



PCTF Verified Organization Conformance Profile

Document Status: Final Recommendation V1.0

In accordance with the [DIACC Operating Procedures](#), a Final Recommendation is a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document was developed by DIACC's [Trust Framework Expert Committee](#) with input from the public gathered and processed through an open peer review process. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the [Pan-Canadian Trust Framework Work Programme](#). Changes to this document that may affect certification and Trustmark status will be defined in the Pan-Canadian Trust Framework Assessment component.

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the [DIACC Controlling Policies](#).

IPR: [DIACC-Intellectual Property Rights V1.0 PDF](#) | © 2020

Table of Contents

- 1 Introduction to the PCTF Verified Organization Conformance Profile 3
 - 1.1 About PCTF Conformance Criteria 3
- 2 Verified Organization Conventions 3
 - 2.1 Conformance Criteria Keywords 4
- 3 Verified Organization Conformance Criteria 4
- 4 Revision History 20

1 Introduction to the PCTF Verified Organization Conformance Profile

This document specifies the Conformance Criteria of the PCTF Verified Organization Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the PCTF, please see the PCTF Model Overview. The PCTF Model Overview provides the PCTF's goals and objectives, a high-level model outline of the PCTF, and contextual information.

Each PCTF component is made up of two documents:

1. **Overview** – Introduces the subject matter of the component. The overview provides information essential to understanding the Conformance Criteria of the component. This includes definitions of key terms, concepts, and the Trusted Processes that are part of the component.
2. **Conformance profile** – Specifies the Conformance Criteria used to standardize and assess the integrity of the Trusted Processes that are part of the component.

1.1 About PCTF Conformance Criteria

The PCTF promotes trust through a set of auditable business and technical requirements for various processes.

A process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition – an output on which other processes often depend. Conformance Criteria are the requirements and specifications that comprise a standard for these processes. They can be used to assess the integrity of a process. In the PCTF context, a process is designated a Trusted Process when it is audited and certified as conforming to Conformance Criteria defined in a PCTF conformance profile.

The integrity of a process is paramount because many Participants—across jurisdictional, Organizational, and sectoral boundaries and over the short-term and long-term—rely on the output of that process. Conformance criteria are therefore central to the trust framework because they specify the requirements that ensure process integrity.

Note

- PCTF Conformance Criteria do not replace or supersede existing laws and regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.

2 Verified Organization Conventions

Each PCTF component includes conventions that ensure consistent use and interpretation of terms and concepts appearing in the component. **The PCTF Verified Organization Component Overview** provides conventions for this component. These conventions include definitions and descriptions of the following items that are referred to in this conformance profile:

- Key terms and concepts
- Abbreviation and acronyms
- Roles
- Levels of Assurance
- Trusted Processes and associated conditions
- Event Types – Several criteria in this profile refer to "Event Type or business activity". For a complete listing of these Event Types see Appendix A of the overview document.

Note

- Conventions may vary between PCTF components. Readers are encouraged to review the conventions for each PCTF component they are reading.
- Defined Terms – For purposes of this conformance profile, terms and definitions listed in both the PCTF Verified Organization Component Overview and the PCTF Glossary apply. Key terms and concepts described and defined in this section, or the PCTF Verified Organization Component Overview, or the PCTF Glossary are capitalized throughout this document.
- Hypertext Links – Hypertext links may be embedded in electronic versions of this document. All links were accessible at time of writing.

2.1 Conformance Criteria Keywords

Throughout this document the following terms indicate the precedence and/or general rigidity of the conformance criteria and are to be interpreted as noted below.

- **MUST** means that the requirement is absolute as part of the conformance criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the conformance criteria.
- **SHOULD** means that while there may exist valid reasons in particular circumstances to ignore the requirement, the full implications must be understood and carefully weighed before choosing to not adhere to the conformance criteria or choosing a different option as specified by the conformance criteria.
- **SHOULD NOT** means that a valid exception reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing to not conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Note

- The above listed keywords appear in **bold** typeface and ALL CAPS throughout this conformance profile.

3 Verified Organization Conformance Criteria

The following sections define Conformance Criteria that are essential requirements for the Trusted Processes of Verified Organization Component. The Verified Organization Trusted Process are:

1. Organizational Identity Establishment (Foundational and Contextual)
2. Organizational Identity Issuance (Foundational and Contextual)
3. Organizational Identity Resolution
4. Organizational Identity Validation
5. Organizational Identity Verification
6. Organizational Identity Maintenance
7. Organizational Identity Linking

Conformance criteria are categorized by Trusted Process and profiled in terms of Levels of Assurance (LOA). Conformance Criteria are grouped by topic within each category. For ease of reference, a specific conformance criterion may be referred to by its category and reference number. Example: “BASE1” refers to “Baseline Conformance Criteria reference No. 1”.

Note

- Baseline Conformance Criteria are also included as part of this conformance profile.
- Conformance Criteria specified in other PCTF components of may also be applicable to Verified Organization Trusted Processes under certain circumstances.
- LOA 4 is out of scope for this version. Reference is retained as a placeholder for future development.

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
BASE	Baseline				
1	The Responsible Authority MUST provide to relying parties and other stakeholders a description of its program or services that includes the following information: <ol style="list-style-type: none"> 1. Nature of the program or service. 2. Intended recipients or clients the of program or service. 3. Jurisdictions covered by the program or service (if applicable). 	Y	Y		
2	The Responsible Authority SHOULD specify to Relying Parties and other parties the Organization(s) for which its services are provided.	Y	Y		
3	The Responsible Authority SHOULD specify to Relying Parties and other parties its mandate and authority as these relate to Organizational Verification.	Y			

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
4	The Responsible Authority MUST specify to Relying Parties and other parties its mandate and authority as these relate to Organizational Verification.		Y		
SERVICE PROVIDERS					
5	The Responsible Authority MUST be a juridical Entity (private or public sector) (e.g., government department, public sector agency, corporation, association, etc.).	Y	Y		
6	A Responsible Authority MUST identify any Authorized Agents it employs to carry out a Verified Organization Trusted process.	Y	Y		
7	<p>If a Responsible Authority relies on Authorized Agents to carry out a Verified Organization Trusted Process, that Responsible Authority MUST:</p> <ol style="list-style-type: none"> 1. Ensure a written agreement concerning arrangements between the parties is in place. 2. Provide documentation attesting to the existence and general provisions of the written agreement for the arrangement in effect for review by Relying Parties and other parties. Contractual specifics need not be part of this disclosure. 3. Be able to provide evidence that its Authorized Agents meet all Conformance Criteria and LOAs specified in this conformance profile and applicable to the Responsible Authority on whose behalf it operates. 4. Ensure its Authorized Agent(s) make it known to Relying Parties and other parties that they provide services on the Responsible Authority's behalf. 	Y	Y		
PRIVACY AND SECURITY					
8	The Responsible Authority MUST adhere to the privacy risk management practices of the PCTF and any selected Conformance Profiles.	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
9	The Responsible Authority MUST ensure i) the integrity, ii) the confidentiality, and iii) the availability of its services by adhering to a set of information security guidelines and controls (e.g., Communications Security Establishment (CSEC) Information Technology Security Guidance 33 (ITSG-33)) that support these efforts.	Y	Y		
10	The Responsible Authority MUST ensure the integrity of the information in transit and during processing when Identity Information and additional information is presented in electronic form.	Y	Y		
OIDES	Organizational Identity Establishment				
FOUNDATIONAL IDENTITIES					
1	The Responsible Authority that creates the Foundational Identity Record MUST be a Public Sector Organization Registry.		Y		
2	The Responsible Authority SHOULD implement reasonable measures to confirm persons acting on behalf of the Organization as part of Foundational Identity Record creation are entitled to do so by i) authority given them by the Organization or ii) legal or regulatory authority.		Y		
3	The Responsible Authority MUST provide persons acting on behalf of the Organization as part of Foundational Identity Record creation with notice that any false or misleading statements may result in violation of terms or conditions.		Y		
4	The Responsible Authority MUST confirm persons acting on behalf of the Organization understand and agree with the notice (specified in OIDES3) that any false or misleading statements may result in violation of terms or conditions.		Y		
5	All transactions relating to the creation of a Foundational Identity Record MUST be confirmed with and referenceable to a relevant Event Type.		Y		
6	The Responsible Authority MUST identify the legal name of the Organization.		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
7	The Responsible Authority SHOULD identify the business name and/or operating name of the Organization and indicate the name by which an Organization is referred to in a its jurisdiction.		Y		
8	<p>Creation of a Foundational Identity Record MUST be confirmed with and referenceable to at least two of the following pieces of information:</p> <ol style="list-style-type: none"> 1. Date of creation in Canada 2. Organization Type (from relevant registry) <ol style="list-style-type: none"> 1. Association 2. Corporation 3. Trust 4. Sole Proprietorships 5. Partnerships 6. Co-Operatives 7. Credit Unions 8. Other 3. Event Type 4. Event date 		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
9	<p>The Responsible Authority MUST record the minimum Organizational Identity Information:</p> <ol style="list-style-type: none"> 1. Assigned Identifier that uniquely distinguishes an Organization 2. Legal name indicating the name by which an Organization is legally recognized or referred to 3. Event Type <ol style="list-style-type: none"> 1. Event date (if available, in whole or in part) <ol style="list-style-type: none"> 1. Event Year, Event Month, Event Day (if available) 2. Place of event <ol style="list-style-type: none"> 1. At least one of: Municipality Name, Province/Territory Code, Province/Territory Name <p>Note</p> <ul style="list-style-type: none"> • If the process being assessed confirms at least one of the above bulleted points and at least one of the sub-bulleted points, then it meets the criteria for a Level 2 Assurance 		Y		
10	<p>The Responsible Authority SHOULD collect and record additional information during creation of the Foundational Identity Record (e.g., Organization mailing and/or physical address, Organizational/business activity, owner contact information).</p> <p>If additional information is collected, the Responsible Authority MUST identify the reason for collecting the additional information.</p>		Y		
CONTEXTUAL IDENTITIES					

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
11	The Responsible Authority SHOULD implement reasonable measures to confirm persons acting on behalf of the Organization as part of Contextual Identity Record creation are entitled to do so by i) authority given them by the Organization or ii) legal or regulatory authority.	Y			
12	The Responsible Authority MUST implement reasonable measures to confirm persons acting on behalf of the Organization as part of Contextual Identity Record creation are entitled to do so by i) authority given them by the Organization or ii) legal or regulatory authority.		Y		
13	The Responsible Authority MUST provide persons acting on behalf of the Organization as part of Contextual Identity Record creation with notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
14	The Responsible Authority MUST confirm persons acting on behalf of the Organization understand and agree with the notice (specified in OIDES13) that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
15	The Responsible Authority MUST provide the ability for Authorized Personnel to create an Identity Record for the Organization unless the Identity Record is created through automated systems.	Y	Y		
16	The Responsible Authority MUST enforce access controls to ensure only Authorized Personnel can create a Contextual Identity Record for the Organization.	Y	Y		
17	All transactions relating to the creation of a Contextual Identity Record MUST be confirmed and reference a relevant Event Type or business activity of the Responsible Authority.	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
18	A minimum of one piece of Foundational Evidence of Organizational Identity Information SHOULD be used i) as a source of information and/or ii) to corroborate information provided by persons acting on behalf of the Organization in the creation of a Contextual Identity Record.	Y			
19	A minimum of one piece of Foundational Evidence of Organizational Identity MUST be used i) as a source of information and/or ii) to corroborate information provided by persons acting on behalf of the Organization in the creation of a Contextual Identity Record.		Y		
20	The Responsible Authority MUST identify the Legal name of the Organization.	Y	Y		
21	The Responsible Authority SHOULD identify the business name and/or operating name of the Organization and indicate the name by which an Organization is referred to in a its jurisdiction.	Y	Y		
22	The Responsible Authority SHOULD identify the Legal Status of the Organization.	Y			
23	The Responsible Authority MUST identify the Legal Status of the Organization.		Y		
24	The Responsible Authority MUST record the minimum Organizational Identity Information: <ol style="list-style-type: none"> 1. Assigned Identifier that uniquely distinguishes the Organization. 2. Legal name indicating the name by which an Organization is legally recognized or referred to. 	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
25	<p>The Responsible Authority MAY collect and record additional information during creation of a Contextual Identity Record (e.g., Organization mailing and/or physical address, Organizational/business activity, owner contact information).</p> <p>If additional information is collected, the Responsible Authority MUST identify the reason for collecting the additional information.</p>	Y			
26	<p>The Responsible Authority SHOULD collect and record additional information during creation of a Contextual Identity Record (e.g., Organization mailing and/or physical address, Organizational/business activity, owner contact information).</p> <p>If additional information is collected, the Responsible Authority MUST identify the reason for collecting the additional information.</p>		Y		
OIDIS	Organizational Identity Issuance				
FOUNDATIONAL IDENTITIES					
1	The Responsible Authority that issues the Foundational Evidence of Organizational Identity Information MUST be a Public Sector Organization Registry.		Y		
2	The issued Foundational Evidence of Organizational Identity Information MUST relate to the registration of an Event Type or business activity applicable to the Organization - OR - indicate the status of the Organization's existence.		Y		
3	The issued Foundational Evidence of Organizational Identity Information MUST be consistent with information held in the Foundational Identity Record.		Y		
4	The issued Foundational Evidence of Organizational Identity Information MUST identify the Responsible Authority that issued the evidence.		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
5	The Responsible Authority issuing the Foundational Evidence of Organizational Identity MUST take reasonable measures to ensure the evidence is issued to the rightful recipient.		Y		
CONTEXTUAL IDENTITIES					
6	The issued Contextual Evidence of Organizational Identity Information MUST be consistent with information held in the Contextual Identity Record.	Y	Y		
7	The issued Contextual Evidence of Organizational Identity Information MUST identify the Responsible Authority that issued the evidence.	Y	Y		
8	The Responsible Authority MUST include the Level of Assurance of the Organization's identity when the Contextual Evidence of Organizational Identity was issued. The Responsible Party only needs to provide this information if and when requested by a Relying Party.	Y	Y		
9	The Responsible Authority issuing the Contextual Evidence of Organizational Identity MUST take reasonable measures to ensure the evidence is issued to the rightful recipient.	Y	Y		
OIDRS	Organizational Identity Resolution				
1	The Responsible Authority MUST ensure that the Foundational Identity Record or Contextual Identity Record uniquely resolves to only one Organization within a specified population or jurisdiction (including, if and where applicable, legal name, date of creation, address, identification number/name).	Y	Y		
OIDVA	Organizational Identity Validation				
1	Persons acting on behalf of the Organization MUST be able to provide proof of their identity.	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
2	<p>The Organization Verifier MUST ensure the information required to validate the Organization's Identity can be:</p> <ol style="list-style-type: none"> 1. Presented by persons acting on behalf of the Organization; or 2. Obtained from sources of Foundational Evidence of Organizational Identity or Contextual Evidence of Organizational Identity. 	Y	Y		
3	<p>The Organization Verifier MAY request Identity Information that indicates the existence/compliance through a status certificate issued by a Public Sector Organization Registry (e.g., Certificate of Compliance, Certificate of Existence).</p>	Y	Y		
4	<p>In cases where Identity Information and additional information is presented in the form of physical documents which are not verifiable electronically (i.e., cryptographically), the Organization Verifier's validation processes MUST include document inspection tasks sufficiently rigorous to detect fraudulent documents.</p>	Y	Y		
5	<p>The Organization Verifier MAY accept self-assertion of Identity Information by persons acting on behalf of the Organization.</p>	Y			
6	<p>The Organization Verifier MAY accept self-assertion of additional information (e.g., addresses) by persons acting on behalf of the Organization.</p>	Y			
7	<p>The Organization Verifier SHOULD request/accept Foundational Evidence of Organizational Identity or Contextual Evidence of Organizational Identity.</p>	Y			
8	<p>The Organization Verifier MUST request/accept Foundational Evidence of Organizational Identity.</p>		Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
9	Contextual Evidence of Organizational Identity MUST be validated against an Identity Record (Foundational or Contextual). If Validation against an Identity Record (Foundational or Contextual) is not feasible, then the Contextual Evidence of Organizational Identity MUST be confirmed by a trained examiner.	Y	Y		
10	Foundational Evidence of Organizational Identity SHOULD be validated against a Foundational Identity Record.	Y			
11	Foundational Evidence of Organizational Identity MUST be validated against a Foundational Identity Record. If Validation against a Foundational Identity Record is not feasible, then the Foundational Evidence of Organizational Identity MUST be confirmed by a trained examiner.		Y		
12	Contextual Evidence of Organizational Identity SHOULD be confirmed as originating from the Responsible Authority.	Y	Y		
13	Foundational Evidence of Organizational Identity SHOULD be confirmed as originating from the Responsible Authority.	Y			
14	Foundational Evidence of Organizational Identity MUST be confirmed as originating from the Responsible Authority.		Y		
15	The Organization Verifier MUST be able to validate that the Identity Information and additional information corresponds to a specific Organization within a given population.	Y	Y		
16	Identity Information MUST acceptably match assertion(s) provided by persons acting on behalf of the Organization and all instances of (foundational and/or contextual) evidence of identity presented by persons acting on behalf of the Organization.	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
17	<p>If identity Information in Validation sources does not exactly match i) assertion(s) provided by persons acting on behalf of the Organization and ii) all instances of (foundational and/or contextual) evidence of identity presented by persons acting on behalf of the Organization, the Organization Verifier MUST indicate the level of error in the information to the Relying Party.</p> <p>LOA requirements should be considered when determining an acceptable level of error. For example, a higher LOA would tolerate minimal error.</p>	Y	Y		
18	The Organization Verifier SHOULD provide a validity period for Validation results to the Relying Party.	Y			
19	The Organization Verifier MUST provide a validity period for Validation results to the Relying Party.		Y		
OIDVE	Organizational Identity Verification				
1	The Responsible Authority SHOULD undertake the Verification steps it deems necessary.	Y			
2	The Responsible Authority MUST undertake the Verification steps it deems necessary.		Y		
3	The Organization Verifier MAY employ an out-of-band confirmation as an additional method to ensure a person acting on behalf of the Organization relates to the Organization whose identity is being verified.	Y	Y		
4	The Organization Verifier SHOULD confirm that Foundational Evidence of Organizational Identity originates from the relevant Public Sector Organization Registry.	Y			
5	The Organization Verifier MUST confirm that Foundational Evidence of Organizational Identity originates from the relevant Public Sector Organization Registry.		Y		
OIDMA	Organizational Identity Maintenance				
FOUNDATIONAL IDENTITIES					

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
1	Any change to Organizational Identity Information MUST result in a timely update to the Foundational Identity Record of that Organization.		Y		
2	The Responsible Authority MUST provide persons acting on behalf of the Organization as part of Organizational Identity Maintenance with notice that any false or misleading statements may result in violation of terms or conditions.		Y		
3	The Responsible Authority MUST confirm persons acting on behalf of the Organization understand and agree with the notice (specified in OIDMA2) that any false or misleading statements may result in violation of terms or conditions.		Y		
4	The Responsible Authority MUST implement reasonable measures to confirm persons acting on behalf of the Organization as part of Foundational Identity Record maintenance are entitled to do so by i) authority given them by the Organization or ii) legal or regulatory authority.		Y		
5	All transactions resulting in a change to a Foundational Identity Record MUST be confirmed with and referenceable to a relevant Event Type.		Y		
6	All transactions resulting in a change to a Foundational Identity Record MUST be confirmed by the relevant Public Sector Organizational Registry.		Y		
7	The Responsible Authority SHOULD provide subscribed or otherwise known Relying Parties notification that Foundational Evidence of Organizational Identity has been updated.		Y		
CONTEXTUAL IDENTITIES					
1	Any changes to Organizational Identity Information MUST result in a timely update to the Contextual Identity Record of that Organization.	Y	Y		
2	The Responsible Authority MUST provide persons acting on behalf of the Organization as part of Organizational Identity Maintenance with notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
3	The Responsible Authority MUST confirm persons acting on behalf of the Organization understand and agree with the notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
4	The Responsible Authority SHOULD implement reasonable measures to confirm persons acting on behalf of the Organization as part of Contextual Identity Record maintenance are entitled to do so by i) authority given them by the Organization or ii) legal or regulatory authority.	Y			
5	The Responsible Authority MUST implement reasonable measures to confirm persons acting on behalf of the Organization as part of Contextual Identity Record maintenance are entitled to do so by i) authority given them by the Organization or ii) legal or regulatory authority.		Y		
6	The Responsible Authority MAY provide the ability for Authorized Personnel to update a Contextual Identity Record for the Organization.	Y	Y		
7	The Responsible Authority SHOULD enforce access controls to ensure only Authorized Personnel can update a Contextual Identity Record for the Organization.	Y			
8	The Responsible Authority MUST enforce access controls to ensure only Authorized Personnel can update a Contextual Identity Record for the Organization.		Y		
9	All transactions relating to the maintenance of a Contextual Identity Record MUST be confirmed and reference a relevant Event Type or business activity of the Responsible Authority.	Y	Y		
10	The Responsible Authority MUST ensure the information required to update the Organization's Contextual Identity Record can be presented by persons acting on behalf of the Organization.	Y	Y		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
11	The Responsible Authority SHOULD ensure the information required to update the Organization's Contextual Identity Record can be obtained from sources of Foundational Evidence of Organizational Identity or Contextual Evidence of Organizational Identity.	Y	Y		
12	The Responsible Authority SHOULD provide subscribed or otherwise known Relying Parties notification that Contextual Evidence of Organizational Identity has been updated.	Y	Y		
OIDLI	Organizational Identity Linking				
1	The Responsible Authority SHOULD perform an Identity Verification process to ensure that the assigned identifiers reference the same Organization before creating a link.	Y			
2	The Responsible Authority MUST perform an Identity Verification process to ensure that the assigned identifiers reference the same Organization before creating a link.		Y		
3	Where applicable (e.g., extra-provincial and/or extra-country establishment) the Responsible Authority MUST specify the Organization's linkages in multiple jurisdictions. This can be achieved through an acknowledgement of a review transaction of the relevant documents.		Y		

Table 1. PCTF Verified Organization Component Conformance Criteria

4 Revision History

Version	Date of Issue	Author(s)	Description
0.01	2019-11-18	PCTF Editing Team	Initial draft for review
0.02	2019-12-20	PCTF Editing Team	Update per initial review comments
1.0	2020-02-05	TFEC/PCTF Editing Team	Approved as Draft Recommendation V1.0. Component is now in the Draft Recommendation stage
1.1	2020-04-20	PCTF Editing Team	Updates from public review of the Draft Recommendation V1.0.
1.0	2020-09-16	TFEC/PCTF Editing Team	Approved as Final Recommendation V1.0