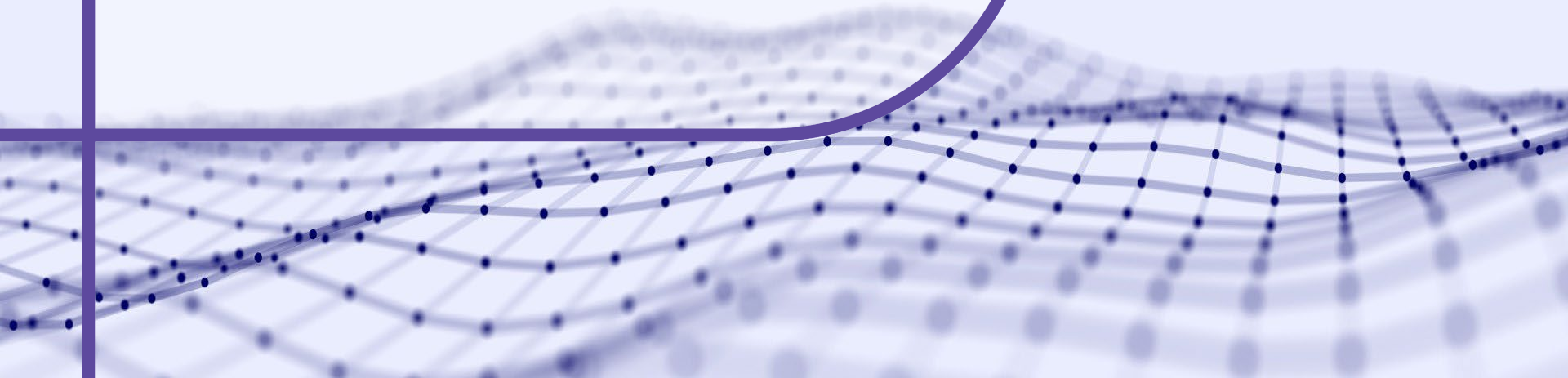
Perkins Coie

THE COMPLIANCE COLLECTIVE

Cybersecurity Compliance: New Requirements and Essential Strategies

NOVEMBER 20, 2025
PRESENTED BY: AMELIA GERLICHER, DAVID AARON, ANDREW PAK



Presenters

Amelia Gerlicher
Partner

David Aaron
Senior Counsel

Andrew Pak
Senior Counsel

Agenda

- Data Security Regulation + Recent Trends
- Working with the NIST Cybersecurity Framework
- Working with Legal

Data Security Regulation

Overview of U.S. Approaches

Perkins Coie

In 2024...

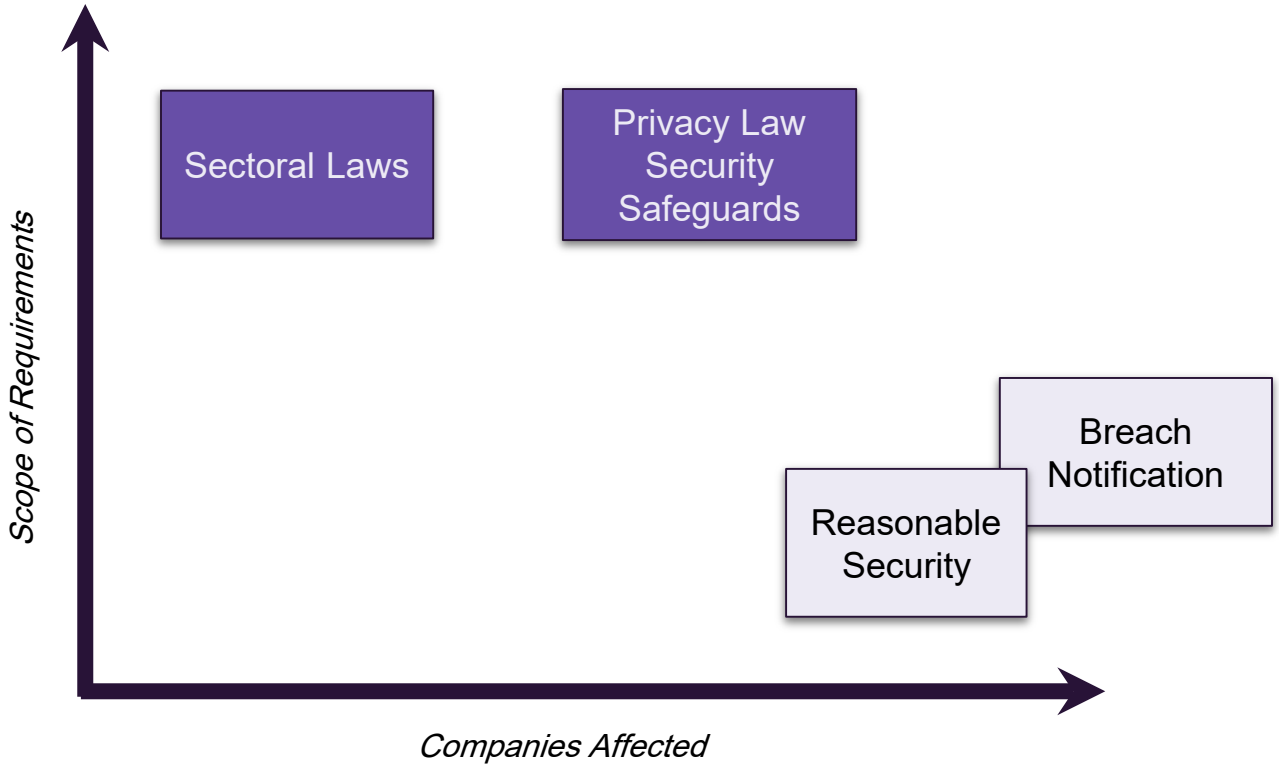
5,000
Breaches

1.35B
Affected people

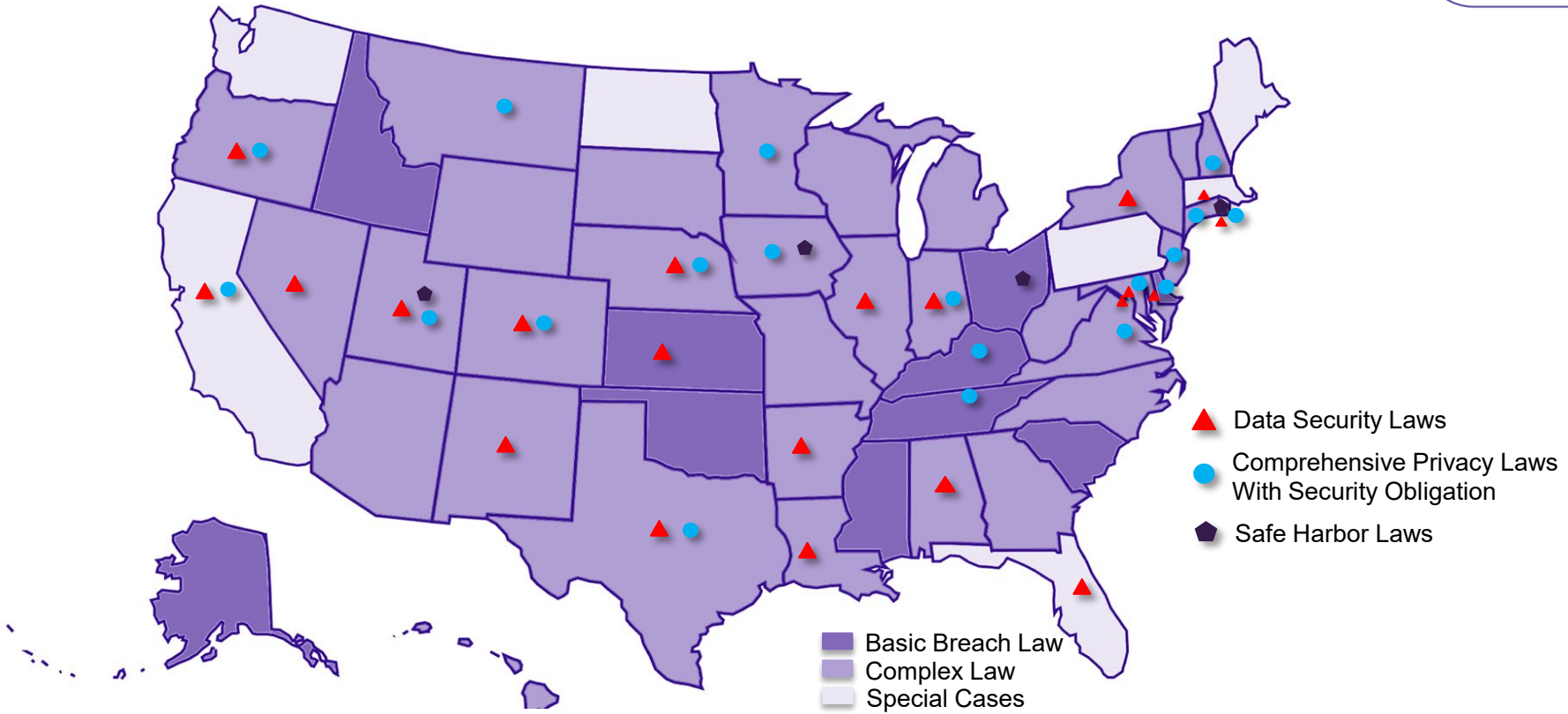
$813M
Ransom paid

$10.5T
Business costs

U.S. Security Laws

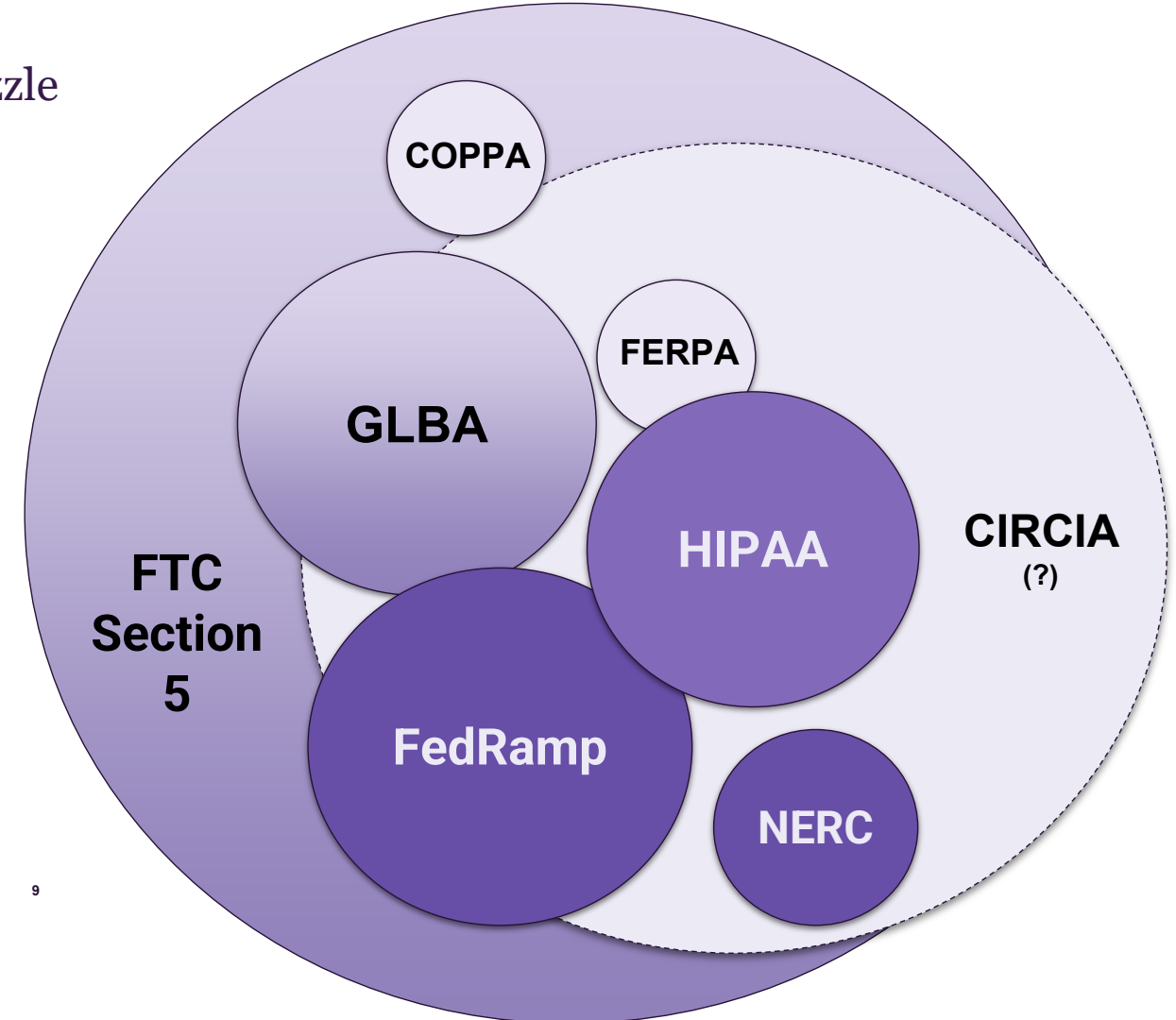


U.S. Security and Breach Landscape



See PerkinsCoie.com/StateBreachChart

The Federal Puzzle (circa 2023)



What’s New?

New(ish) Federal Cyber Regimes

COPPA

For businesses processing children's information:

- Specific security program requirements
- Risk assessment + annual revisit
- Retention policy and regular deletion

Effective June 2025

Safeguards Rule

For nonbank financial businesses

- Lengthy list of security program requirements
- Risk assessment + annual revisit
- Monitoring and Board reporting requirements
- Incident response plan and notice to the FTC

Effective June 2024

EO 14117, DOJ Data Security Program, CISA Controls

For U.S. persons transferring data abroad

- Regulates transfers of U.S. persons' sensitive data to threat countries
- Compliance analysis often requires data mapping
- Long-term compliance:
  - Implementing CISA Level I & II security controls
  - Periodic audits

Effective July 2025

Department of Defense - Controlled Unclassified Information

For government contractors

- Affirmative security obligations
  - CMMC (requirements rolling out)
    - 3 assessment levels
    - No more self-certification
  - DFARS 7012
  - NIST SP 800-171 (federal contractors/CUI)

- Aggressive incident reporting timeline and scope
- False Claims Act/Whistleblowers

Effective November 2025

Other Specific Security Requirements (Federal & State)

Perkins Coie

And don't forget…

- HIPAA
- FTC Section 5
- NYDFS
- NERC-CIP
- GLBA (for other institutions)

What's New:

CCPA Cyber Audit Requirements

Who is covered by the cyber audit requirement?

"Businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security [shall] perform a cyber security audit on an annual basis."

Cal. Civ. Code 1798.185

Business: CCPA defined term meaning entity that determines the means and processing of customers' PI (+ revenue or # threshold)

Significant Risk = data broker *or* revenue + *processing* threshold

- Minimum annual gross revenue ($26.6M, inflation adjusted)
- 250,000 CA consumers' PI *or* 50,000 CA consumers' sensitive PI

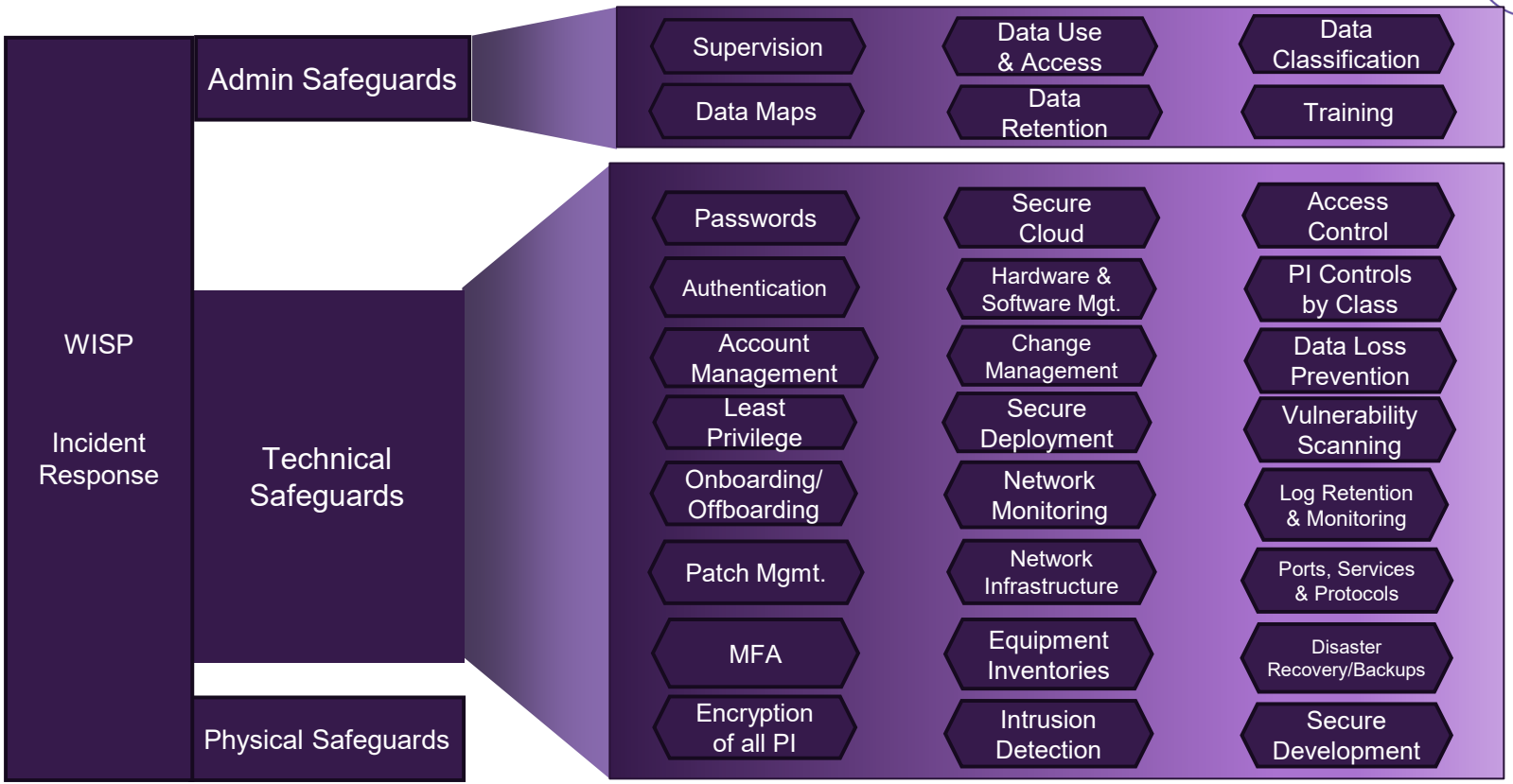
➔ Contractors and service providers can be covered by virtue of their processing activities only

Thorough and Independent Annual Audit

- **Qualified, objective, independent professional auditor** with knowledge of cybersecurity
  - Internal: May not participate in cybersecurity otherwise and must report to different executive reporting line
- **Evidence** required; may not rely primarily on assertions
- Covering calendar year; report due following April 1

AUDIT SCOPE	➢ Assess how the **program** protects personal information, including documentation, implementation, and compliance ➢ Required consideration of 45 controls across 18 areas ➢ Plus anything else the company does to secure PI

Components of Information Security Program in California



California-Specific Audit Report

- Articulates the **processes, activities, and components** reviewed, including evidence and documentation
- Identifies the statutory components reviewed and **their effectiveness** in protecting personal information
- Identify and **describe in detail** the status of any **gaps and weaknesses** that increase risks to PI
    - Must proactively identify any extra components that increase risk
- **Document plan** + time frame to address gaps
- Identify changes to any prior reports
- Identify all **CA breach notices** (to consumer or regulator)

Enforcement

- Report completion and independence is **certified** to CalPrivacy by executive - not submitted
- CalPrivacy can—and we expect will—request as part of investigatory authority
- Requirement is the **audit and its thoroughness**, not the controls themselves
    - But, we expect enforcement will be based on lack of controls
- Enforcement authority includes **fines** up to **$2,663** for each violation or **$7,988** for each intentional violation

Challenges

Different scope, specificity, purpose	• Requirements based on data, identity, purpose, business line • Lack of clarity–or too much clarity–on required elements
Different timelines and audience	• Regulators require different reports, assessments, and audits at different times • Regulator priorities differ from each other and the company
Legal risk from the process and the program	• Direct compliance risk • Required audits/assessments generally not privileged • Third-party litigation risk

Using CSF

Can we use another audit?

(f) A business may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose, provided that it meets all of the requirements of this Article, either on its own or through supplementation. For example, a business may have engaged in an audit that uses the **National Institute of Standards and Technology Cybersecurity Framework 2.0** and meets all of the requirements of this Article.

Can we use another audit?

If it meets all the requirements

- Scope includes written program plus all listed controls deemed applicable to the company's protection of personal information
- Assesses effectiveness of protecting personal information
- Report describes gaps and weaknesses and timeline to fix

Alignment with other frameworks varies

- All controls align with CSF
- Chosen control regimes (SOC 2, ISO) will need review and alignment

NIST Cybersecurity Framework (CSF) 2.0

NIST Cybersecurity Framework (CSF) 2.0

What?

–Think of it as an approved list of the right questions that will give you the facts you need to be able to engage with any set of cybersecurity requirements. In this case, it's a list of about 100 assertions about what your organization can or cannot say about its overall security program.

Where?

–Within a tracker that you maintain internally, that you and your teams can draw from as needed, and that contains references to the evidence you would use in an audit or exam to support your representation.

When?

–Before you have the audit.

NIST Cybersecurity Framework (CSF) 2.0

Why?

–To account for the significant redundancy/overlap between any and all cybersecurity requirements because the same set of facts (and support for such facts) will be relevant to more than one requirement (e.g., CCPA and NY DFS Part 500).

How?

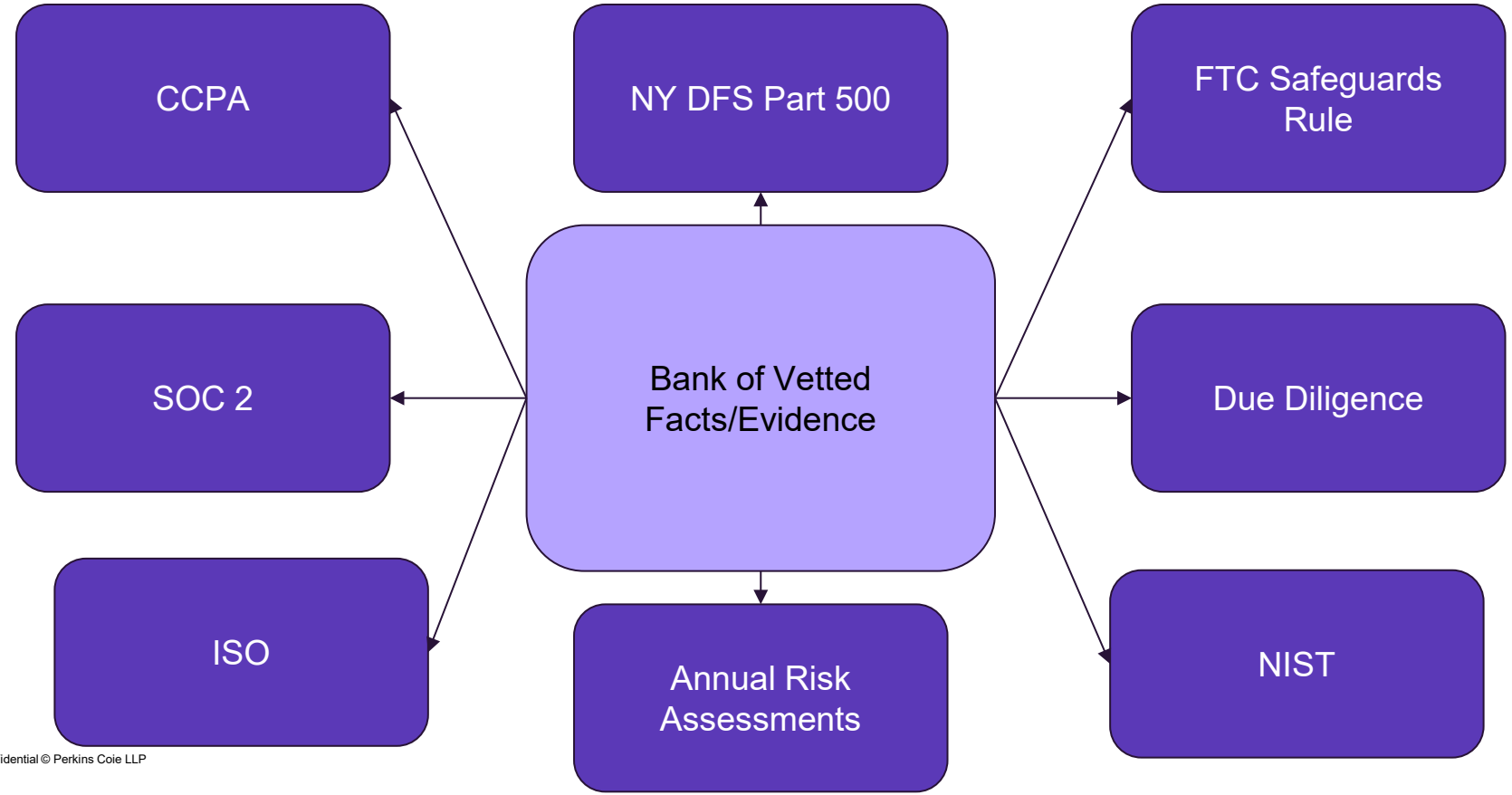
–It creates a bank of assertions or representations your organization can or cannot make about what it does from a security perspective.

–If someone asks you what your organization does in terms of cybersecurity, are you generally looking at your internal policy to answer those questions? Those policies are directives, the collection of findings that are tracked in assessments like the CSFaddress the issue of “how you would prove you do those things.”

Who?

–Legal, if you want to claim privilege over any aspect of the pre-audit work.

Value Proposition



Audit Tools

Frameworks

–NIST Cybersecurity Framework (CSF) 2.0

–CRI Profile

Security Program Review

What?

–Legal assessment + review of security policy stack for compliance

Why?

–Security-drafted policies often are not legally compliant from regulatory perspective

–Changing privacy law requirements add investigative potential

Involving Legal

Why involve Legal?

External validation

Involving counsel provides a lens outside of cyber/audit frameworks, focused on legal compliance and clarity. Attorneys can also bring a unique lens as to how statements might be interpreted by potential litigants and regulators.

Candid discussions about legal risk

Security audit work that is not under privilege is subject to later disclosure to regulators, litigation opponents, and other third parties. This either limits candor or creates potentially damaging records in future litigation.

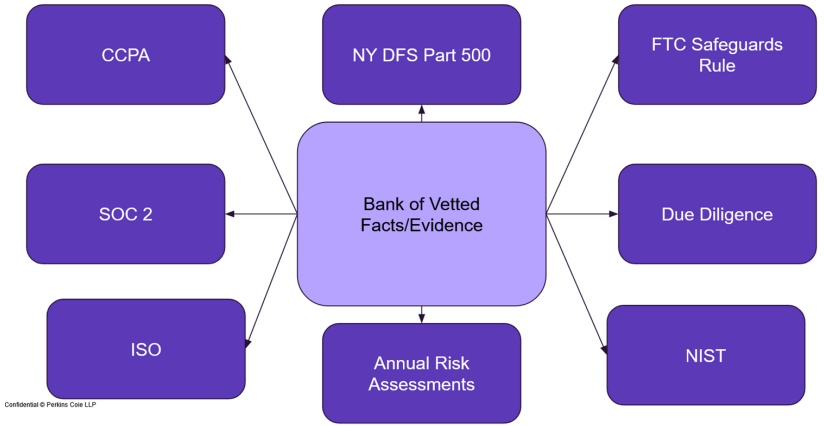
A Brief Reminder on Attorney-Client Privilege

- **Communications** for the purpose of **legal advice**
- Activities undertaken for a **legal purpose**
- Decided in the case of a dispute based on applicable law
- Narrower than work product; less leeway for non-lawyer activities

➢ Lawyers must be **actively involved** and **providing legal advice**.

Factual Clearinghouse: Benefits Beyond the Privilege

- Forces translation of “cybersecurity” into understandable assertions that senior management can engage with meaningfully
- Provides a clear path for risk, compliance, and legal to engage efficiently, which is during the fact-gathering process
- Prevents an organization from giving different answers to the same question, in regulatory exams, audits, assessments, due diligence, etc.
- Provides a vetted and guided process for operations to “update” the evidence/proof of compliance year over year



Thank you!

Questions?

