



AICPA/CICA

Privacy Risk Assessment Tool

User Guide



Table of Contents

I.	Introduction	2
II.	Installation	3
III.	General Information	3 – 4
IV.	Getting Started	4 – 5
V.	PRA Tool - Scoring Input Template	6 – 8
VI.	PRA Tool – Scoring Summary	9 – 11
VII.	Privacy Risk Assessment Team Action Items	11 – 12
VIII.	Privacy Resources	12
IX.	AICPA/CICA Privacy Task Force Members	13

I. Introduction

Privacy has become a significant business risk to organizations that collect, use, retain and disclose personally identifiable information about customers and employees. Whether complying with numerous privacy laws in jurisdictions where the organization does business — or meeting customers' and employees' expectations for handling their personal information — executive management, boards of directors, owners and privacy professionals are looking for guidance and tools on how to address this business concern.

A good first step within an organization is to perform a privacy-risk assessment. The Privacy Risk Assessment Tool developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) is designed to help CPAs and Chartered Accountants (CAs), management, owners and other privacy professionals accomplish this task in an effective and comprehensive manner. The Tool uses the 10 principles and 73 criteria contained in the AICPA/CICA Generally Accepted Privacy Principles, aicpa.org/privacy or cica.ca/privacy. It provides principles and criteria of good privacy practices contained in many privacy laws and regulations worldwide that may serve as benchmarks for your organization's privacy program.

The Privacy Risk Assessment Tool was designed in Microsoft Excel to make it as user-friendly and intuitive as possible. This User Guide will describe the features and functionality of the tool.

Do you have suggestions for enhancing this tool? Please send your comments to privacytool@aicpa.org.

II. Installation

Instructions for installing the AICPA/CICA Privacy Risk Assessment (PRA) Tool:

- Download the AICPA/CICA Privacy Risk Assessment Tool from aicpa.org/privacy or cica.ca/privacy.
- Follow the installation instructions.
- A new folder named AICPA Privacy Tool will be created on your computer (C:\), with the following files copied to the folder:
 - 10 Privacy Risk Assessment Tool – Scoring Input Template files
 - Privacy Risk Assessment Tool – Scoring Summary file

Note: Do not change the file names: the PRA Tool – Scoring Summary file contains links to each of the 10 PRA Tool – Scoring Input Templates files.

III. General Information

- The AICPA/CICA Privacy Risk Assessment Tool uses the 10 principles and 73 criteria in the AICPA/CICA Generally Accepted Privacy Principles (GAPP). GAPP is available for download at aicpa.org/privacy or cica.ca/privacy.
- The 10 Privacy Principles of GAPP are:
 1. Management
 2. Notice
 3. Choice and Consent
 4. Collection
 5. Use, Retention and Disposal
 6. Access
 7. Disclosure to Third Parties
 8. Security for Privacy
 9. Quality
 10. Monitoring and Enforcement

- The Privacy Risk Assessment Tool is designed to assist CPAs, CAs and privacy professionals in helping organizations assess privacy risks.
- The Privacy Risk Assessment Tool has two components, both of which are contained in Excel files:
 - PRA Tool – Scoring Input Template (10 separate files with unique names: User 1, User 2, etc.)
 - PRA Tool – Scoring Summary
- The PRA Tool – Scoring Input Template includes the 10 principles and 73 criteria and is used by the risk assessment team to record scores for each of the criteria.
- The PRA Tool – Scoring Summary is configured to automatically update scores from up to 10 PRA Tool – Scoring Input Templates.
- All cells in each file are protected, with the exception of those cells that require input from the individual participating in the assessment.
Note: A password was not used when protecting the files.
- Printing: The PRA Tool – Scoring Summary and Scoring Input Templates have been formatted for printing.
- The Header/Footer for each file and worksheet contains an area in which users can document who completed the scoring input, scope of the assessment and the date completed.

IV. Getting Started

- Assign someone in the organization to lead the privacy risk assessment. This individual should be a privacy professional who possesses a good understanding of privacy laws and regulations, privacy best practices, business operations, risk assessments, and current privacy practices and controls within the organization. This could be someone from the organization's privacy office, legal, IT, risk management, internal audit or an outside consultant. A CPA or CA possesses many of these skill sets.

- Determine if the privacy risk assessment should be performed under attorney-client privilege.

Meet with legal counsel for guidance and discuss the scope and objective of the privacy risk assessment. If it is completed under attorney-client privilege, legal counsel will control communication and distribution of the results of the assessment.

- Assemble the team that will perform the privacy risk assessment and complete the AICPA/CICA Privacy Risk Assessment Tool. Refer to sections V and VI below for detailed instructions on completing the Privacy Risk Assessment Tool.

The Risk Assessment Tool will accommodate up to 10 individuals. The individuals selected for the assessment team should possess a good understanding of the organization's privacy practices and controls, as well as privacy laws and regulations with which the organization must comply.

Because one assessor may not have full knowledge of the privacy practices and controls for all 10 principles assessed, every effort should be made to assemble a team that will provide full coverage of the 10 principles and 73 criteria in the Risk Assessment Tool.

- Utilize good project management skills, such as establishing budgets, timelines, documentation requirements, analyzing results, action items and identifying priorities.
- After the assessment team has been selected, provide a copy of the PRA Tool – Scoring Input Template to the assessors (up to 10) who will be completing the assessment.

Note: Provide a separate PRA Tool - Scoring Input Template for each assessor, using a file with a unique name for each assessor. For example, Assessor One would receive the PRA Tool – Scoring Input Template – User 1, Assessor Two would receive the PRA Tool – Scoring Input Template – User 2, and so on.

Do not change file names: there are cross-links in the PRA Tool – Scoring Summary that are dependent on the file-naming convention.

- After the assessors have entered scores in their respective Scoring Input Templates, copy the files into the AICPA Privacy Tool folder.
- After the completed PRA Tool - Scoring Input Templates have been copied into the AICPA Privacy Tool folder, open the PRA Tool – Scoring Summary file and select "UPDATE" if prompted to update the PRA Tool – Scoring Summary file.

V. PRA Tool—Scoring Input Template

- The PRA Tool – Scoring Input Template includes 10 principles and 73 criteria and is used by the risk assessment team to record scores for each of the criterion.

Note to assessor: If you do not have adequate knowledge or understanding of the privacy practices and controls for a given criterion, please leave the scoring input cell blank.

- There are 10 uniquely named PRA Tool – Scoring Input Template files to accommodate up to 10 assessors.
- Do not rename the file, because the cross-links in the PRA Tool – Scoring Summary file are dependent on the naming convention.
- The file is protected, except for the cells requiring input from the assessors.
- The cells requiring assessor scores are restricted to entering one of the three scores available (2 = Low Risk, 5 = Medium Risk or 8 = High Risk). A drop-down score menu is provided for each cell, or the assessor may manually enter the scores. Refer to the Scoring Guidance Worksheet section below for guidance on scoring.
- Scoring Input (worksheet tab):
 - The Header/Footer contains an area in which users can document the assessor's name ("completed by"), scope of the assessment and the date completed.
 - Column 1: 10 Principles and 73 Criteria.
Each criterion has a reference number that cross-references to the AICPA/CICA Generally Accepted Privacy Principles' criteria.

- Column 2: Criteria Description
Assessors are encouraged to consult GAPP for illustrative controls and procedures, and additional considerations regarding each criterion.
- Column 3: Likelihood of a Control Failure
As an assessor scoring each criterion, think in terms of whether the organization’s practices and controls are in place and working as intended. For example, the organization may have a control to restrict access to personal information, and the assessor knows that tightly controlled access to restricted information can warrant a lower risk rating. However, if the assessor knows the organization does not have an effective program to keep unauthorized individuals from accessing personal information, a higher risk rating may be appropriate.
- Column 4: Business Impact
Score this area as if the risk or control failure has occurred. Factors to consider when scoring business impact include reputation impact, monetary loss, regulatory and legal implications, customer impact, business operations and so forth.
- Column 5: Effort/Cost to Mitigate
Factors to consider when scoring this area include the staffing effort to remediate, time to implement a solution, complexity of the computing environment, capital expenditures required, cultural resistance from business owners, and so forth.
- Scoring Input Help (worksheet tab):
This section provides definitions, guidance and considerations when assessing the three scoring categories (Likelihood of a Control Failure, Business Impact and Effort/Cost to Mitigate) in the PRA Tool – Scoring Input Template.
- Scoring Guidance (worksheet tab):
There are three scores the assessor may enter into the Scoring Input Template (2 = Low Risk, 5 = Medium Risk, or 8 = High Risk). To help the assessor determine an appropriate score for that criterion, he or she may want to consider the following characteristics of different maturity levels for internal controls from COBIT 4.1.¹

1. Control Objectives for Information and related Technology (COBIT®) 4.1 found at www.isaca.org/cobit/.

Score	Characteristics
2 = Low Risk	<p>Maturity Level 5 – Optimized</p> <p>Maturity Level 4 – Managed and Measurable</p> <ul style="list-style-type: none"> • An effective internal control and risk management environment is in place. • A formal documented evaluation of privacy controls occurs frequently. • Many privacy controls are automated and regularly reviewed. • There is consistent follow-up to address identified privacy control weaknesses. • Privacy control evaluation is continuous, based on self-assessments and gap and root-cause analyses.
5 = Medium Risk	<p>Maturity Level 3 – Defined Process</p> <ul style="list-style-type: none"> • Privacy controls are in place and adequately documented. • Operating effectiveness is periodically evaluated and there are an average number of issues. • Management is able to deal predictably with most privacy control issues; however, some control weaknesses persist and impacts still could be severe. • Employees are aware of their responsibilities for privacy control.
8 = High Risk	<p>Maturity Level 2 – Repeatable but Intuitive</p> <p>Maturity Level 1 – Initial/Ad Hoc</p> <ul style="list-style-type: none"> • Privacy controls are in place but not documented. • Operational control is dependent on knowledge and motivation of individuals. • Effectiveness of privacy controls is not adequately evaluated. • Many privacy control weaknesses exist and are not adequately addressed. • Management actions to resolve privacy control issues are not prioritized. • Employees may not be aware of their responsibilities.

- After the assessor has completed the scoring, return the electronic file to the privacy risk assessment team lead to copy into the AICPA Privacy Tool folder.

Note: Do not change the name of the file.

VI. PRA Tool – Scoring Summary

- After the completed PRA Tool – Scoring Input Templates are copied into the AICPA Privacy Tool folder, open the PRA Tool – Scoring Summary file to view the risk-assessment scores for the 10 privacy principles.

Note: When the file launches, select “Update” if necessary to automatically update the scoring from the completed Scoring Input Template files in the AICPA Privacy Tool folder.

- Instructions (worksheet tab):

This section is a general-reference guide for using the Privacy Risk Assessment Tool.

- Scoring Input Help (worksheet tab):

This section provides definitions, guidance and considerations when assessing the three scoring categories (Likelihood of a Control Failure, Business Impact and Effort/Cost to Mitigate) from the PRA Tool – Scoring Input Template.

- Scoring Guidance (worksheet tab):

Refer to explanation in Section V of this document.

- 10 Privacy Principles (worksheet tabs):

- This section of the Scoring Summary recaps the scoring by each assessor for each privacy principle. This section of the file is automatically updated from the completed PRA Tool – Scoring Input Template files located in the AICPA Privacy Tool folder.

Note: Select “Update” when opening the PRA Tool – Scoring Summary file.

- An average score for each privacy principle is calculated for each of the three scoring categories and presented in the Average Score row. For example, for the Management Principle, the Average Score row reads “Average Score – 14 Criteria,” as displayed in the following exhibit.
- An average score for each criterion is also calculated for each of the three scoring categories and displayed in the Total row.

**Privacy Risk Assessment Scoring Summary
– Management Principle
AICPA/CICA GAPP**

Scoring: 2=Low Risk, 5=Medium Risk, 8=High Risk

1.0 Management	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
14 Criteria	Average Score - 14 Criteria	2.8	5.3	3.7
Privacy Policies (1.1.0)	Policies are defined for: notice, choice/consent, collection, use/retention, access, disclosure, security, quality, and monitoring and enforcement.			
Input 1		5	5	2
Input 2		2	5	2
Input 3		2	2	5
Input 4		5	5	2
Input 5		5	8	5
Input 6		2	5	5
Input 7		2	5	2
Input 8		5	8	5
Input 9		2	5	5
Input 10		2	2	2
	Average Score	3.2	5.0	3.5

Note: #DIV/0! will display in the cell until the completed PRA Tool – Scoring Input Template files are updated to the PRA Tool – Scoring Summary file.

- Summary Risk Chart Input (worksheet tab):

A chart that recaps the scoring input for each of the 10 generally accepted privacy principles used to build the Summary Risk Chart (worksheet tab). The cells in this table are cross referenced to the appropriate cells in each of the privacy principle worksheet tabs and should not be modified.

- Summary Risk Chart (worksheet tab):

A chart that graphically displays the average scoring input for each of the 10 generally accepted privacy principles. The X-axis illustrates the likelihood of a control failure. The Y-axis illustrates the business impact and the size of the “balloons” indicate the effort/cost to mitigate the impact.

Note: Because the graphical displays on this chart are dependent upon the scoring by the assessment team, the labels for each bubble may need to be adjusted for appropriate viewing — some bubbles may overlay others. Unprotect the worksheet first in order to move the label for each “balloon” to its desired location. Protect the worksheet when finished.

- Detail Risk Chart Input (worksheet tab):

A chart that recaps the scoring input for each of GAPP’s 73 privacy criteria. The cells in this table are cross referenced to the appropriate cells in the privacy principle worksheet tabs and should not be modified.

VII. Privacy Risk Assessment Team Action Items

After the privacy risk assessment team completes the scoring for GAPP’s 10 principles and 73 criteria, the team should analyze the results and agree that the scoring represents the privacy environment of the organization.

Suggested action steps for the privacy risk assessment team:

- Identify and analyze any criteria that had wide scoring variations from the assessors (e.g., several rated the criteria Low Risk and several rated it High Risk). Discuss the criteria among the team to determine if general consensus can be reached. Follow up with appropriate business owners if necessary to help reach agreement.

- Identify and analyze the privacy principles that came in with a High Risk score. Discuss among the team to validate consensus with the rating.
- Identify and analyze the privacy principles that came in with a Low Risk score. Discuss among the team to validate consensus with the rating.
- At this point, the team may want to narrow their focus to selected principles they would like to address in greater detail. This would include analyzing scoring results for each criterion for the selected principles and focusing on them.

Examples of action items include:

- meeting with business owners to discuss results of the privacy risk assessment;
- documenting practices and controls around the criteria;
- determining if remediation efforts are necessary to mitigate any unnecessary risks;
- assigning responsibility to identify appropriate remediation efforts;
- performing a privacy audit of a selected area; and
- obtaining privacy professionals to help address the privacy risks with greater risk.

VIII. Privacy Resources

American Institute of Certified Public Accountants - aicpa.org/privacy

Canadian Institute of Chartered Accountants - cica.ca/privacy

IX. AICPA/CICA Privacy Task Force Members

Everett Johnson, CPA, Chair

Ken Askelson, CPA.CITP, CIA, Vice Chair

Eric Federing - KPMG

Philip M. Juravel, CPA.CITP - Juravel & Company, LLC

Sagi Leizerov, Ph.D., CIPP - Ernst & Young

Rena Mears, CPA.CITP, CIPP, CISSP, CISA – Deloitte & Touche, LLP

Robert Parker, FCA, CA-CISA, CMC

Marilyn Prosch, Ph.D., CIPP - Arizona State University

Doron Rotman, CPA (Israel), CIPP, CISA, CIA, CISM - KPMG

Kerry Shackelford, CPA - Coalfire System, Inc.

Don Sheehy, CA-CISA, CIPP/C – Deloitte & Touche, LLP

Nancy A. Cohen, CPA.CITP, CIPP - AICPA

Nicholas F. Cheung, CA, CIPP/C - CICA

