**OBJECT OF VERIFICATION**

Confirmation of an organization’s claim of conformity to National Standard of Canada, CAN/CIOSC 103-1, Digital Trust and Identity – Part 1: Fundamentals through the provision of objective evidence, that the specified requirements in CAN/CIOSC 103-1 have been fulfilled.

**ASSURANCE ENGAGEMENT**

An assurance engagement is an engagement in which an independent practitioner performs procedures with an aim to obtain sufficient appropriate evidence in order to express a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the measurement or evaluation of an underlying subject matter against criteria.

Using the Canadian Standards for Assurance Engagement (e.g. CSAE 3000 and CSAE 3001) published in the *CPA Canada Handbook – Assurance*, a practitioner can undertake an assurance engagement on a variety of subject matters. For example, management of an entity may request a practitioner to express an opinion on management’s evaluation of whether the entity’s system/tool/process meets the requirements of a specific CIOSC standard. The CIOSC Standard forms the criteria against which management evaluates the entity’s system/tool/process.

**TYPES OF ASSURANCE ENGAGEMENTS AND REPORTS**

***“Reasonable” assurance vs. “Limited” assurance***

A practitioner can provide two levels of assurance engagements – a reasonable assurance engagement (in some cases referred to as an “audit”) and a limited assurance engagement (in some cases referred to as a “review”). Determining the level of assurance is a choice based upon the extent of assurance an entity requires or prefers. The key difference between the two types of assurance is the evidence obtained and the type of opinion expressed. The suitability of the criteria is not contingent on the level of assurance.

The Table below illustrates the key differences between the two levels of assurance engagements.

|  |  |  |
| --- | --- | --- |
|  | **Reasonable Assurance** | **Limited Assurance** |
| **Criteria** | The suitability of criteria is not contingent on the level of assurance. If criteria are not suitable for a reasonable assurance engagement, they would also not be suitable for a limited assurance engagement. | |
| **Level of Assurance** | High level of assurance, but not absolute level of assurance[[1]](#footnote-1). | Lower than in a reasonable level of assurance, but a level of assurance that is meaningful by providing confidence to users about the subject matter being reported. |
| **Reporting** | The practitioner expresses an opinion on whether management’s statement that the entity’s specific system/tool/process met the requirements of the CIOSC standard is fairly stated, in all material respects.  See Appendix E for an illustrative Independent practitioner’s reasonable assurance report. | The practitioner expresses a conclusion on whether anything has come to their attention that causes them to believe that management’s statement that the entity’s specific system/tool/process met the requirements of the CIOSC standard is not fairly stated, in all material respects[[2]](#footnote-2).  See Appendix F for an illustrative Independent practitioner’s limited assurance report. |

**An “Attestation” engagement vs. “Direct” engagement**

Assurance engagements (reasonable or limited assurance engagements) can be further differentiated into attestation engagements and direct engagements.

In an attestation engagement, management of the entity prepares an explicit, written statement of the entity’s compliance with the CIOSC standard for an external party and the practitioner then reports on this statement. In a Direct engagement, management does not prepare an explicit, written statement for an external party of the entity’s compliance with the CIOSC standard and the practitioner reports directly on the entity’s compliance with the CIOSC standard.

Attestation engagements are generally preferred by users because:

1. management is responsible for their business, and therefore, they are in a better position to assert the entity’s compliance with specific criteria or a standard.
2. management better understands the intended users and what information would be meaningful to them.

The table below illustrates the key differences between the two engagements.

| **Key Differences** | **Attestation Engagement** | **Direct Engagement** |
| --- | --- | --- |
| **Measurer / evaluator** | Management measures or evaluates the entity’s specific system/tool/process against the criteria used for the particular engagement (e.g., the CIOSC Standard) and provides an explicit, written statement to intended users about the outcome of that measurement or evaluation. The practitioner then reports on management’s statement. | The entity’s management does not provide a statement to the intended users. Practitioner (rather than management) measures or evaluates the entity’s specific system/tool/process against the criteria used for the particular engagement and reports directly to intended users about the outcome of that measurement or evaluation..  While management does not provide a statement to the intended users, the practitioner seeks from management a written acknowledgement of responsibility for the specific system/tool/process. |
| **Reporting** | The practitioner’s report includes an opinion on whether management’s statement that the entity’s specific system/tool/process has met the requirements of the CIOSC standard is fairly stated, in all material respects. | The practitioner’s report includes an opinion on whether the entity’s specific system/tool/process has met the requirements of the CIOSC standard. |

**COMPETENCE OF PERSONNEL**

*The criteria for competence of personnel for the verification team and body.*

**CONDUCTING AN ASSESSMENT**

*The process steps to be undertaken as a minimum in conducting the verification activities to achieve the intended results.*

**LEVEL OF ASSURANCE**

*The level of assurance, if required, and the materiality.*

**EVIDENCE GATHERING**

*The evidence gathering activities of verification.*

All evidence provided and or collected during the assessment process will be held in confidence (including publicly available evidence)

See Conformance Criteria

**REPORTING**

*The reporting requirements.*

**REVIEW**

*The review activities including the confirmation that all activities have been completed in accordance with the programme requirements.*

**INTERPRETATION**

*The way in which the results of the verification are to be interpreted and what the consequences are of the results — this also means that it should be laid down which findings prevent the issuance of a verification statement.*

**VERIFICATION STATEMENTS**

*The wording used for verification statements, because sector specific terminology can be used.*

*The verification statement issued on the basis of the evaluation of the claim in order to be in accordance with the validation/verification carried out.*

**Illustrative Management Statement**

*The following is an example management statement to illustrate how XYZ Organization may present management’s evaluation of XYZ’s* ***Digital Identity Program*** *based on the* ***National Standard of Canada, CAN/CIOSC 103-1,******Digital Trust and Identity – Part 1: Fundamentals*** *and its assertion that the Program has met the requirements of the standard. In the following examples, the entity presents a description (not included below) of its Program and processes in place throughout a period of time (note - point in time reporting is also an option but not illustrated in the following appendices) to demonstrate how it adhered to the requirements of the National Standard of Canada, along with the example management statement.*

XYZ Organization's Management’s Statement

We are responsible for designing, implementing, operating, and maintaining XYZ Organization’s (XYZ) Digital Identity Program (program) throughout the period January 1, 20XX to December 31, 20XX to achieve XYZ’s requirements for creating and maintaining trust in digital systems and services that, as part of an XYZ Organization’s mandate, assert and or consume Identity and Credentials in data pertaining to people and Organizations. Our description of the program is presented in attachment A and identifies the aspects of the program, covered by our statement. *[Note: the description is not included in this illustrative example]*

We have evaluated XYZ’s program against the National Standard of Canada, CAN/CIOSC 103-1, established by the CIO Strategy Council of Canada (the applicable criteria) throughout the period January 1, 20XX to December 31, 20XX.

There are inherent limitations in any program, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, XYZ cannot guarantee that its program, is absolutely compliant with the applicable criteria.

We confirm, to the best of our knowledge and belief, that the description fairly presents XYZ’s program, and that the program met the applicable criteria throughout the period January 1, 20XX to December 31, 20XX.

**Illustrative Independent Attestation Practitioner’s Report (Reasonable Assurance Engagement)**

*The following is an example reasonable assurance (audit) attestation report to illustrate how a practitioner may report on their evaluation of management’s statement (see example in Appendix D) that its system met the requirements of the* ***National Standard of Canada, CAN/CIOSC 103-1,******Digital Trust and Identity – Part 1: Fundamentals****. Note that in this example:*

* *management is responsible for preparing both an appropriate description of the program as well as a written statement that it has assessed the program and that the program has met the requirements of the National Standard of Canada, CAN/CIOSC 103-1, Digital Trust and Identity – Part 1: Fundamentals (Appendix A);*
* *the practitioner’s opinion is expressed in terms of management’s statement and the applicable criteria; and*
* *the practitioner attaches management’s statement (Appendix A) to the practitioner’s report*.

Independent Practitioner’s Reasonable Assurance Report

To: [Addressee]

We have undertaken a reasonable assurance engagement to report on the accompanying statement by XYZ Organization (XYZ) that its Digital Identity Program (program) met the requirements set out in the National Standard of Canada, CAN/CIOSC 103-1, Digital Trust and Identity – Part 1: Fundamentals, established by the CIO Strategy Council of Canada (the “applicable criteria”) throughout the period January 1, 20XX, to December 31, 20XX.

**Management's Responsibility**

Management of XYZ is responsible for preparing the attached description of XYZ’s program, for evaluating the program against the applicable criteria, and for preparing its attached statement. Management is also responsible for such internal control as management determines necessary to enable and maintain the conformity of XYZ’s program with the applicable criteria.

**Our Independence and Quality Control**

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

**Our Responsibility**

Our responsibility is to express a reasonable assurance opinion on management’s statement based on the evidence we have obtained.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements (CSAE) 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether the management’s statement is fairly stated, in all material respects.

Reasonable assurance is a high level of assurance but is not a guarantee that an engagement conducted in accordance with this standard will always detect a material instance of non-conformity with specified requirements when it exists. Instances of non-conformity can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of users of our report. A reasonable assurance engagement involves performing procedures to obtain evidence about management's statement of its system’s conformity with the specified requirements. The nature, timing and extent of procedures selected depends on our professional judgment, including an assessment of the risks of material misstatement of management's statement, whether due to fraud or error, and involves obtaining evidence about management's statement.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

**Opinion**

In our opinion, management’s statement that XYZ’s Digital Identity Program met the applicable criteria throughout the period January 1, 20XX, to December 31, 20XX is fairly stated, in all material respects.

Practitioner's signature

City, Province

Date

**Illustrative Independent Attestation Report (Limited Assurance Engagement)**

*The following is an example limited assurance (sometimes referred to as negative assurance) attestation report to illustrate how a practitioner may report on management’s statement (see example in Appendix D) that its program met the requirements of the* ***National Standard of Canada, CAN/CIOSC 103-1,******Digital Trust and Identity – Part 1: Fundamentals****. Note that in this example:*

* *management is responsible for preparing both an appropriate description of the program as well as a written statement that it has assessed the program and that the program has met the requirements of the the National Standard of Canada, CAN/CIOSC 103-1, Digital Trust and Identity – Part 1: Fundamentals (Appendix A);*
* *the practitioner’s conclusion is expressed in terms of management’s statement and the applicable criteria*
* *the practitioner attaches management’s statement (Appendix A) to the practitioner’s report.*

Independent Practitioner’s Limited Assurance Report

To: [Addressee]

We have undertaken a limited assurance engagement to report on the accompanying statement by XYZ Organization’s (XYZ) that its Digital Identity Program (program) met the requirements set out in the National Standard of Canada, CAN/CIOSC 103-1, Digital Trust and Identity – Part 1: Fundamentals, established by the CIO Strategy Council of Canada (the “applicable criteria”) throughout the period January 1, 20XX, to December 31, 20XX.

**Management's Responsibility**

Management of XYZ is responsible for preparation of the attached description of XYZ’s program, for evaluating the system against the applicable criteria, and for preparing its attached statement. Management is also responsible for such internal control as management determines necessary to enable XYZ’s compliance with the applicable criteria.

**Our Independence and Quality Control**

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

**Our Responsibility**

Our responsibility is to express a limited assurance conclusion on management’s statement based on the evidence we have obtained.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements (CSAE) 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires us to plan and perform our engagement to conclude whether anything has come to our attention that causes us to believe that management’s statement is not fairly stated, in all material respects.

A limited assurance engagement involves performing procedures (primarily consisting of making inquiries of and reviewing information provided by management and others within the entity, as appropriate, and applying analytical procedures) and evaluating the evidence obtained. The procedures are selected based on our professional judgment, which includes identifying areas where the risks of material misstatement in the management statement are likely to arise.

The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement and, consequently, the level of assurance obtained is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed.

**Conclusion**

Based on the procedures we have performed and the evidence we have obtained, nothing has come to our attention that causes us to believe that management’s statement that XYZ’s Digital Identity Program met the applicable criteria throughout the period from January 1, 20X1 to December 31, 20X1, is not fairly stated, in all material respects.

Practitioner's signature

City, Province

Date

**RECORDS**

*Requirements regarding what records the verification body should retain as an evidence of conducting verification.*

1. Reasonable assurance is not an absolute level of assurance because there are inherent limitations to any engagement which make most of the evidence from which the practitioner draws conclusions and bases their opinion *persuasive* rather than *conclusive*. [↑](#footnote-ref-1)
2. This style of reporting is known as negative assurance. [↑](#footnote-ref-2)