

WebTrust[®] for Certification Authorities

COMBINED US (AICPA) STANDARDS – AT-C205 AND ISAE 3000 REPORT

Published 1 October 2023

Version 1.0

Copyright © 2023 by Chartered Professional Accountants of Canada (“CPA Canada”). All rights reserved. These Principles and Criteria may be reproduced and distributed provided that reproduced materials are not in any way directly or indirectly offered for sale or profit and attribution is given.

Introduction¹

Inquiry

May a U.S. Certified Public Accountant (CPA) perform a WebTrust examination in accordance with both AT-C section 205 of the attestation standards issued by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3000 (Revised) of the assurance standards issued by the International Auditing and Assurance Standards Board (IAASB)?

Reply

Yes. A U.S. CPA may be engaged to perform a WebTrust examination for a U.S. Certification Authority (CA) under both standards. A frequently asked question titled “Use of standards that have not been established by a body designated by AICPA Council” clarifies that a member is permitted to apply any relevant alternative standards in an attestation examination. Therefore, a U.S. CPA who performs a WebTrust examination in accordance with AT-C section 205 may also perform the examination in accordance with ISAE 3000 (Revised) and issue one report that states that the examination was performed in accordance with the attestation standards established by the AICPA and ISAE 3000 (Revised) issued by the IAASB, provided the U.S. CPA complies with the requirements of both sets of standards and there are no conflicts between AT-C section 205 and ISAE 3000 (Revised) that would lead the U.S. CPA to reach a different conclusion with respect to the opinion.

Although many of the requirements of AT-C section 205 and ISAE 3000 (Revised) are similar, there are certain differences. For example, under the requirements of ISAE 3000 (Revised), a practitioner may issue an examination report without obtaining a written assertion from the responsible party; under AT-C section 205, a practitioner is not permitted to issue an examination report if the practitioner has not obtained such an assertion from the responsible party, except when the responsible party is not the engaging party. In a WebTrust examination under ISAE 3000 (Revised) a management assertion is expected to accompany the report, however.

A WebTrust examination performed in accordance with both the attestation standards and ISAEs is expected to be similar in scope and approach to a WebTrust examination performed in accordance with only the attestation standards. To make it easier for U.S. CPAs engaged to examine and report under both sets of standards, the Auditing Standards Board (ASB) has published “Substantive Differences Between International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, and AT-C sections 105, *Concepts Common*

¹ This was adapted from AICPA Guide Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (AICPA. October 2022) Appendix G.

to *All Attestation Engagements*, and 205, *Assertion-Based Examination Engagements*, of *Statements on Standards for Attestation Engagements*,” which identifies the substantive differences between the requirements of the attestation standards (AT-C sections 105 and 205) and ISAE 3000 (Revised). The document is available on the [AICPA website](#).

When the U.S. CPA has performed a WebTrust examination in accordance with the attestation standards and the ISAEs, the U.S. CPA would indicate in the report that the examination *was also conducted in accordance with ISAE 3000 (Revised)*. In addition, the U.S. CPA’s report would need to include the elements of the auditor’s report included in paragraphs .63–.68 of AT-C section 205 and paragraph .69 of ISAE 3000 (Revised).

The following is an illustrative report that meets the requirements in AT-C section 205 and ISAE 3000 (Revised) related to the contents of the report, when the U.S. CPA is reporting under both standards. The illustrative WebTrust report is prepared in accordance with AT-C section 205; additions included to meet the requirements of ISAE 3000 (Revised) are shown in ***boldface italics***.

Example U.S. 1.1 – Unmodified opinion, reporting on management’s assertion, period of time

REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of ABC Certification Authority, Inc. (“ABC-CA”)

Scope²

We have examined ABC-CA management’s assertion³ that for its Certification Authority (CA) operations at <LOCATION>⁴, for its CAs as enumerated in Attachment A [or list Root Subordinate CAs in scope]⁵, ABC-CA has

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [name and version of certification practice statement(s)]; and
 - [name and version of certificate policy(ies) (if applicable)]⁶

2 Subheadings are optional and can be removed if desired.

3 Hyperlink to assertion.

4 CA processing locations as defined in the “Reporting Guidance” section.

5 Reference to an appendix or replace with list of Root and Subordinate CAs in scope. Refer to “Reporting Guidance” section.

6 At least one of these documents should be hyperlinked. Refer to “Reporting Guidance” section. If the CA does not have a separate CP then remove the second bullet.

- maintained effective controls to provide reasonable assurance that:
 - [ABC-CA’s Certification Practice Statement(s) is(are) consistent with its Certificate Policy(ies)]⁷
 - ABC-CA provides its services in accordance with its Certificate Policy(ies) (if applicable) and Certification Practice Statement(s)⁸
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by ABC-CA); and
 - subordinate CA certificate requests are accurate, authenticated and approved
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity

throughout the period <DATE> to <DATE> based on the WebTrust Principles and Criteria for Certification Authorities v2.x.⁹

[(If external Registration Authorities (RAs) are used) ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA’s business practices. Our examination did not extend to the controls exercised by these external registration authorities.]¹⁰

[ABC-CA does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.]¹¹

7 Remove bracketed text / bullet if CA has a combined CP and CPS document.

8 If CA has a combined CP / CPS then remove references to Certificate Policy.

9 Include applicable version number and hyperlink to the criteria document.

10 Remove bracketed text if external RAs are not used.

11 Modify this paragraph as appropriate to exclude certain criteria from scope. Please note that criteria can be excluded only if the CA does not provide the related service.

Certification Authority’s responsibilities

ABC-CA’s management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.x.

Practitioner’s responsibilities

Our responsibility is to express an opinion on ABC-CA management’s assertion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants **and in accordance with International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board**. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management’s assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with **the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants’ Code of Ethics for Professional Accountants**.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion management’s assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of ABC-CA’s services other than its *CA operations at <LOCATION>*¹², nor the suitability of any of ABC-CA’s services for any customer’s intended purpose.

Use of the WebTrust seal

[(If a seal is issued) ABC-CA’s use of the WebTrust for Certification Authorities 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.]¹³

[Practitioner’s signature]

[Practitioner’s city and state]

[Date of practitioner’s report]

12 CA processing locations as defined in the “Reporting Guidance” section.

13 Remove bracketed text if a seal is not issued.