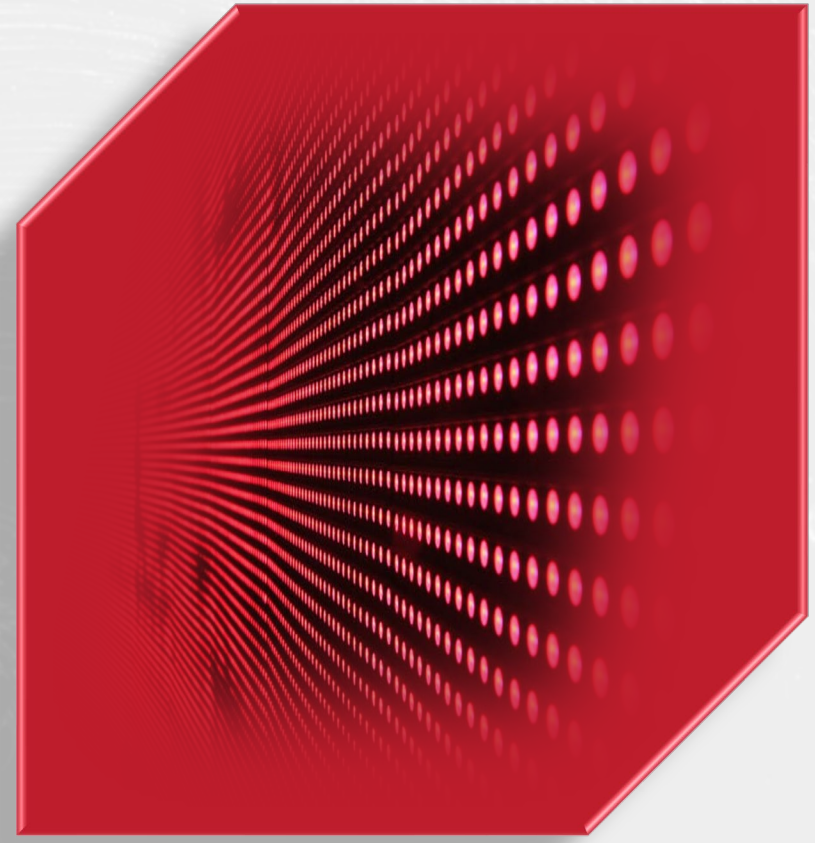
Zaviant

CIPL
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Ballard Spahr LLP



AI & Third-Party Risk Management

Everything You Need to Know About Leveraging AI to Manage Third-Party Risk

Agenda

- Introductions
- Regulatory Landscape
- Third-Party Risk Management
- Identify, Categorize, Assess, Report
- Leveraging AI

Zaviant

Introductions

Panelists

Will Sweeney
Managing Partner
Zaviant

Greg Szewczyk
Partner and Co-Chair of Privacy and Data Security Group
Ballard Spahr LLP

Matthew Reisman
Director of Privacy and Data Policy
Centre for Information Policy Leadership

Zaviant

Regulatory Landscape

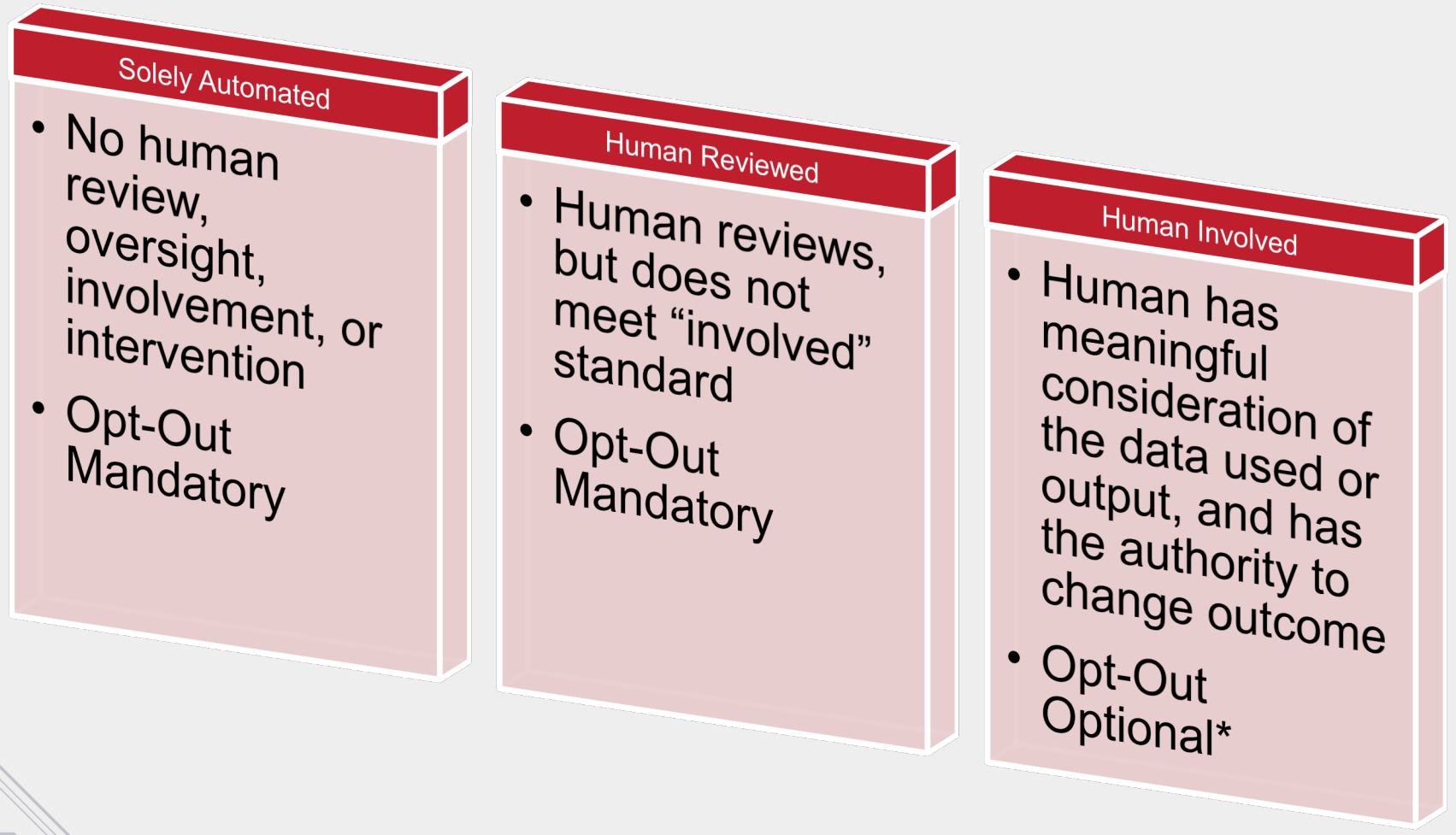
State Privacy Law Considerations

- Potential Impact on Applicability Thresholds
- Disclosure Obligations
- Opt Out Rights
- Risk Assessment Requirements

Colorado Regulations—Transparency

- What decisions are subject to profiling
- Categories of data processed
- Non-technical, plain language explanation of
  - The logic used
  - How it was used in the decision-making process
  - Human involvement
- Evaluation for accuracy, fairness, or bias
- Benefits and potential consequences
- How to exercise opt-out rights

Colorado Regulations—Opt Outs



California Draft Regulations

[MODIFICATIONS TO] § 7051. Contract Requirements for Service Providers and Contractors. [Green double-underline illustrates proposed additions to existing section 7051, subsection (a)(6).]

(a)(6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, to assist the business in completing the business's cybersecurity audit pursuant to Article 9, to assist the business in conducting the business's risk assessment pursuant to Article 10, to assist the business in providing meaningful information to the consumer about its Automated Decisionmaking Technology, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from

California Draft Regulations

§ 7154. Additional Requirements for Businesses that Process Personal Information to Train Artificial Intelligence or Automated Decisionmaking Technology.

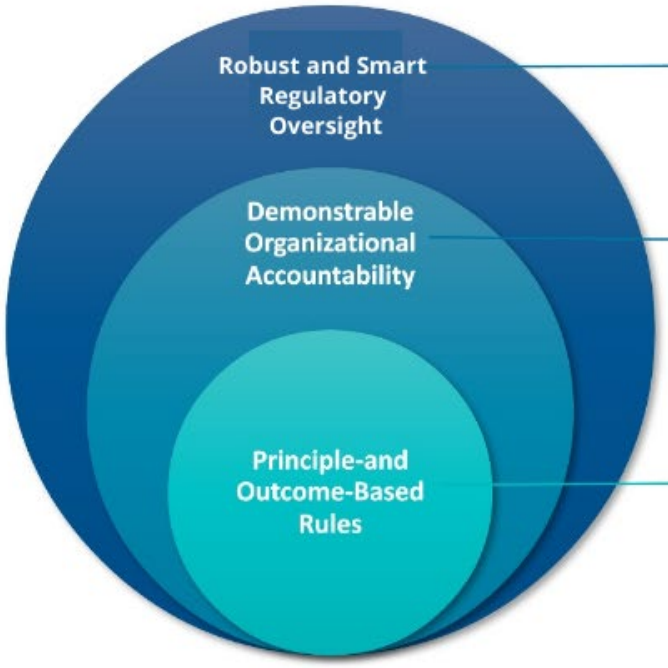
(a) If a business has processed or is processing personal information to train artificial intelligence or Automated Decisionmaking Technology, and has made or is making that artificial intelligence or Automated Decisionmaking Technology available to other persons for their own use, the business shall provide to those other persons a plain language explanation of the appropriate purposes for which the persons may use the artificial intelligence or Automated Decisionmaking Technology.

(1) The business shall document in its own risk assessment how it has provided or plans to provide the required information to those persons, and any safeguards the business has implemented or will implement to ensure that the artificial intelligence or Automated Decisionmaking Technology is used for appropriate purposes by other persons.

(b) If a business has processed or is processing personal information to train artificial intelligence or Automated Decisionmaking Technology, and has made or is making that artificial intelligence or Automated Decisionmaking Technology available to other businesses ("recipient-businesses") for any processing activity set forth in section 7150, subsection (b), the business shall provide all facts necessary for those recipient-businesses to conduct the recipient-businesses' risk assessments.

(1) The business shall document in its own risk assessment how it has provided or plans to provide the necessary facts to those recipient-businesses.

CIPL Global AI Regulation Recommendations



- Coordination and cooperation across regulatory bodies
- Cooperation-based regulatory oversight and ongoing regulatory innovation (e.g. regulatory sandboxes and policy prototyping)
- Global cooperation and interoperability

- Organizational accountability at the core of the framework.
- Incentivize the adoption of accountable AI practices
- Liability for party most closely associated with harm

- Technology-neutral framework
- Risk-based approach
- Build on existing legal foundations and evolve (with targeted regulatory and co-regulatory interventions and interpretations)
- Empower individuals through transparency, explainability, and redress mechanisms

CIPL Work on AI

Delivering Sustainable AI Accountability in Practice

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Report 1 Artificial Intelligence and Data Protection in Tension

- Details the widespread use, capabilities and potential of AI applications
- Examines tensions between AI technologies and some data privacy legal requirements

Report 2 Hard Issues and Practical Solutions

- Dives deeper into some of the hardest challenges of AI and data protection and puts forward concrete approaches to mitigating the tensions
- Outlines best practices and tools that organizations are currently developing to enable accountable and human-centric AI

How the GDPR Regulates AI

- Explores the applicability of the GDPR generally to AI
- Investigates the GDPR provisions that are of particular relevance in the context of AI and that specifically regulate the use of AI

Response to and engagement with global regulatory initiatives

- EU AI Act
- US Blueprint for an AI Bill of Rights
- UK National AI Strategy
- Brazil AI Bill
- Canada Artificial Intelligence and Data Act (AIDA)

Current workstream

- New paper on Ten Recommendations for Global AI Regulation
- Accountable AI Mapping Project

Zaviant

Third Party Risk Management

Third-Party Risk Management

Establish your third-party risk management program:

Identify

- *Identify* the full population of third parties you work with
- Work with internal teams to ensure full population
- Regulatory requirements

Categorize

- *Categorize* your third parties based on:
  - Risk – Low, Medium, High
  - Nature of services being provided
  - Location and types of data being processed

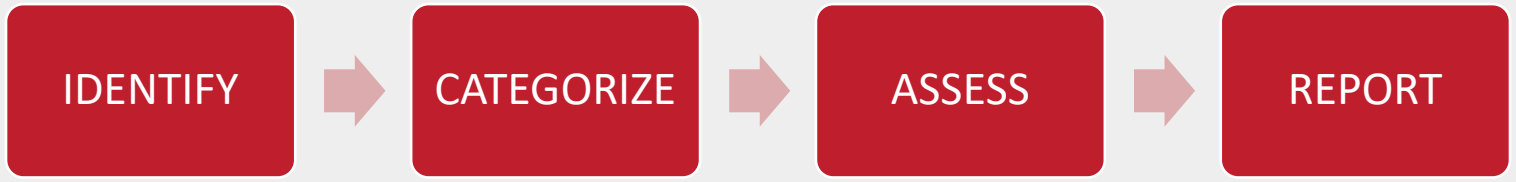
Assess

- Determine assessment criteria and *assess*:
  - Maturity of data security & privacy programs
  - Risks your third parties represent to your business
  - Identify and known vulnerabilities or gaps
  - Create risk waivers and gain internal acceptance of identified risks

Report

- Identify risk team and *report* to management and key stakeholders:
  - Monitor risks on an ongoing basis
  - Conduct regular assessments and identify assessment cadence
  - Monitor risk waivers for appropriateness
  - Follow up with third-parties on open risks / gaps
  - Leverage tooling to identify breaches, legal risks, and identified vulnerabilities

METHODOLOGY



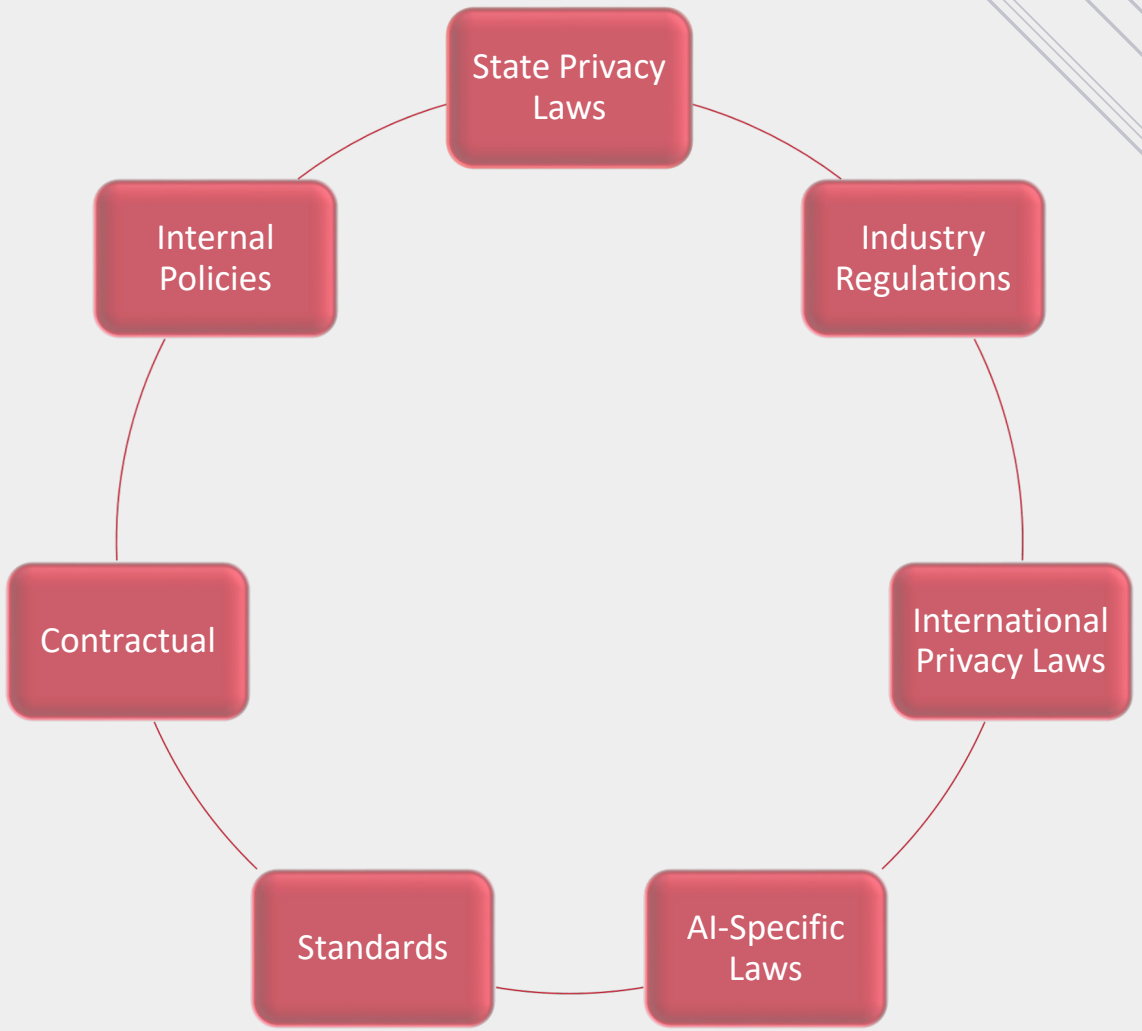
Zaviant

Identify

Identify

Identify

- *Identify* the full population of third parties you work with
- Work with internal teams to ensure full population
- Determine regulatory requirements



Practical Considerations in Negotiations

- Sufficient information on how data is being used
- Scope of exceptions to limited use
  - Undefined internal improvements
  - Expansions of aggregate, anonymized, and deidentified carve-outs
- Representations on compliance
- Disconnect between terminology and legal roles
  - Impact on disclosures and contractual obligations

AI and Data Protection Principles

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Data Protection Requirements	Tensions To Resolve	Artificial Intelligence
Legal basis for processing		Insufficient/limited variety of legal bases may undermine full range and stages of AI
Consent		Not practical to obtain consent for the processing of personal data (including sensitive data)
Data minimisation		Needs sufficient volumes and diversity of data for research, analysis, operation, training and to avoid bias
Purpose specification and limitation		Uses data for new and unforeseen purposes beyond original scope
Transparency		May produce unexplainable and unanticipated outcomes; hard to provide meaningful notice
Retention limitation		Needs to retain data for AI training, traceability, audit and oversight
Individual rights		Difficult to facilitate access, correction, deletion or explanation of the logic involved
Rules on automated decision-making		Automated decision-making capabilities are inherent to AI
Cross border data transfer restrictions		Needs to use diverse and geographically disperse data

CIPL's Report on AI and Data Protection - https://bit.ly/2QUP2xy

Zaviant

Categorize

AI Governance Mapped to CIPL Accountability Framework

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Principles endorsed from the top; Ethical councils / advisory bodies with diverse skills and experiences

Leadership and Oversight

Risk Assessment

Risk and impact assessments integrated across themes, where possible (privacy, AI, human rights)

Policies and Procedures

Documented policies and procedures for development / deployment /use

Transparency

Contextualized approach to transparency and explainability

Training and Awareness

Organization-wide and function-specific training

Monitoring and Verification

Audits, reviews, red-teaming

Response and Enforcement

Procedures for acting on findings of audits + reviews

Vendor Risk Management

Due to the inability to control the cybersecurity programs of third-parties, Supply Chain Risk Management or Vendor Risk Management should continuously monitor the risk to reduce vulnerabilities and ensure business continuity. The organization may not be able to control the supply chain vendor security, but it can decide whether to accept, reject, mitigate, or transfer those risks to protect the data.

Categorize based on data, services rendered, and sensitivity

01 Define All Data

- Develop a data classification policy and process
- What types of data is processed, accessed, and stored?
- Who are the data owners?
- What level of protections are required by each data type? (i.e., encryption levels, backup requirements, etc.)

02 Vendor List

- List all vendors with proper contact information, responsibility matrices. Create database if this is a large amount
- Review all contracts and validate appropriate third-party information security requirements are documented
- List of all systems, networks, and software that are accessed by vendors
- Where is it accessed? Through VPN, Web API, direct access, etc.?
- What information is transmitted or accessed?

03 Customers

- Define whose data is being hosted on your behalf (e.g., customers, BSI, etc.).

Zaviant

Assess

Colorado Regulations – Risk Assessment

- Specific Requirements
  - Purpose and specific data
  - Necessity, benefits, and risks
  - Names and categories of recipients, including third parties and processors
  - Expectations of consumers
  - Safeguards and alternatives
- Timing
  - Before
  - Annually*
  - Material change in level of risk
- Subject to regulator requests

AI Governance Mapped to CIPL Accountability Framework: Highlights

Principles endorsed from the top; Ethical councils / advisory bodies with diverse skills and experiences

Leadership and Oversight

Risk Assessment

Risk and impact assessments integrated across themes, where possible (privacy, AI, human rights)

Policies and Procedures

Documented policies and procedures for development / deployment /use

Transparency

Contextualized approach to transparency and explainability

Training and Awareness

Organization-wide and function-specific training

Monitoring and Verification

Audits, reviews, red-teaming

Response and Enforcement

Procedures for acting on findings of audits + reviews

AI Risk Assessments

- Algorithmic impact assessment or fairness assessment tools to monitor and continuously test algorithms to avoid human bias, unfair discrimination and concept drift throughout the entirety of AI lifecycles
- Ethics impact assessment / human rights impact assessment / Data protection impact assessment
- Developing standardized risk assessment methodologies, which consider the benefits and the likelihood and severity of risk factors on individuals and/or society, level of human oversight involved in individually automated decisions with legal effects as well as their explainability according to context and auditability
- Trade-offs documentation (e.g., accuracy—data minimization, security—transparency, impact on few—benefit to society) for high-risk processing as part of the risk assessment
- Data quality assessment via KPIs
- Data evaluation against the purpose—quality, provenance, personal or not, synthetic, in-house or external sources
- Framework for data preparation and model assessment – including feature engineering, cross-validation, back-testing, validated KPIs by business
- Working in close collaboration between business and data experts (data analysts, data engineers, IT and software engineers) to regularly assess the needs and accuracy results to ensure that the model can be properly used

Zaviant

Third Party Risk Management

Establish a Supply Chain Risk Management Framework

01. Risk tolerance needs to be defined for the organization for accepting, transferring, mitigating, or even refusing vendor risks

02. Assign Trust Level - purpose of this is that the same type of risk assessment cannot be conducted for all vendors. It is necessary to identify the vendors with the greatest risk and prioritize them

03. Determine which vendors and services are in scope from an active risk management perspective

04. What data is created, accessed, transmitted and/or stored

05. Due-diligence assessments are performed for vendors, depending on the level of internal versus vendor-owned controls

06. This will establish a Trust-Level Rating and determine requirements for assessments, reassessments, and monitoring

07. The purpose is to focus on the vendors that matter most, and limiting unnecessary work for lower-risk vendors

08. Trust levels should be reviewed yearly and when a major (defined) change happens, or new vendor is being considered

Third Party Risk Management

Determine Assessment Types - example below

Trust-Level Rating	Assessment Type	Frequency	Framework
Low	Vendor self-assessment	Once	Custom Questionnaire
Moderate	Remote review, infrastructure assessment	Yearly	Ex. ISO 27k, NIST 800-171, COBIT
High	Onsite review, infrastructure and application assessment	Yearly	Ex. ISO 27k, NIST 800-171, COBIT

Zaviant

Report

Third Party Risk Management.

Monitor and Report

1. Monitor and routinely assess vendors based on their Trust-Level Rating
2. Should include vendor security posture and risk levels with clearly defined risks relating to the data and organization
3. Reports to be furnished to inform internal stakeholders, internal auditors, board, etc.

AI & Third-Party Risk Management

Leveraging AI Tooling

AI tools can be used for a variety of purposes to help:

- Speed up onboarding time of new third parties
- Gain more information about identified risks
  - What is the risk, why is it important, who is responsible for mitigating the risk and how can it be mitigated
- Identify third parties that have experienced breaches, security threats, or fraud
- Update risk scoring for third parties

Benefits of using AI as part of third-party risk management:

- Increased insight into third-party risks
- Quicker risk review procedures with automated decision making
  - Annual recertifications, report analysis, risk questionnaires
- Map identified risks
  - Against industry standard information security frameworks
  - Against existing and emerging data privacy and compliance regulations
- Train your team more quickly and accelerate your third-party risk management program
- Identify gaps between previously defined contractual obligations and new contractual obligations

THANK YOU!

Will Sweeney
Managing Partner
Zaviant

Greg Szewczyk
Partner and Co-Chair of Privacy and Data Security Group
Ballard Spahr LLP

Matthew Reisman
Director of Privacy and Data Policy
Centre for Information Policy Leadership