



# PCTF Verified Organization Conformance Profile Draft Recommendation V1.0

This Draft Recommendation has been developed by the [Digital ID & Authentication Council of Canada](#) (DIACC) Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. Comments submitted by the public are subject to the [DIACC Contributor Agreement](#).

DIACC expects to modify and improve this Draft Recommendation based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of truly Pan-Canadian input. Comments made during the review will be considered for incorporation to the next draft. DIACC will prepare a disposition of comments to provide transparency with regard to how each comment was handled.

Forthcoming PCTF releases will expand, clarify, and refine the content of this document.

---

## Contents

1. [Introduction to the PCTF Verified Organization Conformance Profile](#)
  - 1.1. [About PCTF Conformance Criteria](#)
2. [Verified Organization Conventions](#)
  - 2.1. [Conformance Criteria Keywords](#)
3. [Verified Organization Conformance Criteria](#)

## 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 Pan-Canadian 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

- 36 includes definitions of key terms, concepts, and the Trusted Processes that are part of  
37 the component.
- 38 2. Conformance profile – Specifies the Conformance Criteria used to standardize and  
39 assess the integrity of the Trusted Processes that are part of the component.

## 40 1.1 About PCTF Conformance Criteria

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

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

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

53 Note

- 54 • PCTF Conformance Criteria are intended to complement existing legislation and  
55 regulations. Participants in the Digital Identity Ecosystem are expected meet the  
56 legislative and regulatory requirements applicable in their jurisdictions.

## 57 2 Verified Organization Conventions

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

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

69 Note

- 70 • Conventions may vary between PCTF components. Readers are encouraged to review  
71 the conventions for each PCTF component they are reading.

- 72 • Defined Terms – For purposes of this conformance profile, terms and definitions listed in  
73 both the PCTF Verified Organization Component Overview and the PCTF Glossary  
74 apply. Key terms and concepts described and defined in this section, or the PCTF  
75 Verified Organization Component Overview, or the PCTF Glossary are capitalized  
76 throughout this document.  
77 • Hypertext Links – Hypertext links may be embedded in electronic versions of this  
78 document. All links were accessible at time of writing.

## 79 2.1 Conformance Criteria Keywords

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

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

94 Note

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

## 97 3 Verified Organization Conformance 98 Criteria

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

- 102 1. Organizational Identity Establishment (Foundational and Contextual)
- 103 2. Organizational Identity Issuance (Foundational and Contextual)
- 104 3. Organizational Identity Resolution
- 105 4. Organizational Identity Validation
- 106 5. Organizational Identity Verification
- 107 6. Organizational Identity Maintenance
- 108 7. Organizational Identity Linking

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

113 Note

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

119

Reference	Conformance Criteria	Level of Assurance (LOA)				
		LOA 1	LOA 2	LOA 3	LOA 4	
120	<b>BASE</b>	<b>Baseline</b>				
121	1	The Responsible Authority <b>MUST</b> meet all legal and regulatory requirements applicable to the Verified Organization Trusted Process it performs.	Y	Y		
122	2	The Responsible Authority <b>MUST</b> provide to relying parties and other stakeholders a description of its program or services that includes the following information:  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). 4. Approximate size, characteristics and composition of the Subject population.	Y	Y		
123	3	The Responsible Authority <b>SHOULD</b> specify to Relying Parties, assessors, and other parties the Organization(s) for which its services are provided.	Y	Y		
124	4	The Responsible Authority <b>SHOULD</b> specify to Relying Parties, assessors, and other parties its mandate and authority as these relate to Organizational Verification.	Y			

	Reference	Conformance Criteria	Level of Assurance (LOA)			
125	5	The Responsible Authority <b>MUST</b> specify to Relying Parties, assessors, and other parties its mandate and authority as these relate to Organizational Verification.		Y		
126	<b>SERVICE PROVIDERS</b>					
127	6	The Responsible Authority <b>MUST</b> be a registered public or private Entity (e.g., government department, public sector agency, corporation, association, etc.).	Y	Y		
128	7	A Responsible Authority <b>MAY</b> rely on one or more Authorized Agents to carry out a Verified Organization Trusted Process.	Y	Y		

129

Reference	Conformance Criteria	Level of Assurance (LOA)			
8	<p>If a Responsible Authority relies on Authorized Agents to carry out a Verified Organization Trusted Process, that Responsible Authority <b>MUST</b>:</p> <ol style="list-style-type: none"> <li>1. Ensure a written agreement concerning arrangements between the parties is in place.</li> <li>2. Provide for review by Relying Parties, assessors, and other parties documentation attesting to the existence and general provisions of the written agreement for the arrangement in effect. Contractual specifics need not be part of this disclosure.</li> <li>3. Ensure its Authorized Agent(s) meet or exceed all Conformance Criteria and LOAs specified in this conformance profile applicable to the Responsible Authority on whose behalf it operates.</li> <li>4. Be able to provide evidence that all Authorized Agents comply with the Conformance Criteria specified herein to the necessary LOA.</li> <li>5. Ensure its Authorized Agent(s) make it known to Relying Parties, assessors, and other parties that they provide services on the Responsible Authority's behalf.</li> </ol>	Y	Y		
130	<b>PRIVACY AND SECURITY</b>				
131	9	The Responsible Authority <b>SHOULD</b> adhere to the privacy risk management practices of the PCTF and any selected Conformance Profiles.			
132	10	The Responsible Authority <b>MUST</b> adhere to the privacy risk management practices of the PCTF and any selected Conformance Profiles.			

Reference	Conformance Criteria	Level of Assurance (LOA)				
133	11 The Responsible Authority <b>MUST</b> 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			
134	12 In cases where Identity and additional information is presented in electronic form (including API-based and digital certificate-based) appropriate processes <b>MUST</b> be employed to ensure the integrity of the information in transit and during processing.	Y	Y			
135	<b>OIDES</b>	<b>Organizational Identity Establishment</b>	<b>LOA 1</b>	<b>LOA 2</b>	<b>LOA 3</b>	<b>LOA 4</b>
136	<b>FOUNDATIONAL IDENTITIES</b>					
137	1 The Responsible Authority that creates the Foundational Identity Record <b>MUST</b> be a Public Sector Organization Registrar.		Y			
138	2 The Responsible Authority <b>MUST</b> implement reasonable measures to confirm persons acting on behalf of the subject as part of Foundational Identity Record creation are entitled to do so by i) authority given them by the Subject or ii) legal or regulatory authority.		Y			
139	3 The Responsible Authority <b>MUST</b> provide persons acting on behalf of the Subject as part of Foundational Identity Record creation with written notice that any false or misleading statements may result in violation of terms or conditions.		Y			
140	4 The Responsible Authority <b>MUST</b> confirm persons acting on behalf of the Subject understand and agree with the notice (specified in OIDES3) that any false or misleading statements may result in violation of terms or conditions.		Y			

	Reference	Conformance Criteria	Level of Assurance (LOA)			
141	5	All transactions relating to the creation of a Foundational Identity Record <b>MUST</b> be confirmed with and referenceable to a relevant Event Type.		Y		
142	6	The Responsible Authority <b>MUST</b> identify the legal name of the Organization.		Y		
143	7	The Responsible Authority <b>SHOULD</b> identify the business name and/or operating name indicating the name by which an Organization is referred to in a jurisdiction.		Y		
144	8	<p>Creation of a Foundational Identity Record <b>MUST</b> be confirmed with and referenceable to at least two of the following pieces of information:</p> <ol style="list-style-type: none"> <li>1. Date of creation in Canada</li> <li>2. Organization Type (from relevant registrar) <ol style="list-style-type: none"> <li>a. Association</li> <li>b. Corporation</li> <li>c. Trust</li> <li>d. Sole Proprietorships</li> <li>e. Partnerships</li> <li>f. Co-Operatives</li> <li>g. Credit Unions</li> <li>h. Other</li> </ol> </li> <li>3. Event Type</li> <li>4. Confirmation of event date</li> </ol>		Y		



Reference	Conformance Criteria	Level of Assurance (LOA)			
145	<p>The Responsible Authority <b>MUST</b> record the minimum Organizational Identity Information:</p> <ol style="list-style-type: none"> <li>1. Assigned Identifier that uniquely distinguishes an Organization</li> <li>2. Legal name indicating the name by which an Organization is legally recognized or referred to</li> <li>3. Event Type               <ol style="list-style-type: none"> <li>a. Event date (if available, in whole or in part)                   <ol style="list-style-type: none"> <li>i. Event Year, Event Month, Event Day (if available)</li> </ol> </li> <li>b. Place of event                   <ol style="list-style-type: none"> <li>i. At least one of: Municipality Name, Province/Territory Code, Province/Territory Name</li> </ol> </li> </ol> </li> </ol> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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</li> </ul>		Y		
146	<p>The Responsible Authority <b>SHOULD</b> collect and record additional information during creation of the Foundational Identity Record (e.g., Mailing and/or physical address, Organizational/business activity, owner information).</p>		Y		
147	<b>CONTEXTUAL IDENTITIES</b>				
148	<p>The Responsible Authority <b>SHOULD</b> implement reasonable measures to confirm persons acting on behalf of the subject as part of Contextual Identity Record creation are entitled to do so by</p> <ol style="list-style-type: none"> <li>i) authority given them by the Subject or</li> <li>ii) legal or regulatory authority.</li> </ol>	Y			

	Reference	Conformance Criteria	Level of Assurance (LOA)			
149	12	The Responsible Authority <b>MUST</b> implement reasonable measures to confirm persons acting on behalf of the subject as part of Contextual Identity Record creation are entitled to do so by i) authority given them by the Subject or ii) legal or regulatory authority.		Y		
150	13	The Responsible Authority <b>MUST</b> provide persons acting on behalf of the Subject as part of Contextual Identity Record creation with written notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
151	14	The Responsible Authority <b>MUST</b> confirm persons acting on behalf of the Subject 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		
152	15	The Responsible Authority <b>MUST</b> 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		
153	16	The Responsible Authority <b>MUST</b> provide Authorized Personnel that can create Contextual Identity Records with written notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
154	17	The Responsible Authority <b>SHOULD</b> enforce access controls to ensure only Authorized Personnel can create a Contextual Identity Record for the Organization.	Y			
155	18	The Responsible Authority <b>MUST</b> enforce access controls to ensure only Authorized Personnel can create a Contextual Identity Record for the Organization.		Y		

	Reference	Conformance Criteria	Level of Assurance (LOA)			
156	19	All transactions relating to the creation of an Identity Record <b>SHOULD</b> be confirmed and reference a relevant Event Type or business activity of the Responsible Authority.	Y			
157	20	All transactions relating to the creation of a Contextual Identity Record <b>MUST</b> be confirmed and reference a relevant Event Type or business activity of the Responsible Authority.		Y		
158	21	All transactions relating to the creation of a Contextual Identity Record <b>SHOULD</b> be confirmed with and referenceable to a relevant Event Type.	Y			
159	22	All transactions relating to the creation of a Contextual Identity Record <b>MUST</b> be confirmed with and referenceable to a relevant Event Type or business activity.		Y		
160	23	A minimum of one piece of Foundational Evidence of Organizational Identity <b>SHOULD</b> be used i) as a source of information and/or ii) to corroborate information provided by persons acting on behalf of the Subject in the creation of a Contextual Identity Record.	Y			
161	24	A minimum of one piece of Foundational Evidence of Organizational Identity <b>MUST</b> be used i) as a source of information and/or ii) to corroborate information provided by persons acting on behalf of the Subject in the creation of a Contextual Identity Record.		Y		
162	25	The Responsible Authority <b>MUST</b> identify the Legal name of the Organization.	Y	Y		
163	26	The Responsible Authority <b>SHOULD</b> identify the business name and/or operating name indicating the name by which an Organization is referred to in a jurisdiction.	Y	Y		
164	27	The Responsible Authority <b>SHOULD</b> identify the Legal Status of the Organization.	Y			

	Reference	Conformance Criteria	Level of Assurance (LOA)			
165	28	The Responsible Authority <b>MUST</b> identify the Legal Status of the Organization.		Y		
166	29	The Responsible Authority <b>MUST</b> record the minimum Organizational Identity Information:  1. Assigned Identifier that uniquely distinguishes the Subject. 2. Legal name indicating the name by which an Organization is legally recognized or referred to.	Y	Y		
167	30	The Responsible Authority <b>MAY</b> collect and record additional information during creation of a Contextual Identity Record (e.g., Mailing and/or physical address, Organizational/business activity, owner information).	Y			
168	31	The Responsible Authority <b>SHOULD</b> collect and record additional information during creation of a Contextual Identity Record (e.g., Mailing and/or physical address, Organizational/business activity, owner information).		Y		
169	<b>OIDIS</b>	<b>Organizational Identity Issuance</b>	<b>LOA 1</b>	<b>LOA 2</b>	<b>LOA 3</b>	<b>LOA 4</b>
170	<b>FOUNDATIONAL IDENTITIES</b>					
171	1	The Responsible Authority that issues the Foundational Evidence of Organizational Identity Information <b>MUST</b> be a Public Sector Organization Registrar.		Y		
172	2	The issued Foundational Evidence of Organizational Identity Information <b>MUST</b> relate to the registration of an Event Type or business activity applicable to the Subject -or- indicate the status of the Subject's existence.		Y		
173	3	The issued Foundational Evidence of Organizational Identity information <b>MUST</b> be consistent with information held in the Foundational Identity Record.		Y		

	Reference	Conformance Criteria	Level of Assurance (LOA)			
174	4	The issued Foundational Evidence of Organizational Identity information <b>MUST</b> identify the Responsible Authority that issued the evidence.		Y		
175	5	The Responsible Authority issuing the Foundational Evidence of Organizational Identity <b>MUST</b> take reasonable measures to ensure the evidence is issued to the rightful recipient.		Y		
176	<b>CONTEXTUAL IDENTITIES</b>					
177	6	The issued Contextual Evidence of Organizational Identity information <b>MUST</b> be consistent with information held in the Contextual Identity Record.	Y	Y		
178	7	The issued Contextual Evidence of Organizational Identity information <b>MUST</b> identify the Responsible Authority that issued the evidence.	Y	Y		
179	8	The Responsible Authority <b>MUST</b> include the Level of Assurance of the Subject's identity when the Contextual Evidence of Organizational Identity. The Responsible Party only needs to provide this information if and when requested by a Relying Party.	Y	Y		
180	9	The Responsible Authority issuing the Foundational Evidence of Organizational Identity <b>MUST</b> take reasonable measures to ensure the evidence is issued to the rightful recipient.	Y	Y		
181	<b>OIDRS</b>	<b>Organizational Identity Resolution</b>	<b>LOA 1</b>	<b>LOA 2</b>	<b>LOA 3</b>	<b>LOA 4</b>
182	1	The Responsible Authority <b>MUST</b> ensure that the Foundational Identity Record or Contextual Identity Record uniquely resolves to only one Subject within a specified population or jurisdiction of interest (including, if and where applicable, legal name, date of creation, address, identification number/name).	Y	Y		
183	<b>OIDVA</b>	<b>Organizational Identity Validation</b>	<b>LOA 1</b>	<b>LOA 2</b>	<b>LOA 3</b>	<b>LOA 4</b>

	Reference	Conformance Criteria	Level of Assurance (LOA)			
184	1	Persons acting on behalf of the Subject <b>MUST</b> be able to claim which individual they are within a population.	Y	Y		
185	2	The Organization Verifier <b>MUST</b> ensure the information required to validate the Subject's Identity can be: <ul style="list-style-type: none"> <li>1. Presented by persons acting on behalf of the Subject; or</li> <li>2. Obtained from sources of Foundational Evidence of Organizational Identity or Contextual Evidence of Organizational Identity.</li> </ul>	Y	Y		
186	3	The Organization Verifier <b>MAY</b> request Identity Information that <b>MUST</b> indicate existence/compliance through a status certificate issued by a federal or provincial/territorial Public Sector Organization Registrar (e.g., Certificate of Compliance, Certificate of Existence).	Y	Y		
187	4	The Organization Verifier <b>MUST</b> ensure that the information sources and technology used to perform the Validation process are understood by all actors and is fit for purpose.	Y	Y		
188	5	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 <b>MUST</b> include document inspection tasks sufficiently rigorous to detect fraudulent documents.	Y	Y		
189	6	The Organization Verifier <b>MAY</b> accept self-assertion of Identity Information.	Y			
190	7	The Organization Verifier <b>MAY</b> accept self-assertion of additional information (e.g., addresses).	Y			
191	8	The Organization Verifier <b>SHOULD</b> request/accept Foundational Evidence of Organizational Identity or Contextual Evidence of Organizational Identity.	Y			

	Reference	Conformance Criteria	Level of Assurance (LOA)			
192	9	The Organization Verifier <b>MUST</b> request/accept Foundational Evidence of Organizational Identity.		Y		
193	10	Contextual Evidence of Organizational Identity <b>MUST</b> 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 <b>MUST</b> be confirmed by a trained examiner.	Y	Y		
194	11	Foundational Evidence of Organizational Identity <b>SHOULD</b> be validated against a Foundational Identity Record.	Y			
195	12	Foundational Evidence of Organizational Identity <b>MUST</b> be validated against a Foundational Identity Record.  If Validation against a Foundational Identity Record is not feasible, then the Foundational Evidence of Organizational Identity <b>MUST</b> be confirmed by a trained examiner.		Y		
196	13	Contextual Evidence of Organizational Identity <b>SHOULD</b> be confirmed as originating from the Responsible Authority.	Y	Y		
197	14	Foundational Evidence of Organizational Identity <b>SHOULD</b> be confirmed as originating from the Responsible Authority.	Y			
198	15	Foundational Evidence of Organizational Identity <b>MUST</b> be confirmed as originating from the Responsible Authority.		Y		
199	16	The Organization Verifier <b>MUST</b> be able to validate that the Identity and additional information corresponds to a specific Subject within the population.	Y	Y		

	Reference	Conformance Criteria	Level of Assurance (LOA)			
200	17	Identity Information in Validation sources <b>MUST</b> acceptably match information provided by the User and all instances of Foundational Evidence of Organizational Identity and/or Contextual Evidence of Organizational Identity presented by the User.	Y	Y		
201	18	If information in Validation sources does not exactly match information provided by the User and all instances of Foundational Evidence of Organizational Identity and/or Contextual Evidence of Organizational Identity presented by the User the Organization Verifier <b>MUST</b> indicate the level of mismatch (i.e., error) to the Relying Party.	Y	Y		
202	19	The Organization Verifier <b>SHOULD</b> provide a defined validity period for Validation results to the Relying Party.	Y			
203	20	The Organization Verifier <b>MUST</b> provide a defined validity period for Validation results to the Relying Party.		Y		
204	<b>OIDVE</b>	<b>Organizational Identity Verification</b>	<b>LOA 1</b>	<b>LOA 2</b>	<b>LOA 3</b>	<b>LOA 4</b>
205	1	The Responsible Authority <b>MAY</b> undertake the Verification steps it deems necessary.	Y			
206	2	The Organization Verifier <b>MAY</b> employ an out-of-band confirmation as an additional method to ensure the claimant relates to the Organization making the claim.	Y	Y		
207	3	The Organization Verifier <b>SHOULD</b> confirm that Foundational Evidence of Organizational Identity originates from the relevant Public Sector Organization Registrar.	Y	Y		
208	<b>OIDMA</b>	<b>Organizational Identity Maintenance</b>	<b>LOA 1</b>	<b>LOA 2</b>	<b>LOA 3</b>	<b>LOA 4</b>
209	<b>FOUNDATIONAL IDENTITIES</b>					
210	1	Any change to Organizational Identity Information <b>MUST</b> result in a timely update to the Foundational Identity Record of that Organization.		Y		



	Reference	Conformance Criteria	Level of Assurance (LOA)			
211	2	The Responsible Authority <b>MUST</b> provide persons acting on behalf of the Subject as part of Organizational Identity Maintenance with written notice that any false or misleading statements may result in violation of terms or conditions.		Y		
212	3	The Responsible Authority <b>MUST</b> confirm persons acting on behalf of the Subject understand and agree with the notice (specified in OIDMA2) that any false or misleading statements may result in violation of terms or conditions.		Y		
213	4	The Responsible Authority <b>MUST</b> implement reasonable measures to confirm persons acting on behalf of the subject as part of Foundational Identity Record maintenance are entitled to do so by i) authority given them by the Subject or ii) legal or regulatory authority.		Y		
214	5	All transactions resulting in a change to a Foundational Identity Record <b>MUST</b> be confirmed with and referenceable to a relevant Event Type.		Y		
215	6	All transactions resulting in a change to a Foundational Identity Record <b>MUST</b> be confirmed by the relevant Public Sector Organizational Registrar.		Y		
216	7	The Responsible Authority <b>SHOULD</b> provide Relying Parties notification that Foundational Evidence of Organizational Identity has been updated.		Y		
217	<b>CONTEXTUAL IDENTITIES</b>					
218	1	Any changes to Organizational Identity Information <b>SHOULD</b> result in a timely update to the Contextual Identity Record of that Organization.	Y			
219	2	Any change to Organizational Identity Information <b>MUST</b> result in a timely update to the Contextual Identity Record of that Organization.		Y		

	Reference	Conformance Criteria	Level of Assurance (LOA)			
220	3	The Responsible Authority <b>MUST</b> provide persons acting on behalf of the Subject as part of Organizational Identity Maintenance with written notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
221	4	The Responsible Authority <b>MUST</b> confirm persons acting on behalf of the Subject understand and agree with the notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
222	5	The Responsible Authority <b>SHOULD</b> implement reasonable measures to confirm persons acting on behalf of the subject as part of Contextual Identity Record maintenance are entitled to do so by i) authority given them by the Subject or ii) legal or regulatory authority.	Y			
223	6	The Responsible Authority <b>MUST</b> implement reasonable measures to confirm persons acting on behalf of the subject as part of Contextual Identity Record maintenance are entitled to do so by i) authority given them by the Subject or ii) legal or regulatory authority.		Y		
224	7	The Responsible Authority <b>MAY</b> provide the ability for Authorized Personnel to update a Contextual Identity Record for the Organization.	Y	Y		
225	8	The Responsible Authority <b>MUST</b> provide Authorized Personnel that can update Contextual Identity Records with written notice that any false or misleading statements may result in violation of terms or conditions.	Y	Y		
226	9	The Responsible Authority <b>SHOULD</b> enforce access controls to ensure only Authorized Personnel can update a Contextual Identity Record for the Organization.	Y			

	Reference	Conformance Criteria	Level of Assurance (LOA)			
227	10	The Responsible Authority <b>MUST</b> enforce access controls to ensure only Authorized Personnel can update a Contextual Identity Record for the Organization.		Y		
228	11	All transactions relating to the maintenance of a Contextual Identity Record <b>SHOULD</b> be confirmed and reference a relevant Event Type or business activity of the Responsible Authority.	Y			
229	12	All transactions relating to the maintenance of a Contextual Identity Record <b>MUST</b> be confirmed with and reference a relevant Event Type or business activity of the Responsible Authority.		Y		
230	13	All transactions relating to the maintenance of a Contextual Identity Record <b>SHOULD</b> be confirmed with and referenceable to a relevant Event Type or business activity of the Responsible Authority..	Y			
231	14	The Responsible Authority <b>MUST</b> ensure the information required to update the Subject's Contextual Identity Record can be presented by persons acting on behalf of the Subject.	Y	Y		
232	15	The Responsible Authority <b>SHOULD</b> ensure the information required to update the Subject's Contextual Identity Record can be obtained from sources of Foundational Evidence of Organizational Identity or Contextual Evidence of Organizational Identity.	Y	Y		
233	16	The Responsible Authority <b>SHOULD</b> provide Relying Parties notification that Contextual Evidence of Organizational Identity has been updated.	Y	Y		
234	<b>OIDLI</b>	<b>Organizational Identity Linking</b>	<b>LOA 1</b>	<b>LOA 2</b>	<b>LOA 3</b>	<b>LOA 4</b>

	Reference	Conformance Criteria	Level of Assurance (LOA)			
235	1	The Responsible Authority <b>SHOULD</b> perform an Identity Verification process to ensure that the assigned identifiers reference the same Subject before creating a link.	Y			
236	2	The Responsible Authority <b>MUST</b> perform an Identity Verification process to ensure that the assigned identifiers reference the same Organization before creating a link.		Y		
237	3	The Responsible Authority <b>SHOULD</b> perform an Identity Verification process to ensure that the assigned identifiers reference the same Subject and validate the Subject's Identity Information with a Public Sector Organization Registrar before creating a link.	Y			
238	4	The Responsible Authority <b>MUST</b> perform an Identity Verification process to ensure that the assigned identifiers reference the same Subject and validate the Subject's Identity Information with a Public Sector Organization Registrar before creating a link.		Y		
239	5	Where applicable (e.g., extra-provincial and/or extra-country establishment) the Responsible Authority <b>MUST</b> 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**