

# Frequently Asked Questions on the Use of Generally Accepted Privacy Principles in WebTrust Engagements

## Table of Contents

FREQUENTLY ASKED QUESTIONS ON THE USE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES IN WEBTRUST ENGAGEMENTS.....	1
<b>Table of Contents</b> .....	<b>1</b>
<b>Introduction</b> .....	<b>1</b>
<b>Relationship of GAPP and Trust Services</b> .....	<b>2</b>
<i>QUESTION 1 – GAPP AND WEBTRUST</i> .....	2
<i>QUESTION 2 - GAPP AND SYSTRUST</i> .....	2
<i>QUESTION 3 - WORDING OF WEBTRUST ONLINE PRIVACY REPORT</i> .....	2
<i>QUESTION 4 - SCOPE OF A WEBTRUST ONLINE PRIVACY AUDIT</i> .....	2
<i>QUESTION 5 –THE EXAMINATION AND REPORT COVERAGE OF ALL TEN PRIVACY PRINCIPLES...</i>	3
<i>QUESTION 6 – ONLINE SEGMENT VS. PRIVACY NOTICE</i> .....	3
<i>QUESTION 7- RELATIONSHIP BETWEEN TRUST SERVICES, GAPP, AND WEBTRUST</i> .....	4
<i>QUESTION 8 – RESOURCE GUIDANCE</i> .....	4
<i>QUESTION 9 - WEBTRUST CONSUMER PROTECTION SEAL EXISTENCE</i> .....	4
<i>QUESTION 10 – ISSUANCE OF COMBINED REPORT</i> .....	4
<i>QUESTION 11 – COMPARISON OF TRUST SERVICES PRINCIPLES</i> .....	5
<b>Appendix A- Illustrative Independent Practitioner’s WebTrust Report</b> .....	<b>6</b>
<i>ILLUSTRATION ONE —REPORTING ON MANAGEMENT’S ASSERTION</i> .....	6
<i>ILLUSTRATIVE MANAGEMENT ASSERTION</i> .....	7
<i>ILLUSTRATION 2—REPORTING DIRECTLY ON THE SUBJECT MATTER</i> .....	8

## Introduction

Generally Accepted Privacy Principles (GAPP) are privacy principles and criteria that have been developed by AICPA and CICA to assist organizations in creating an effective privacy program that addresses their privacy risks and business opportunities. GAPP can be used by organizations to perform privacy strategic and business planning, privacy gap and risk analysis, benchmarking, privacy policy design and implementation, performance measurement, and to monitor and audit privacy programs. GAPP consists of ten generally accepted privacy principles, supported by criteria, based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

The WebTrust service is one of several types of Trust Services engagements and is an audit examination of management’s assertions related to an ecommerce-based business segment. Upon attainment of a CA practitioner’s unqualified audit report, the entity may choose (under certain conditions) to display a WebTrust Seal and an accompanying auditor’s report on its Web site. The audit examination requires the use of CICA Section 5025 - Standards for Assurance Engagements. GAPP supersedes the online privacy principle and criteria that were used in a WebTrust engagement and is broader in scope (for example, they can be applied to an entire enterprise, not just the ecommerce-based business segment).

These Frequently Asked Questions (FAQs) provide suggestions and clarifications on the application of GAPP in audit engagements, with emphasis on those engagements in which the superseded Trust Services' online privacy principle and criteria were used previously. This includes WebTrust Online Privacy and other Trust Services engagements. The responses represent views expressed by the AICPA/CICA Privacy Task Force and do not necessarily represent the official views of the American Institute of Certified Public Accountants (AICPA) or the Canadian Institute of Chartered Accountants (CICA).

## Relationship of GAPP and Trust Services

### Question 1 – GAPP and WebTrust

Can GAPP be used in a WebTrust engagement?

Yes - The privacy criteria in GAPP have now been incorporated into *Trust Services Principles, Criteria and Illustrations* for use in a WebTrust engagement. Please refer to [Appendix C](#) of the CPA/CA practitioner version of Generally Accepted Privacy Principles on the AICPA website. It is also available on the [CICA website](#).

When the privacy engagement relates to an online segment, an entity may choose to display a WebTrust Online Privacy seal. For these engagements, the scope needs to include, as a minimum, an online business segment of the entity.

### Question 2 - GAPP and SysTrust

Can GAPP be used in a SysTrust engagement?

GAPP can not be used in a SysTrust engagement. A SysTrust engagement focuses on controls within one defined system. A privacy audit engagement (such as WebTrust), on the other hand, focuses on protection of personal information throughout lifecycle (i.e., from collection through destruction) within the business or business segment, as defined by the terms of the engagement. This often involves more than one system.

### Question 3 - wording of WebTrust online privacy report

How would a WebTrust online privacy report be worded using GAPP?

See [Appendix A](#) to these FAQs.

### Question 4 - scope of a WebTrust online privacy audit

What is the scope of a WebTrust online privacy audit using GAPP?

As set out in [Appendix C](#) of the CPA/CA practitioner version of "Generally Accepted Privacy Principles":

The scope of the engagement can cover (1) either all personal information or only certain identified types of personal information, such as customer information or employee information, and (2) all business segments and locations for the entire entity or only certain identified segments of the business (such as retail operations, but not manufacturing operations or such as only operations originating on the entity's Web site) or geographic locations (such as only Canadian operations). In addition:

- o The scope of the engagement generally should be consistent with the description of the entities and activities covered in the privacy notice (see GAPP Criterion 2.2.2). The scope often could be narrower, but ordinarily not broader, than that covered by the related privacy notice.
- o The scope of the engagement should cover all of the activities in the “information lifecycle” for the relevant personal information. These should include collection, use, retention, disclosure and destruction, de-identification or anonymization. Defining a segment that does not include this entire cycle could be misleading to the user of the practitioner’s report.
- o If the identified personal information included in the scope of the examination is commingled with other information not in the scope of the engagement, the privacy assurance engagement needs to cover controls over all of the information from the point of commingling forward.

Using the above guidance, a report can be issued on an online system as an identified business segment subject to the provisions in the preceding three bullets.

**Question 5 –the examination and report coverage of all ten privacy principles**

In a WebTrust online privacy engagement, does the examination and report need to cover all ten privacy principles?

Yes - Generally Accepted Privacy Principles are founded on the following 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.*

This privacy objective is equivalent to a single Trust Services Principle (e.g., Security, Availability). This privacy objective can only be met through an examination and meeting of the ten privacy principles.

As set out in Appendix C of the CPA/CA practitioner version of “Generally Accepted Privacy Principles:

“A privacy assurance report ordinarily covers all ten principles. All of their relevant criteria need to be met during the period covered by the report to issue an unqualified report.”

**Question 6 – online segment vs. privacy notice**

For a WebTrust online privacy engagement, what is the difference between the description of the online segment covered by the examination (set out in the practitioner’s report) and the organization’s privacy notice (typically referenced from its web site)?

They are entirely different in purpose. The privacy notice provides information as to the organization’s privacy policies that are disclosed as being in place. The description of the online segment provides the description of the online business segment being subjected to examination.

In a WebTrust engagement, the practitioner is engaged to examine both that an entity maintained effective controls over the system under review (in this case, GAPP), and that it complied with its commitments regarding the stated Trust Services Principle(s) (in this case, its disclosures in its privacy notice).

Ideally, when using GAPP for the online engagement, organizations may consider having a separate privacy notice covering the systems subject to examination to reduce any confusion.

### **Question 7- relationship between Trust Services, GAPP, and WebTrust**

What is the relationship between Trust Services, GAPP, and WebTrust?

**Trust Services** are a set of professional assurance and advisory services based on a common framework to address the risks and opportunities of Information Technology. It includes the following principles and criteria:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

**GAPP** represents the related principles and criteria for Privacy in this framework.

The **WebTrust** service consists of an examination of an ecommerce-based business segment and, upon attainment of an unqualified assurance report, allows the entity to display a WebTrust Seal and an accompanying auditor's report on its Web site. As discussed in question 1, WebTrust Online Privacy is likewise an examination of an online business segment and, upon attainment of an unqualified assurance report, an entity may choose to display a WebTrust Online Privacy seal.

### **Question 8 – resource guidance**

Where can I find resource guidance for Trust Services and Privacy Services?

These can be found as follows:

Trust Services:

- [AICPA](#)
- [CICA](#)

Privacy Services:

- [AICPA](#)
- [CICA](#)

The CICA offers the following products for Privacy Services (see the Store at <https://www.knotia.ca>):

- 20 Questions Businesses Should Ask About Privacy – No. 04420
- Solutions for Today's Privacy Issues – No. 02980

### **Question 9 - WebTrust Consumer Protection Seal existence**

The WebTrust Consumer Protection Seal was available in the past for entities that met the Trust Services Processing Integrity and Online Privacy Principles. Can this seal continue to be issued?

No.

This special seal and related practitioner's report was seldom used and is now discontinued. However, a WebTrust seal, without the "Consumer Protection" designation could still be issued.

### **Question 10 – issuance of combined report**

Can you issue one combined report on Privacy (using GAPP) and another Trust Services principle (such as availability)?

Yes, but the task force does not recommend a combined report in this scenario. Since privacy needs to address the entire information cycle from collection to destruction there are often several systems involved. Unless the other principle (i.e., availability in this scenario) also covers all systems involved in the entire information lifecycle, a combined report ordinarily would be overly complex and difficult for a user to understand. It is preferable to issue two separate reports that can be linked by a common seal.

**Question 11 – comparison of Trust Services Principles**

Can you summarize how the various types of Trust Services principles and criteria relate to the different services?

See table below.

	<b>Attestation Engagement With No Seal or Other CICA Branding</b>	<b>Trust Services</b>	
		<b>SysTrust</b>	<b>WebTrust</b>
<b>Principles:</b>			
<b>Availability</b>	Yes	Yes	Yes
<b>Security</b>	Yes	Yes	Yes
<b>Process integrity</b>	Yes	Yes	Yes
<b>Confidentiality</b>	Yes	Yes	Yes
<b>Privacy - GAPP</b>	Yes	No	Yes
<b>System</b>		Any system described in system description	Online system
<b>Seal</b>	No seal.	SysTrust Logo can be licensed for use	WebTrust Logo can be licensed for use
<b>Public Report</b>	Yes	Yes	Yes
<b>Other</b>			

## Appendix A- Illustrative Independent Practitioner's WebTrust Report

### Illustration One —Reporting on Management's Assertion

#### Auditor's WebTrust Privacy Report

To the Management of ABC Company, Ltd.:

We have audited ABC Company, Inc.'s (ABC Company) management assertion that, during the period Xxxx xx, 2008 through Yyyy yy, 2008 it:

Maintained effective controls over the privacy of personal information collected in its \_\_\_\_\_ [description of the entities and activities covered, for example "the mail-order catalog-sales operations"] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, and disclosed in accordance with its commitments in its privacy notice related to the Business and with criteria set forth in Generally Accepted Privacy Principles, issued by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants, and

Complied with its commitments in its privacy notice.

This assertion is the responsibility of management. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with ABC Company's commitments in its privacy notice and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, ABC Company's management assertion that, during the period Xxxx xx, 2008 through Yyyy yy, 2008, ABC Company:

Maintained effective controls over privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained and disclosed in accordance with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles; and  
Complied with its commitments in its privacy notice,

is, in all material respects, fairly stated.

*OR*

In our opinion, ABC Company management's assertion referred to above is fairly stated, in all material respects, in accordance with ABC Company's privacy notice and with criteria set forth in Generally Accepted Privacy Principles.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

ABC Company's use of the WebTrust Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[Name of CA firm]  
Chartered Accountants

[City, Province]  
[Date]

### **Illustrative Management Assertion**

During the period Xxxx xx, 2008 through Yyyy yy, 2008, ABC Company, in all material respects:

Maintained effective controls over the privacy of personal information collected in our \_\_\_\_\_business [*description of the activities covered, for example "the mail-order catalog-sales operations"*] (the Business) to provide reasonable assurance that the personal information was collected, used, retained and disclosed in accordance with our commitments in the privacy notice related to the Business and with the criteria set forth in Generally Accepted Privacy Principles, issued by the Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants and, Complied with our commitments in our privacy notice.

## Illustration 2—Reporting Directly on the Subject Matter

### Auditor's WebTrust Privacy Report

To the Management of ABC Company, Ltd.:

We have audited (1) the effectiveness of ABC Company, Inc.'s (ABC Company) controls over the personal information collected in its \_\_\_\_\_ [*description of the entities and activities covered, for example "the mail-order catalog-sales operations"*] business (the Business) to provide reasonable assurance that the personal information was collected, used, retained, and disclosed in accordance with its commitments in its privacy notice and with criteria set forth in Generally Accepted Privacy Principles, issued by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants, and (2) ABC Company's compliance with its commitments in its privacy notice related to the Business during the period Xxxx xx, 2008 through Yyyy yy, 2008. ABC Company's management is responsible for maintaining the effectiveness of these controls and for compliance with its commitments in its privacy notice. Our responsibility is to express an opinion based on our audit.

Our audit was conducted in accordance with standards for assurance engagements established by the CICA. Those standards require that we plan and perform our audit to obtain reasonable assurance as a basis for our opinion. Our audit included (1) obtaining an understanding of ABC Company's controls over the privacy of personal information, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with ABC Company's commitments in its privacy notice, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, during the period Xxxx xx, 2008 through Yyyy yy, 2008 ABC Company, in all material respects (1) maintained effective controls over privacy of personal information collected in the Business to provide reasonable assurance that the personal information was collected, used, retained, and disclosed in accordance with its commitments in its privacy notice and with criteria set forth in the Generally Accepted Privacy Principles; and (2) complied with its commitments in its privacy notice.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

ABC Company's use of the WebTrust Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

[*Name of CA firm*]  
Chartered Accountants

[*City, Province*]  
[*Date*]