

**PRIVACY**

# Generally Accepted Privacy Principles

– Overview and Uses

**IIA & ISACA Denver - March 10, 2009**

**Kerry L. Shackelford**

**AICPA Privacy Task Force**



## Outline

- What is Privacy?
- Introducing the GAPP
  - Privacy Principles
  - Structure
  - Basis
- Using the GAPP
  - Business
  - Government
  - Public Accounting
  - Academia
  - Internal Audit
- Resources
- Q&A



## What is Privacy? 1791

- “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

The Fourth Amendment – U. S. Constitution

# What is Privacy? 1890

“The right to be let alone”

Samuel D. Warren

HARVARD

LAW REVIEW.

---

---

VOL. IV.

DECEMBER 15, 1890.

NO. 5.

---

---

THE RIGHT TO PRIVACY.



## What is Privacy? 1990

- The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Alan Westin, *The Equifax Report on Consumers in the Information Age*, XVIII (1990).

## What is Privacy? 2009 – The Auditors & Consultants

- **PRIVACY** is defined as *the rights and obligations of individuals and organizations with respect to the*
  - Collection
  - Use
  - Disclosure
  - Retention, and
  - Destruction*...of personal information.*

## CVS Caremark 2/18/08 Press Release

- CVS Caremark Corporation announced today that it has entered into an agreement with the U.S. Federal Trade Commission (FTC) and the U.S. Department of Health and Human Services Office for Civil Rights (OCR) concerning disposal of patient information at its retail pharmacy stores.
- CVS Caremark ... agreed to settle the matter in order to avoid the time and expense of further legal proceedings.
- COST: \$2,250,000

## Data Losses

- 2009 – To date through 2/25/09

<b>Total Breaches:</b>	<b>83</b>
<b>Records Exposed:</b>	<b>1,104,546</b>

- 2008

<b>Total Breaches:</b>	<b>656</b>
<b>Records Exposed:</b>	<b>35,691,255</b>

Source: [www.idtheftcenter.org](http://www.idtheftcenter.org)

## PRIVACY RISK AND BUSINESS

- Privacy is a risk management issue
  - Threats
    - Litigation
    - Negative publicity
    - Financial losses
    - Operational disruptions
    - Customer distrust

## OVERALL PRIVACY OBJECTIVE

- Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA/CICA.

## It's Polling Time

- Have you heard of Generally Accepted Privacy Principles?
- Are you familiar with the contents of GAPP?
- Have you implemented GAPP in your organization?

## WHAT IS GAPP?

- Generally Accepted Privacy Principles
  - Developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) to help guide organizations in implementing, sustaining and auditing privacy programs.



## What is GAPP?

- A set of 10 privacy principles and 66 related criteria for the handling of personal information throughout an organization.
- Incorporates concepts from domestic and foreign laws, regulations, guidelines, and other bodies of knowledge on privacy.
- One of a series of Trust Services offered by CPAs which also include:
  - Security
  - Processing integrity
  - **Privacy**
  - Availability
  - Confidentiality

## Privacy Principles

1. **Management:** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice:** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

## Privacy Principles

3. **Choice and Consent:** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, retention, and disclosure of personal information.
4. **Collection:** The entity collects personal information only for the purposes identified in the notice.

## Privacy Principles

5. **Use and Retention:** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes **or as required by law or regulations.**
6. **Access:** The entity provides individuals with access to their personal information for review and update.

## Privacy Principles

7. **Disclosure:** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for Privacy:** The entity protects personal information against unauthorized access (both physical and logical).

## Privacy Principles

9. **Quality:** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and Enforcement:** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

## Structure of the GAPP

### Management

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
1.0	The <b>entity</b> defines, documents, communicates, and assigns accountability for its privacy policies and procedures.		
1.1	<b>Policies and Communications</b>		
1.1.0	<b>Privacy Policies</b> The entity defines and documents its privacy policies with respect to: <ul style="list-style-type: none"> <li>• Notice (<a href="#">See 2.1.0</a>)</li> <li>• Choice and <a href="#">Consent</a> (<a href="#">See 3.1.0</a>)</li> <li>• Collection (<a href="#">See 4.1.0</a>)</li> <li>• Use and Retention (<a href="#">See 5.1.0</a>)</li> <li>• Access (<a href="#">See 6.1.0</a>)</li> <li>• Onward Transfer and Disclosure (<a href="#">See 7.1.0</a>)</li> <li>• Security (<a href="#">See 8.1.0</a>)</li> <li>• Quality (<a href="#">See 9.1.0</a>)</li> <li>• Monitoring and Enforcement (<a href="#">See 10.1.0</a>)</li> </ul>	Privacy policies are documented (in writing) and made readily available to <a href="#">internal personnel</a> and <a href="#">third parties</a> who need them.	
1.1.1	<b>Communication to Internal Personnel</b> Privacy policies and the consequences of noncompliance with such policies are communicated at least annually to the entity's internal personnel responsible	The entity: <ul style="list-style-type: none"> <li>• Periodically communicates to internal personnel (for example, on a network or a Web site) relevant information about the entity's privacy policies and</li> </ul>	Privacy policies encompass security policies relevant to the protection of personal information.

## Comparison with International Concepts

AICPA/CICA GAPP	US FTC FIPs	Canada PIPEDA	Australia	US Safe Harbor	EU Data Protection Directive	OECD
<b>Management</b>		Accountability			Notification	Accountability
<b>Notice</b>	Notice	Identifying Purposes, Openness	Openness	Notice	Information to be Given to the Data Subject	Purpose Specification, Openness
<b>Choice &amp; Consent</b>	Choice	Consent	Use and Disclosure	Choice	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Collection Limitation
<b>Collection</b>		Limiting Collection	Collection, Sensitive Information, Anonymity	Data Integrity	Principles Relating to Data Quality, Exemptions and Restrictions	Collection Limitation (including consent)
<b>Use and Retention</b>		Limiting Use, Disclosure, and Retention	Identifiers, Use and Disclosure	(implied but not specified)	Making Data Processing Legitimate, Special Categories of Processing, Principles Relating to Data Quality, Exemptions and Restrictions, The Data Subject's Right to Object	Use Limitation (including disclosure limitation)
<b>Access</b>		Individual Access	Access and Correction	Access	The Data Subject's Right of Access to Data	Individual Participation
<b>Disclosure</b>		Limiting Use, Disclosure, and Retention	Use and Disclosure, Trans-border Data Flows	Onward Transfer	Transfer of Personal Data to Third Countries	Use Limitation
<b>Security for Privacy</b>	Security	Safeguards	Data Security	Security	Confidentiality and Security of Processing	Security Safeguards
<b>Integrity</b>	Integrity	Accuracy	Data Quality	Data Integrity	Principles Relating to Data Quality	Data Quality
<b>Monitoring &amp; Enforcement</b>	Enforcement	Challenging Compliance	(Enforcement by the Office of the Privacy Commissioner)	Enforcement	Judicial Remedies, Liability and Sanctions, Codes of Conduct, Supervisory Authority and Working Party on the Protection of Individuals with Regard to the Processing of Personal Data	Individual Participation

## The USA, EU and Argentina on Privacy –

- “In the United States, everything is allowed, unless prohibited.”
- “In the European Union, everything is prohibited, unless allowed.”
- “In Argentina, everything is allowed, especially those things which are prohibited.”

Carlos Tomassino, Director, School of IT at the National Tech University, Buenos Aires and President of the Argentine Chamber of Electronic Commerce.

## Using the GAPP

- Business
  - Privacy policies and procedures
  - Self-assess against a standard
- Academia
  - Training material
- Audit Firms
  - Consulting
  - Privacy attest
- Internal Auditors
  - Governance, Risk, & Compliance



# Sun Microsystems

## 2007 Corporate Social Responsibility Report

- Our global customer privacy policy governs the capture, storage, and use of personally identifiable information (PII) from Sun technology users and visitors to sun.com. It sets out our fair processing principles and meets international privacy and data protection standards, including European Union (EU) data directives, Generally Accepted Privacy Principles (GAPP), and Organization for Economic Cooperation and Development (OECD) fair information processing principles.



# Microsoft Vendor Privacy Toolkit

- “The Microsoft Vendor Data Protection Requirements (DPR) are applicable to all Microsoft vendors that collect, use, distribute, access, or store Microsoft Personal Information.”
- “The DPR is based on a framework designed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) to measure privacy practices. The Generally Accepted Privacy Principles (GAPP) ...”



## ***Section 7216 Regulations Preparer Disclosure/Use Rules***

- General rule requires that a taxpayer’s SSN not be shared outside the United States even with client consent.
- A proposed exception allows sharing via an “adequate data protection safeguard.”
- An “adequate data protection safeguard” is a data security program, policy and practice that meets or conforms to one of the following privacy or data security frameworks:
- ... “(4) The requirements of the AICPA/CICA Privacy Framework;”

## Fly Clear



In January 2009, Grant Thornton LLP completed Clear's most recent independent privacy audit of Clear's *national* registered traveler program. During its extensive review, Grant Thornton LLP examined the following components of our program:

- Clear's privacy policy, controls and procedures
- Clear's compliance with its stated privacy policy
- Clear employees' privacy policy training and compliance
- Clear's system design
- Clear's data retention, integrity and security policies and procedures

In its findings, Grant Thornton LLP certified that we comply with the promises made in our [privacy policy](#) and that Clear succeeds in protecting members' personal information.

Clear's next annual independent audit will be completed in February 2010.



## Key Concepts Applicable to Privacy Assurance Engagements

- The report ordinarily covers all 10 principles and their criteria
- Should be performed at the highest level of assurance – “examination”
- Scope can vary to meet needs - all or some personal information, all or some business operations
- 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).

# Amazon.com's Purchase Circles

## March 24, 2001

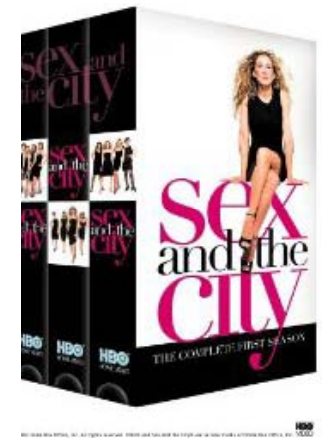
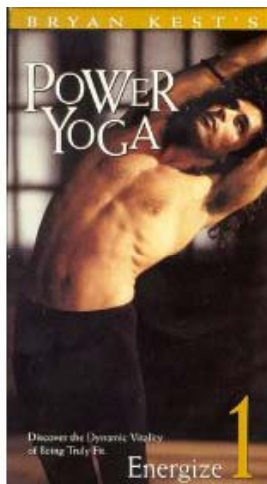
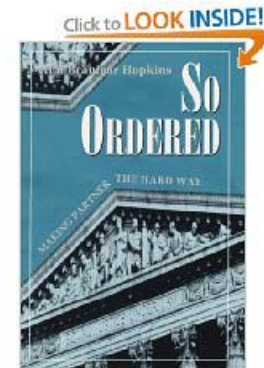
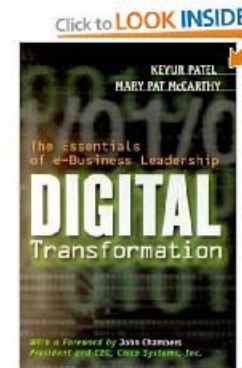
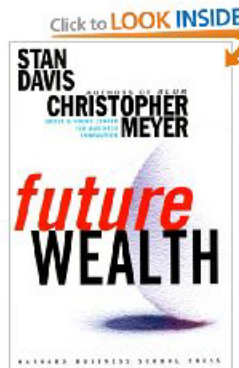
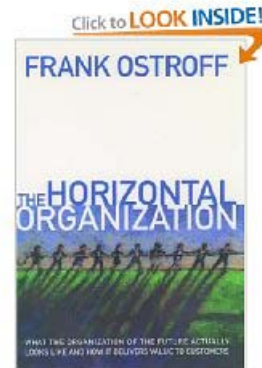
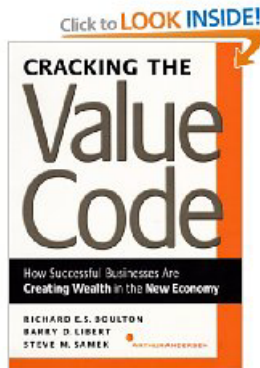
Andersen

DTT

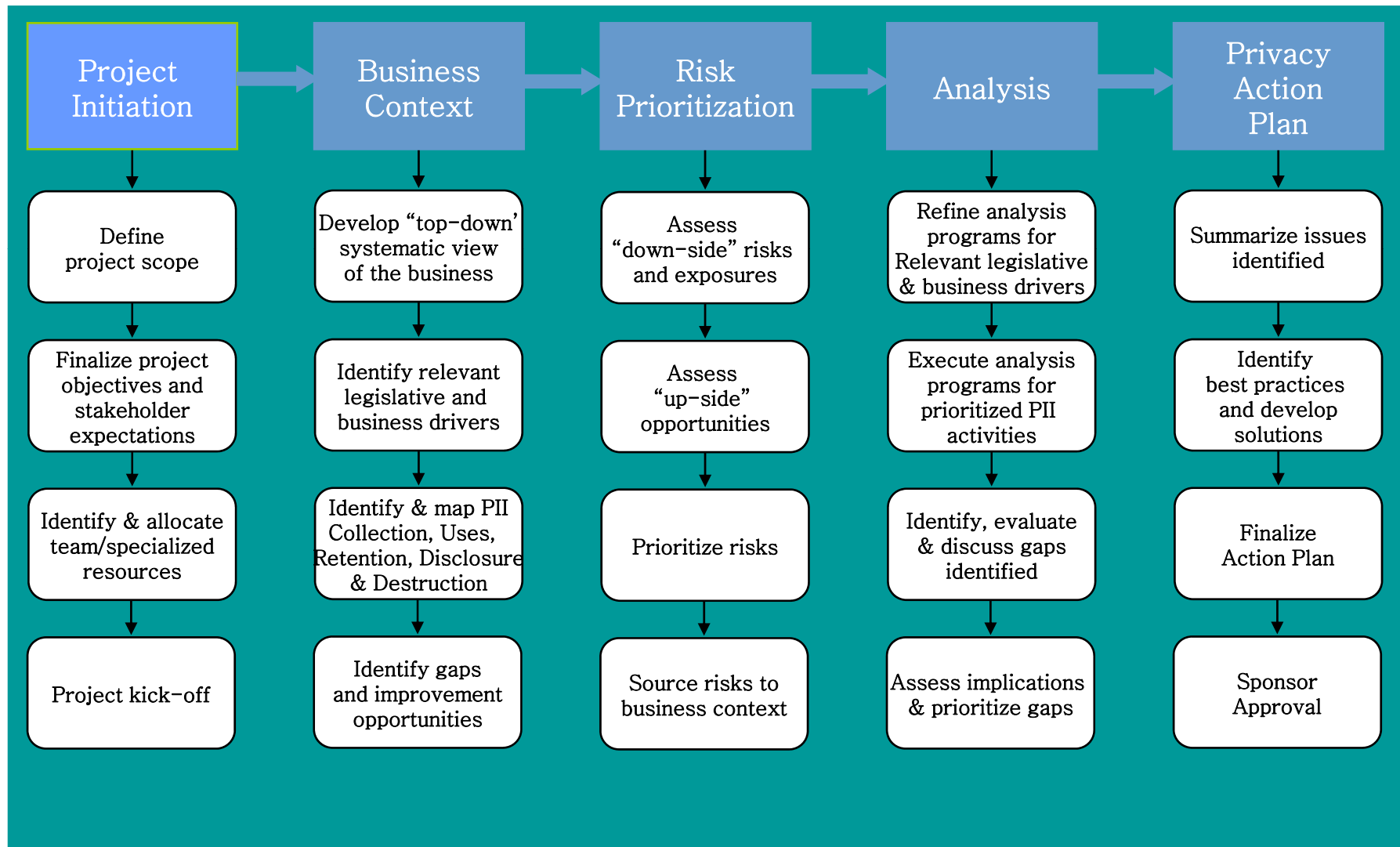
EY

KPMG

PwC



# The Privacy Audit / Risk Assessment - Summarized



# Privacy Review and Security Test

Privacy Review and Security Test

[Client]



[StartMonthYear] to [EndMonthYear]



# Privacy Review and Security Test Project Definition and Objectives

## Project Definition and Objectives

The project was defined in two parts: 1) Privacy Review, and 2) Security Test.

- 1) Privacy Review – Reviewed the business processes involved in the collection, use, and disclosure of personal information and determined their general conformance to the privacy requirements.
- 2) Security Test – Evaluated technical safeguards protecting personal information collected through or accessible through Web sites. Identified vulnerabilities whereby unauthorized individuals could gain access to personal information through the Internet.

This project assisted [Client] in performing a risk assessment by evaluating the privacy and security posture of its business processes for handling personal information.

# Privacy Review and Security Test Project Scope and Limitations

The scope of the project was limited in several regards:

- 1) KLSC did not review and evaluate security policies, security administration procedures, security monitoring, and the technical configuration of components of the IT architecture (aside from what [Client] personnel advised us existed and what is visible from the Internet).
- 2) KLSC did not visit any of the [NN] locations or interview any location personnel. Each location has marketing and sales associates on staff. The locations collect, use and disclose personal information of individuals.
- 3) KLSC did not review and evaluate compliance with privacy requirements from the standpoints of handling the personal information of employees or job applicants (human resources).

As per the services agreement:

- 1) [Client] acknowledges that KLSC is not a law firm and does not provide legal advice.
- 2) [Client] is responsible for determining whether KLSC's observations in the Deliverables are or are not violations of privacy laws and regulations.
- 3) [Client] is responsible for compliance with privacy regulations. KLSC's work is intended solely for the use of [Client] in its efforts to comply in good faith with its privacy policies.

# Privacy Review and Security Test Example – Detailed Observation

[Client]  
Appendix I -- Detailed Observations and Recommendations

Privacy Review and Security Test  
[StartMonthYear] to [EndMonthYear]

Summary & Source	Observation	Business Risk and Impact	Recommendation
<p><b>3. Notice is not provided in telemarketing solicitations prior to the collection of personal information</b></p> <ul style="list-style-type: none"> <li>▪ Review of US/EU Safe Harbor, FAQ 12</li> <li>▪ Review of US/EU Safe Harbor, Workbook, Notice Principle</li> <li>▪ Interview with [Name]</li> </ul>	<p>Associates in telephone sales use scripts to communicate with leads and prospects by telephone.</p> <p>Per [Name], the most frequent question asked by leads and prospects on an outbound telemarketing call is "How did you get my name?"</p> <p>Telemarketing scripts make no mention of privacy or [Client]'s privacy policy.</p> <p>There are no FAQs for telemarketing where the FAQ answers are pre-scripted.</p> <p>The wording of US/EU Safe Harbor, FAQ 12, suggests that [Client] should promptly give individuals an opportunity to decline further direct marketing communication.</p> <p>The US/EU Safe Harbor, Workbook, Notice Principle, states that "... notice must be provided ... when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable."</p>	<p>[Client] may fail to provide notice and offer choice prior to the collection of personal information.</p>	<p>At the point in a telephone sales call at which the user expresses interest and is prepared to provide personal information, notice should be provided.</p> <p>Modify telemarketing scripts to notify the individual that a privacy policy exists and direct the individual as to how they may obtain a written copy of the appropriate privacy notice should they desire one.</p> <p>Provide outbound telemarketing associates with pre-scripted answers to frequently asked questions. Include scripts for questions about privacy as well as DNx requests.</p> <p>At the appropriate point in the script, communicate the individual's right to decline further direct marketing.</p>

# Privacy Review and Security Test Low Hanging Fruit Analysis

Evaluation Criteria	Total Issues	#1 Issues Urgent	#2 Issues Important	#3 Issues-Needs to be Done (#3)
<b>Importance</b>				
▪ Count	87	46	40	1
▪ Percentage	100%	53%	46%	1%
<b>Work Effort</b>				
▪ Easy	58	29	28	1
▪ Medium	16	10	6	0
▪ Hard	13	7	6	0
<b>Cost Impact</b>				
▪ Low	66	33	32	1
▪ Medium	12	6	6	0
▪ High	9	7	2	0
<b>Elapsed Time</b>				
▪ Short	55	29	25	1
▪ Medium	22	10	12	0
▪ Long	10	7	3	0

# Privacy Review and Security Test Prioritized Plan of Action

The recommendations from the detailed observations and recommendations have been organized into a high level, prioritized plan of action. The major captions in the action plan are listed below.

- Execute, Locate or Amend Legal Contracts with Nonaffiliated Third Parties
- Remedy Known Internet Security Weaknesses
- Reduce the Risk of Identity Theft
- Review and Improve Internal Controls in Application Systems
- Review and Improve Internal Network and Server Security
- Amend Privacy Statement/Notice Disclosures as Required or Recommended
- Execute a Contract with [Country] re: Cross-Border Transfers
- Enhance the Privacy Program and Ensure Compliance with Information Policies
- Address Other Miscellaneous Recommendations

## Privacy Review and Security Test Work Performed (1 of 4)

- Planning
  - Selected privacy scan tools – Watchfire, Inc. Privacy XM and Site Integrity XM
  - Selected security scan tools – Sanctum's AppScan and open source Nessus
  - Identified web sites for privacy scan
  - Reviewed internal and external policies
  - Obtained and reviewed process/system flows
  - Interviewed process champions for marketing, sales, loan servicing, and owner services
  - Developed preliminary work plan

## Privacy Review and Security Test Work Performed (2 of 4)

- Privacy Review
  - Developed a privacy requirements matrix
    - Corporate policies
    - US/European Union Safe Harbor program
    - Title V of the US Gramm-Leach-Bliley Act (GLBA)
  - Assessed compliance with privacy requirements
    - Conducted 60+ interviews across 3 locations
    - Compared privacy statements across all websites
    - Assessed GLBA notice against FDIC Part 332 requirements as well as competitor notices
    - Assessed disclosures to non-affiliated third parties
    - Analyzed privacy-related complaints
    - Sampled employees who handle PII

## Privacy Review and Security Test Work Performed (3 of 4)

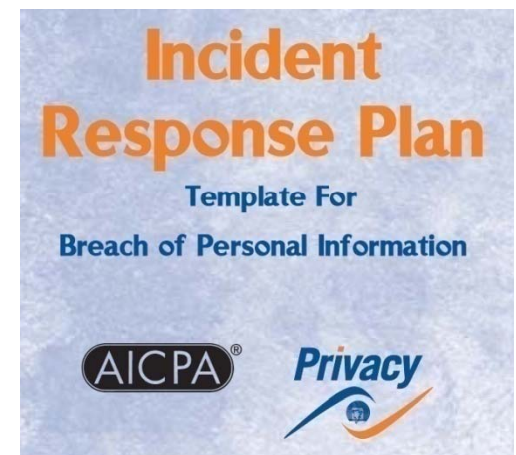
- Privacy Review (continued)
  - Privacy Scan
    - 13 websites
    - Configured the privacy scan parameters
    - Conducted scan one and evaluated results
    - <Client addressed issues>
    - Conducted scan two and evaluated results
  - Considered emerging best practices
    - Evaluated the handling of tax IDs (SSNs)

## Privacy Review and Security Test Work Performed (4 of 4)

- Security Test
  - Scanned 15 websites (live)
  - Nessus Security Scanner (live) - Identifies technical site security vulnerabilities
  - Sanctum's AppScan - Identifies technical application security vulnerabilities
  - Supplemented scan results with manual review of selected hosts, web servers, and applications

## RESOURCES

- The AICPA and the CICA have many resources that will help establish and maintain an effective privacy program.
- AICPA Privacy Resources
  - <http://www.aicpa.org/privacy>
- CICA Privacy Resources
  - <http://www.cica.ca/privacy>
- IIA Privacy Resources
  - <http://www.theia.org/guidance/technology/gtag/gtag5/>



## Services

- Privacy & Security Programs
- IT Auditing
- Compliance
- IT Governance Risk, and Control

Kerry L. Shackelford, CPA, CISA

KLS Consulting, LLC

720-839-6359

[Kerry@KLSConsultingLLC.com](mailto:Kerry@KLSConsultingLLC.com)

