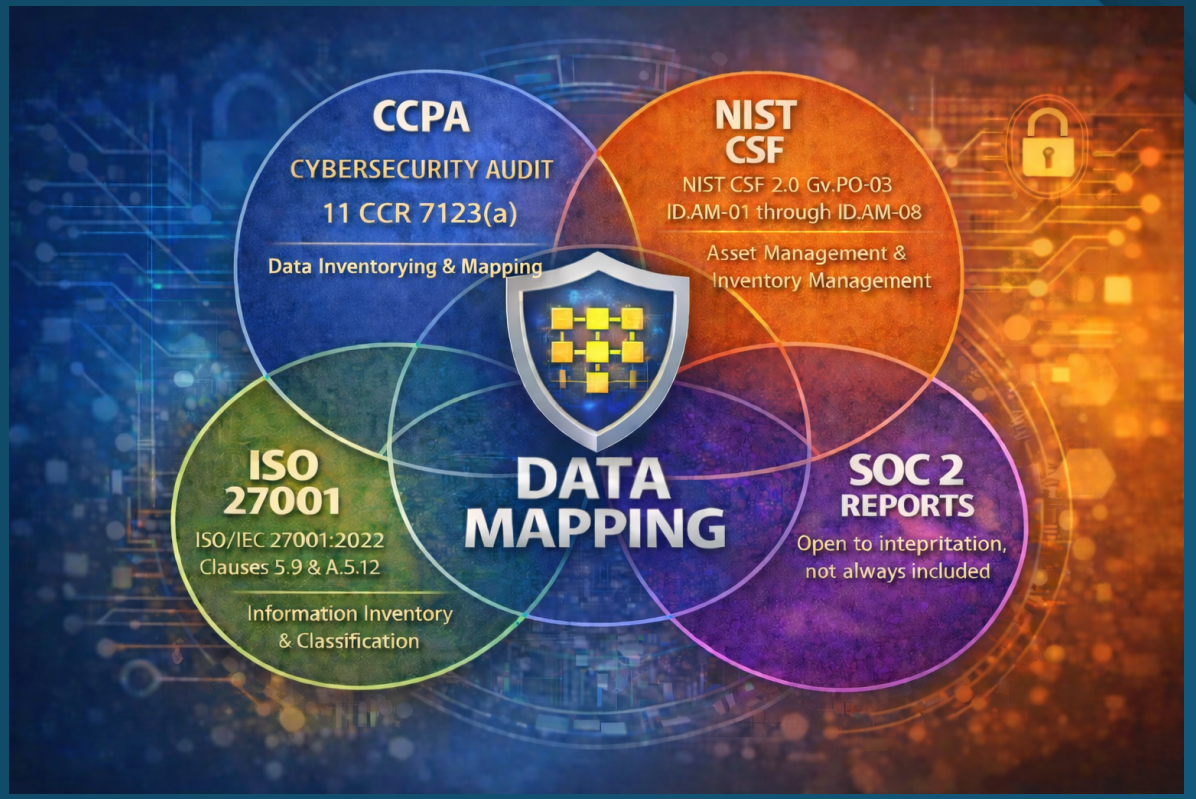
- Describe the cyber program, the criteria used for the audit, and the evidence reviewed
- Explain why the evidence justifies the auditor's findings
- Identify how the business has implemented the 18 controls and addressed the other audit requirements
- Identify and describe gaps or weaknesses
- Document the business's plan to address those gaps or weaknesses
- Provide copies of any breach notifications from the business

Audit report must be provided to member of business's executive management team "who has direct responsibility" for the cyber program.

Audit Reciprocity

- Businesses may use a cybersecurity audit, assessment, or evaluation that they prepared for another purpose to satisfy the cyber audit requirement.
- ***However,*** the alternative report must still meet all the CCPA cybersecurity audit's requirements, either on its own or with supplementation.
- Reg cites NIST CSF v. 2.0 as an example

Audit Reciprocity



Certification to the CPPA

- Each calendar year (April 1) 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.
- The written certification must be completed by a member of the business' executive management team who:
  - Is directly responsible for the business's cybersecurity-audit compliance;
  - Has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and
  - Has the authority to submit the business's certification to the Agency.
- No requirement to file the audit report with CPPA.

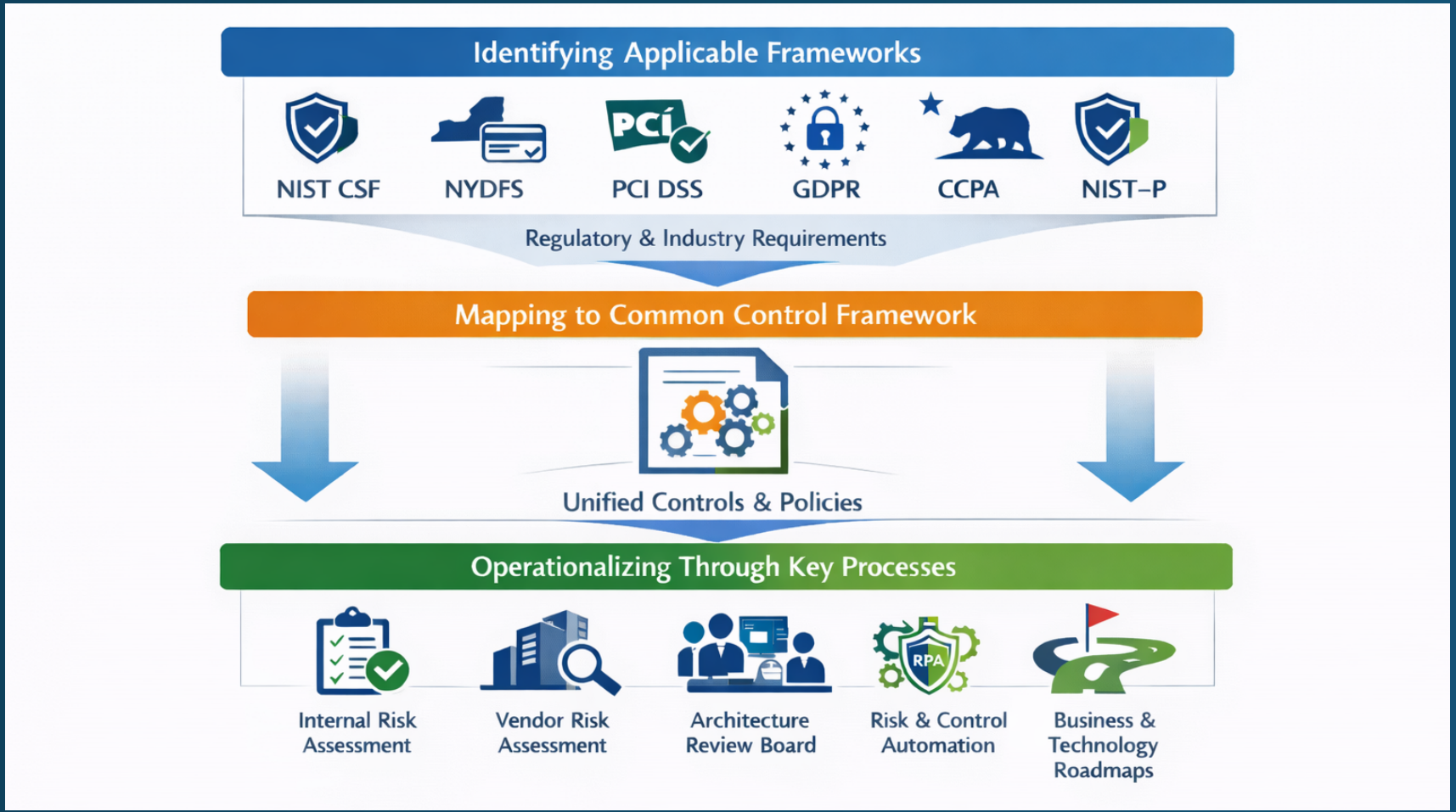
Certification to the CPPA

- Attestation includes: “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.”

Considerations for Attestants

- Decide early who will sign the CPPA certification.
- The attestation requires the individual to attest based on knowledge of the audit.
- Understand how the signatory will acquire sufficient knowledge. Simply reading the audit report may not be enough!
- Potential liability concerns:
  - A false statement is made “knowingly” when it:
    a) is made with ***actual knowledge*** that the statement is false (i.e., where the person making a statement knows a material fact to be true but says otherwise)
    b) is ***deliberately ignorant of the truth or falsity of the information*** (i.e., where the person is aware of a substantial risk that their statements are false, but intentionally avoids taking steps to confirm the statements’ truth or falsity), or
    c) has ***reckless disregard for the truth or falsity of the information*** (i.e., where the person is conscious of a substantial risk that their claims are false, but submits the claims anyway).

Common Control Frameworks



Cybersecurity Audits: Compliance Priorities and Takeaways

Identify and work with your attestant.

- Identify the executive who will sign the annual CPPA certification; brief them on scope and expectations.

Select an independent, qualified auditor.

- Confirm independence (internal or external) and reporting lines that avoid oversight conflicts with the cybersecurity program; document auditor experience and authority to obtain information.

Map and gap against the enumerated controls.

- Perform a readiness assessment against the CPPA's control list; align remediation plans to NIST CSF/CIS Controls while tracking back to the regulation.

Build an audit evidence plan.

- Define artifacts, testing procedures, and sampling; maintain workpapers, qualifications, and supporting materials for at least five years.

Plan timelines and filings.

- Align your audit cycle to the certification deadlines; establish an annual cadence for certification and retention of the audit documentation.

Strengthen vendor and data governance.

- Update contracts and oversight for service providers; refresh data inventories, retention schedules, and secure disposal procedures.

Exercise incident response.

- Run tabletop exercises; verify detection, logging, escalation, and post-incident review are operating effectively.

Coordinate with privacy team.

- Establish common understanding of the CCPA definitions.

Questions? Reach out!

Michael T. Borgia

Partner, DWT

Washington, D.C.

michaelborgia@dwt.com

Andrew M. Lewis

Counsel, DWT

San Francisco, CA

andrewlewis@dwt.com

Andrew Belsick

Director, BDO USA

Pittsburgh, PA

abelsick@bdo.com


Davis Wright
Tremaine LLP