



*Information Systems
Audit and Control
Association®*

< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

AICPA/CICA Enterprise- Wide Privacy Framework

Presented By:

Doron Rotman

**National Privacy Service Leader,
KPMG**

The San Francisco Chapter of ISACA Proudly Announces the 4th Annual:

2004 SF ISACA FALL CONFERENCE

October 4-6, 2004

Agenda

- Introduction to the enterprise-wide Privacy Framework**
- Components of the Privacy Framework**
- The Privacy Framework in the Worlds of Regulation, Self-Regulation, and Best Practice**



Information Systems
Audit and Control
Association®

< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

Introduction to the Enterprise-Wide Privacy Framework

The San Francisco Chapter of ISACA Proudly Announces the 4th Annual:

2004 SF ISACA FALL CONFERENCE

October 4-6, 2004

The Accounting Profession and Privacy

- Privacy is a risk management issue. CPAs help manage organizational risk.
- CPAs measure performance outcomes against stated performance criteria and principles.
- If outcome measurement is to have meaning and engender trust, measurement benchmarks and recognized practices are required.
- U.S. CPAs and Canadian Chartered Accountants have worked together on similar projects in the past.

What is the Privacy Framework?

- ◆ The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have developed a privacy initiative to help guide organizations served by CPAs and Chartered Accountants (CA) in implementing privacy programs.
- ◆ The enterprise-wide privacy framework is one of the tools that has been established.
 - Core set of criteria for privacy and the handling of personal information throughout an organization
 - Incorporates concepts from domestic and foreign laws, regulations, guidelines, and other bodies of knowledge on privacy
 - Part of the overall Trust Services initiative
 - Security
 - **Privacy**
 - Process integrity
 - Availability
 - Confidentiality

What is Privacy?

Privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.

What Does the Framework Address?

- ◆ **The AICPA/CICA privacy framework contains 10 privacy components and related criteria that are essential to the proper protection and management of personal information. These privacy components and criteria are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and in common and leading practices.**
- ◆ **Components of the Privacy Framework**
 - **Management**
 - **Notice**
 - **Choice and Consent**
 - **Collection**
 - **Use and Retention**
 - **Access**
 - **Disclosure**
 - **Security**
 - **Quality**
 - **Monitoring and Enforcement**

What are Criteria?

The criteria identified in the 10 privacy components provide a basis for designing, implementing, maintaining, and evaluating a privacy program in order to meet an entity's needs.

◆ Criteria Characteristics

- Relevant
- Complete
- Objective
- Measurable

◆ Categories

- Policies and communications
- Controls and procedures



< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

Components of the Privacy Framework

The San Francisco Chapter of ISACA Proudly Announces the 4th Annual:

2004 SF ISACA FALL CONFERENCE

October 4-6, 2004

What are the Components?

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.
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.
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.

What are the Components?

6. **Access:** The entity provides individuals with access to their personal information for review and update.
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:** The entity protects personal information against unauthorized access (both physical and logical).
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.

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
1.0	The <u>entity</u> defines, documents, communicates, and assigns accountability for its privacy policies and procedures.		
1.1	Policies and Communications		
1.1.0	Privacy Policies The entity defines and documents its privacy policies with respect to: <ul style="list-style-type: none"> • Notice (See 2.1.0) • Choice and Consent (See 3.1.0) • Collection (See 4.1.0) • Use and Retention (See 5.1.0) • Access (See 6.1.0) • Onward Transfer and Disclosure (See 7.1.0) • Security (See 8.1.0) • Quality (See 9.1.0) • Monitoring and Enforcement (See 10.1.0) 	Privacy policies are documented (in writing) and made readily available to internal personnel and third parties who need them.	<div style="border: 2px solid black; padding: 5px; text-align: center;"> <h2><u>Section Definition</u></h2> </div>
1.1.1	Communication to Internal Personnel 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"> • Periodically communicates to internal personnel (for example, on a report or a Web site) relevant information about the entity's privacy policies and 	



Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
	<p>for collecting, using, retaining, and disclosing <u>personal information</u>. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.</p>	<p>changes to its privacy policies.</p> <ul style="list-style-type: none"> • Requires internal personnel to confirm (initially and periodically) their understanding of an agreement to comply with the entity's privacy policies. • Educates and trains internal personnel (initially and periodically) who have access to personal information or are charged with the security of personal information about privacy awareness concepts, and issues. 	
1.1.2	<p>Responsibility and Accountability for Policies Responsibility and accountability are assigned to a person or group for documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.</p>	<p>The entity assigns responsibility for privacy policies to a designated person or group, such as a corporate privacy officer or a committee. (Those assigned responsibility for privacy policies may be different from those assigned for other policies, such as security.)</p> <p>The authority and accountability of the designated person or group are clearly documented. Responsibilities include:</p> <ul style="list-style-type: none"> • Establishing standards to classify the sensitivity of personal information and to determine the level of protection required • Formulating and maintaining the entity's privacy policies • Monitoring and updating the entity's privacy policies • Delegating authority for enforcing the entity's privacy policies 	<div data-bbox="1201 454 1848 722" style="border: 2px solid black; background-color: yellow; padding: 10px; text-align: center;"> <h2 style="margin: 0;">Responsibility and Accountability for Policies</h2> </div>



Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<ul style="list-style-type: none"> Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices <p>The Board periodically includes privacy in its regular review of corporate governance.</p> <p>The entity requires users, management, and third parties to confirm (initially and annually) their understanding of and agreement to comply with the entity's privacy policies and procedures related to the security of personal information.</p>	
1.2	Procedures and Controls		
1.2.1	Review and Approval Privacy policies and procedures and changes thereto are reviewed and approved by management.	Privacy policies and procedures are: <ul style="list-style-type: none"> Reviewed and approved by senior management or a management committee. Reviewed at least annually and updated as needed. 	<div data-bbox="1252 454 1829 722" style="border: 2px solid black; background-color: yellow; padding: 10px; text-align: center;"> <p><u>Procedures and Controls: Review and Approval</u></p> </div>
1.2.2	Consistency of Privacy Policies and Procedures With Laws and Regulations Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	Corporate counsel or the legal department: <ul style="list-style-type: none"> Determines which privacy regulations are applicable in jurisdictions in which the entity operates. Reviews the entity's privacy policies and procedures to ensure they are consistent with the applicable laws and regulations. 	<div data-bbox="1153 869 1848 1215" style="border: 2px solid black; background-color: yellow; padding: 10px; text-align: center;"> <p>Consistency of Privacy Policies and Procedures With Laws and Regulations</p> </div>



Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
1.2.3	<p>Consistency of Commitments With Privacy Policies and Procedures Entity personnel or advisors review contracts for consistency with privacy policies and procedures and address any inconsistencies.</p>	<p>Management and the corporate counsel or the legal department review all contracts and service-level agreements for consistency with the entity's privacy policies and procedures.</p>	
1.2.4	<p>Infrastructure and Systems Management Entity personnel or advisors review the design, acquisition, implementation, configuration, and management of the infrastructure, systems, and procedures and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies.</p>	<p>Procedures are in place to:</p> <ul style="list-style-type: none"> • Govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, and disclose personal information. • Ensure that the entity's backup and disaster-recovery planning processes are consistent with its privacy policies and procedures. • Classify the sensitivity of classified data, and determine the classes of users who should have access to each class of data. Users are assigned user-access profiles based on their need for access and their functional responsibilities as they relate to personal information. • Assess planned changes to systems and procedures for their potential effect on privacy. • Test changes to system components to minimize the risk of an adverse effect 	

Consistency of Commitments With Privacy Policies and Procedures

Infrastructure and Systems Management



Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<p>information. All test data are <u>anonymized</u>.</p> <ul style="list-style-type: none"> Require the documentation and approval by the privacy officer and business unit manager before implementing the changes to systems and procedures that handle personal information, including those that may affect security. Emergency changes may be documented and approved on an after-the-fact basis. <p>The Information Technology (IT) department maintains a listing of all software and the respective level, version, and patches that have been applied.</p> <p>Procedures exist to provide that only authorized, tested, and documented changes are made to the system.</p>	<div data-bbox="1296 708 1816 901" style="border: 2px solid black; background-color: yellow; padding: 10px; text-align: center;"> <p>Supporting Resources</p> </div>
1.2.5	<p>Supporting Resources Resources are provided by the entity to implement and support its privacy policies.</p>	<p>Management reviews annually the assignment of personnel, budgets, and allocation of other resources to its <u>privacy program</u>.</p>	<div data-bbox="1296 708 1816 901" style="border: 2px solid black; background-color: yellow; padding: 10px; text-align: center;"> <p>Supporting Resources</p> </div>
1.2.6	<p>Qualifications of Personnel The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.</p>	<p>The qualifications of internal personnel responsible for protecting the privacy and security of personal information are ensured by procedures such as:</p> <ul style="list-style-type: none"> Formal job descriptions (including responsibilities, educational and professional requirements and organizational reporting for key privacy management positions) 	<div data-bbox="1296 1065 1829 1258" style="border: 2px solid black; background-color: yellow; padding: 10px; text-align: center;"> <p>Qualifications of Personnel</p> </div>

Reference	Criteria	Illustrations and Explanations of Criteria	Additional Considerations
		<ul style="list-style-type: none"> Hiring procedures (including the comprehensive screening of credentials, background checks, and reference checking) Training programs related to privacy and security matters Performance appraisals (performed by supervisors, including assessments of professional development activities) 	
1.2.7	<p>Changes in Business and Regulatory Environments For each jurisdiction in which the entity operates, the effect on privacy of changes in the following factors is identified and addressed:</p> <ul style="list-style-type: none"> Business operations and processes People Technology Legal Contracts, including service-level agreements <p>Privacy policies and procedures are updated for such changes.</p>	<p>The entity has an ongoing process in place to monitor, assess, and address the effect on privacy of changes in:</p> <ul style="list-style-type: none"> Business operations and processes People assigned responsibility for privacy and security matters Technology (prior to implementation) Legal and regulatory environments Contracts, including service-level agreements with third parties (Changes that alter the privacy and security related clauses in contracts are reviewed and approved by the privacy officer or corporate counsel before they are executed.) 	<div data-bbox="1359 629 1881 972" style="border: 2px solid black; background-color: yellow; padding: 10px; text-align: center;"> <h2 style="margin: 0;">Changes in Business and Regulatory Environments</h2> </div>





< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

The Privacy Framework in the Worlds of Regulation, Self-Regulation, and Best Practice

The San Francisco Chapter of ISACA Proudly Announces the 4th Annual:

2004 SF ISACA FALL CONFERENCE

October 4-6, 2004

Comparison with International Concepts

Privacy Framework	US FTC FIPs	Canada PIPEDA	Australia	US Safe Harbor	EU Data Protection Directive	OECD
Management		Accountability			Notification	Accountability
Notice	Notice	Identifying Purposes, Openness	Openness	Notice	Information to be Given to the Data Subject	Purpose Specification, Openness
Choice & Consent	Choice	Consent	Use and Disclosure	Choice	Criteria for Making Data Processing Legitimate, Data Subject's Right to Object	Collection Limitation
Collection		Limiting Collection	Collection, Sensitive Information, Anonymity	Data Integrity	Principles Relating to Data Quality, Exemptions and Restrictions	Collection Limitation (including consent)
Use and Retention		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)
Access		Individual Access	Access and Correction	Access	The Data Subject's Right of Access to Data	Individual Participation
Disclosure		Limiting Use, Disclosure, and Retention	Use and Disclosure, Trans-border Data Flows	Onward Transfer	Transfer of Personal Data to Third Countries	Use Limitation
Security	Security	Safeguards	Data Security	Security	Confidentiality and Security of Processing	Security Safeguards
Integrity	Integrity	Accuracy	Data Quality	Data Integrity	Principles Relating to Data Quality	Data Quality
Monitoring & Enforcement	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

Privacy Regulation, Self Regulation, and Best Practices

- As indicated in the previous slide, the privacy framework components match those of various privacy regulations.
 - A recent study done by the Ontario privacy commissioners found the framework to aligned with PIPEDA, Canada's Personal Information Protection and Electronic Documents Act
- Where privacy is implemented in a self-regulatory manner, the Framework can serve as a practical resource for the effective incorporation of privacy within the organization.
- The illustrations and additional considerations that are provided with each of the Framework criteria allows for flexible adoption of the criteria and the best practices that are associated with them.

Illustrations

- Company A adopts the Framework as the basis of its privacy program for its U.S.-based online operations. The Framework's components and criteria are described in Company A's online privacy policy. The Framework's criteria and illustrations served as the basis for the SOP Company A adopted.
- Company B adopts the Framework as the basis for its global privacy program so it can follow consistent privacy practices and use similar terminology across its various countries of operations. Although country specific exceptions and variations still exist, they are being captured in policy and procedures. The majority of the organization's transactions are successfully governed by the Framework's privacy criteria.



Information Systems
Audit and Control
Association®

< FOCUS > < DISCOVER > < INTEGRATE > < ADVANCE >

Resources

The San Francisco Chapter of ISACA Proudly Announces the 4th Annual:

2004 SF ISACA FALL CONFERENCE

October 4-6, 2004

Resources

The AICPA and the CICA have many resources that will help you establish and maintain an effective privacy program.

- ◆ AICPA Privacy Framework
 - <http://www.aicpa.org/privacy>
- ◆ CICA Privacy Resources
 - <http://www.cica.ca/privacy>
- ◆ CPA2BIZ Privacy Resources
 - <https://www.cpa2biz.com/ResourceCenters/Information+Security/Privacy/default.htm>