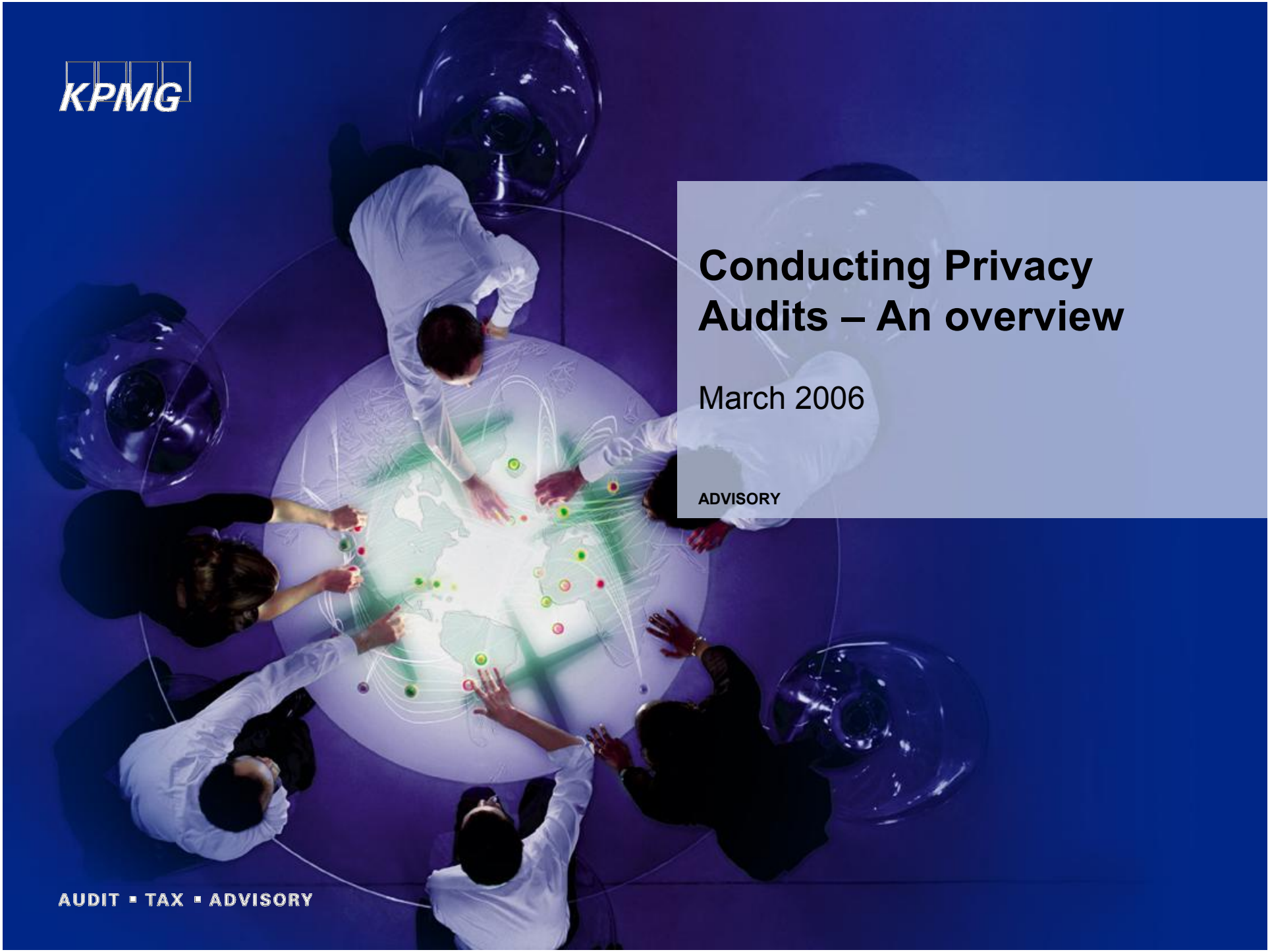


KPMG

Conducting Privacy Audits – An overview

March 2006

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

Why undergo a Privacy Audit?

- Provide independent assurance to third parties –
  - Clients & partners
  - Regulators
- Enhance consumers trust & brand
- Comply with contractual clauses
- Obtain external feedback (“Privacy Scorecard”)
- Replace multiple third party reviews

KPMG's Privacy Solution Delivery Methodology

Strategy & Risk ID	Design & Planning	Development	Implementation	Monitoring & Control
Environmental Analysis • Regulations • Legislation • Market Expectations • Litigation **Business Risk Analysis** • "As Is" Evaluation • Information flows documentation • Information risk evaluation **Privacy Business Strategy** • Compliance mgmt • Customer mgmt • Information mgmt • Risk mgmt **Gap Analysis**	**Policy Development** • Board and Management Endorsement • Corporate • Business Line **Business Processes** • Front office • Back office • 3rd Party Relationships • Marketing • Compliance • Audit **Controls** • Brand risk • Strategic Risk • Operational Risk • Process • Technology • Security • Compliance Risk • Regulatory Risk • Litigation Risk	**Business Process Redesign** **Human Resources** • Communication • Training **Information Systems Modifications** **Security Architecture** **Relationship Management** • Customer Communication • 3rd Parties **Functional Procedures** • Compliance • Legal • Audit	**Business Process Changes** **Information Systems Modifications** **Security Implementation** **Customer Contact Program** • Notification • Opt-In/Opt-Out **Compliance** • Awareness • Training • Reporting • Legal • 3rd Parties contracts	**Compliance Testing Programs** • Corporate • Business Line **Issue Identification & Resolution** **Third Party Assurance** • Privacy Audits • Privacy Seal • Security Audits • Web Seals **Environmental Updates** • Regulations • Legislation • Market Expectations • Litigation

What are Privacy Assurance Services?

- Assurance services are services in which a CPA is engaged to issue an opinion, a review, or an agreed upon procedures report on subject matter or an assertion about the subject matter that is the responsibility of another party.
- An independent, objective, knowledgeable practitioner performs tests of the subject matter to form an opinion or to report on assertions/subject matter.
- In the context of privacy, the privacy program is reviewed based on an objective criteria, such as the *AICPA Generally Accepted Privacy Principles* for
  - The effectiveness of its controls over the collection, use, retention, and disclosure of personal information
  - Compliance with its commitments in the organization's notice.

KPMG

Privacy Assurance Services

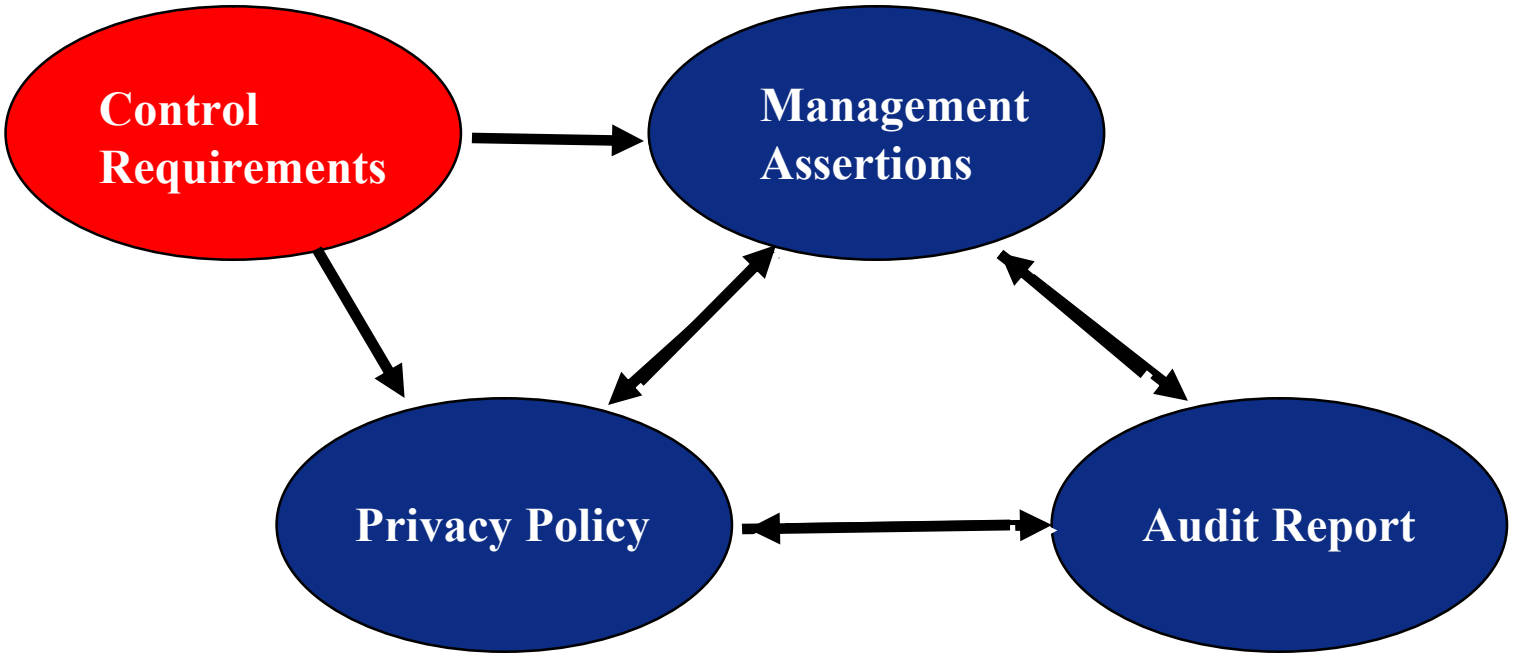
	Privacy Assurance	**Financial Statement Audit**
Professional Standards	*Statements on Standards for Attestation Engagements* issued by the AICPA	*Statement on Auditing Standards*, issued by the AICPA; for SEC registrants *Auditing and Related Professional Practice Standards*, issued by PCAOB
Measurement Criteria	Generally Accepted Privacy Principles **(GAPP)**	Generally Accepted Accounting Principles **(GAAP)**

Measurement Criteria

- Defined in established control requirements that can be tangibly measured and audited
- Provide concrete support for the fulfillment of privacy principles and company policies
- Based on substantive elements deemed to comply with applicable legislation or industry requirement
- AT100: Statement on Standards for Attestation Engagements (SSAE) No. 1, Attestation Standards
- AICPA/CICA Generally Accepted Privacy Principles (GAPP)

KPMG

Attestation Model & Presentation



Scope & Timing

- Scope can vary to meet needs - all or some personal information, all or some business operations
- Cover a specific data flow from cradle to grave. If information combined with other repositories, they are in scope from that point onward
- The engagement covers both effectiveness of controls and compliance with the commitments noted in the notice
- The report will usually cover a period of time (first time can be a point-in-time report).

KPMG

Phased Approach

- Phase 1- Diagnostic
- Phase 2 – Remediation
- Phase 3 – Privacy Examination
- Phase 4 – Privacy Examination Updates

Third parties

- Data transfer to third parties may impact the scope of the engagement
- Points to consider
  - Nature of service
  - Contractual obligations
  - Existing assurances

Getting ready for an Audit

- Review the listing of items required by the auditor for the review (e.g., descriptions of the client's products or services, copies of policies, procedures) – PBC list
- Provide documentation of information life cycle (flowcharts and narratives)
- Provide assistance in mapping the existing controls to the relevant privacy criteria
- Provide assistance in locating supporting documentation for items selected for testing

Questions????

Contact Information

Doron Rotman

drotman@kpmg.com

650 404-4176