PCTF Verified Organization

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, Final Recommendations are 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.

Table of Contents

1. Introduction to the PCTF Verified Organization Component

Content herein concerns itself with the domain specific topic for this Pan-Canadian Trust Framework (PCTF) component. The overview section provides information related to and necessary for consistent interpretation of the included conformance criteria. For a general introduction to the PCTF, please see the PCTF Overview that describes the background, purpose, scope, principles, and objectives of the framework.

1.1 Overview

The ability to verify the Identity of individuals participating in an online transaction is necessary to create privacy, security, and trust. Without this ability, Users remain effectively anonymous and concerns about data breaches, legal and social liabilities, and financial loss persist. The range of transactions available under such conditions is limited in terms of the sensitivity, value, and use of personal information. For this reason, DIACC invests in consistent and auditable rules that support the creation and use digital identities for persons – and these are documented in the PCTF Verified Person Component.

However, the participants in many interactions are not always individual persons. Participants regularly include Organizations – the businesses, non-profit organizations, and other groups of people that routinely interact with individuals and each other (as customers, suppliers, service providers, etc.).

This PCTF component considers organizations, both incorporated and unincorporated, as separate and distinct from the people that make up the organization itself. This applies to large organizations (e.g., large multinational businesses with thousands of employees) and those made up of a single person (e.g., a sole proprietorship). The PCTF does, however, recognize that organizations cannot effectively act on their own; that they are dependent on human representatives. Processes and associated Conformance Criteria to identify the individuals representing an organization are the subject of the PCTF Verified Person component.

1.2 Purpose and Anticipated Benefits

The purpose of this PCTF component is to specify Trusted Processes and associated Conformance Criteria that establish an Organization exists, is real, unique, and identifiable. Once a process is certified as conforming to the associated Conformance Criteria it becomes a trusted process which then can be relied on by other Participants in a Digital Identity Ecosystem.

The PCTF Verified Organization component defines processes and specifies Conformance Criteria for:

1. Establishing and verifying the Identity of an Organization: This includes processes to ensure that an Organization has been properly verified as the expected participant in a

given interaction. An Organization that no longer exists as a legal entity may still have a digital identity with an attribute indicating its status.
2. Creating a trusted digital representation (i.e., a digital Identity) for an Organization. These include processes to establish and maintain a digital representation for a verified Organization.

Once the integrity of these processes is established and assessed through the standardized conformance criteria defined by this PCTF component, stakeholders benefit from business, operational, and technical conventions for the development of reliable, secure, and interoperable technical implementations that:

- Allow Organizations to exchange trustworthy information about themselves with external parties. A primary concern in digital environments is the prevalence of fake businesses setup for fraudulent purposes. For certain industries, confirmation of organization identity is part of know-your-customer requirements. In both cases, the ability to quickly and confidently digitally confirm an organization's identity and other key attributes i) reduces the risk of fraud and financial loss when establishing relationships with other organizations, and ii) reduces cost by eliminating time-consuming manual verification processes.
- Allow service providers, relying parties, etc. to trust that the organizational identity establishment and verification processes used by others meet their own requirements. This potentially reduces cost to relying parties by i) reducing reliance on self-asserted information about an organization, and ii) outsourcing validation, verification, and other identity management processes that are not a core capability of the relying party

1.3 Scope

This PCTF component focuses those Trusted Processes that establish the Identity of the Organizations and the ongoing management of associated digital Identities. This includes:

1. Organizational Identity Establishment
2. Organizational Identity Issuance
3. Organizational Identity Resolution
4. Organizational Identity Validation
5. Organizational Identity Verification
6. Organizational Identity Maintenance
7. Organizational Identity Linking

The scope of this PCTF component does not include:

1. International governments or Organizations as authoritative sources for Identity evidence to verify an Organization. They may be referenced indirectly to establish foundational or contextual sources of Identity.
2. Processes by which stakeholders validate that individuals representing Organizations have the authority to do so.
3. Ownership structure of an Organization and the relevant conditions and processes for granting accessing to services and systems (private or public sector).

1.4 Verified Organization Identity Domains

A key requirement of the PCTF Verified Organization Component is to ensure that an Organization exists. In Canada, creating Organizations and tracking their continued existence is the responsibility of public Organizations mandated by federal, provincial, and territorial governments to administer the laws that govern creation and maintenance of legal Entities. These public Organizations are provincial business registries and Corporations Canada.

Once the Organization legally exists, its relationships with additional public and private sector service providers typically result in the creation of further information (e.g., client identifiers for a credit monitoring agency and government tax account numbers) that can be used to identify the Organization.

Since information that can be used to verify the existence and Identity of an Organization originates with mandated government Organizations but is added to and extended by other Entities, this PCTF component defines two Identity domains to delineate responsibilities for establishing and providing evidence of an Organization's existence and Identity. These domains are:

1. Foundational
2. Contextual

Evidence that can be used to verify the existence and/or Identity of an Organization can originate in either domain:

1. **Foundational Evidence of Organizational Identity** – Information that is created, maintained, and issued to the Organization by a federal, provincial, or territorial business registry or similarly mandated public Organization. Issued when the Organization is first created, Foundational Evidence of Organizational Identity is used to establish and maintain core Organizational Identity (e.g. legal name, operating name, type of Organization) and status (e.g., as an active business or one that has been part of an amalgamation).
2. **Contextual Evidence of Organizational Identity** – Information that is created, maintained, and issued to the Organization by private or public sector Entities. Contextual Evidence of Organizational Identity is most often used for program administration or to facilitate service delivery. Contextual Evidence of Organizational Identity can also be used to link Organizational Identity Information across jurisdictions and services.

Table 1 lists examples of foundational and contextual evidence of Organizational Identity types.

Type	Organization Identity Information	Authoritative Sources and Documents	Issuers
Foundational Evidence of Organizational Identity	Legal name Status Type of Organization	Business registries Certificate of compliance and/or existence, articles of incorporation	Provincial business registrars and Corporations Canada
Contextual Evidence of Organizational Identity	BN9 and BN15 Legal Entity Identifier (LEI) DUNS number Client number	Unique numerical identifier	Private and public sector Organizations

Table 1. Examples of Foundational and Contextual Evidence of Organizational Identity.

1.5 Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Building on a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian Digital Identity Ecosystem.

Figure 1 is an illustration of the components of the draft Pan-Canadian Trust Framework.

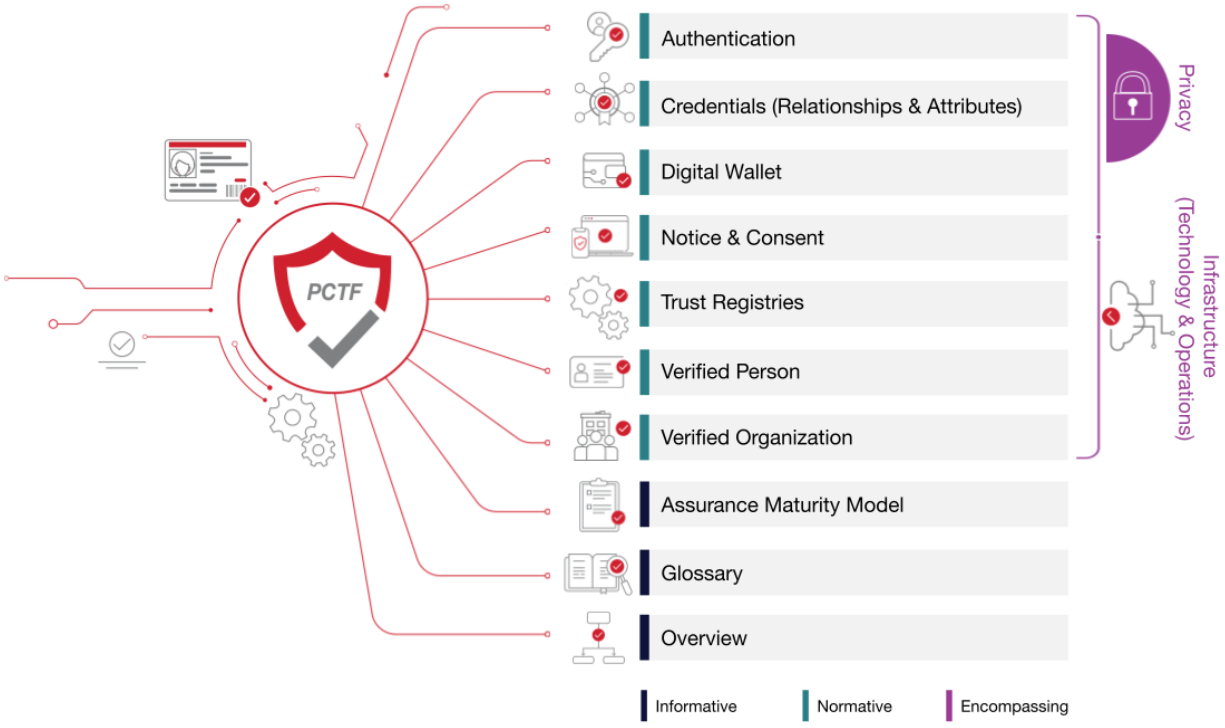

Figure 1. Components of the Pan-Canadian Trust Framework

2. Verified Organization Conventions

This section describes and defines key terms and concepts used in the PCTF Verified Organization Component. This information is provided to ensure consistent use and interpretation of terms appearing in this overview and the PCTF Verified Organization Conformance Profile.

Notes:

- Conventions may vary between PCTF components. Readers are encouraged to review the conventions for each PCTF component they are reading.
- Defined Terms – Key terms and concepts described and defined in this section, the section on Trusted Processes, and 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 Terms and Definitions

For purposes of this PCTF component, terms and definitions listed in the PCTF Glossary and the following terms and definitions apply.

Authorized Agent

Any Entity providing services related to Verified Organization on behalf of a Responsible Authority through a formal relationship.

Assigned Identifier

Letters, numbers, symbols, or a combination thereof that a Responsible Authority allocates to an Organization and which can be used to uniquely identify the Organization within a given context, use, or system.

Authorized Personnel

Staff of a Responsible Authority assigned to perform certain tasks. Typically, employees of or persons working under contract for the Responsible Authority.

Contextual Evidence of Organizational Identity

Information providing evidence of Organizational Identity is usually tied to program administration or service delivery activities. Created by private sector Entities and public sector Entities. Contextual Evidence of Organizational Identity may corroborate Foundational Evidence of Organizational Identity and may include information beyond Organizational Identity Information (e.g., mailing address). This information may be used to assist in linking Organizational Identity Information across jurisdictions and services. Examples include CRA BN registration document, municipal business permit, a DUNS number.

Contextual Identity Record

A record that provides Contextual Evidence of Organizational Identity.

Event Type

A happening in the life of an Organization that may trigger one or more Verified Organization Trusted Processes. Event types include a number of happenings that are specific to Public Sector Organization Registries. See Appendix A for a list of identified Event Types.

Foundational Evidence of Organizational Identity

Information providing evidence of Organizational Identity that is directly tied to a specific foundational event in the life of the Organization (e.g., registration, change of name, amalgamation). Created and issued exclusively by mandated public Organizations, specifically business registrars and Corporations Canada. Foundational Evidence of Organizational Identity establishes core Identity Information (e.g., Legal name, operating name, date of creation, and jurisdiction of creation). Examples include certificates of incorporation or records of business name registration.

Foundational Identity Record

A record that provides Foundational Evidence of Organizational Identity.

Legal Status

An indicator of an Organization's status as a legal Entity at a particular time.

Organization

An Entity that consists of a person or organized body of people with a particular purpose, and whose existence is established by legal statute. Such Organizations have legal standing under the law. Under this definition, Organizations include but are not limited to for-profit businesses, charities, associations, and public sector agencies. Excluded from this definition are informal groups such as certain social and athletic clubs (those that are not otherwise legally constituted).

Public Sector Organization Registry

A government department or registrar (regardless of formal organizational structure or status) operating under the authority of a Canadian federal, provincial, or territorial government and mandated to i) administer the laws and regulations that govern creation and maintenance of legal Entities, and ii) deliver associated programs and services.

Subject

In the context of Verified Organization, Subject always refers to an Organization.

2.2 Abbreviations

The following abbreviations and acronyms appear throughout this overview and the PCTF Verified Organization Conformance Profile.

- BN – Business Number (issued by Canada Revenue Agency)
- CRA – Canada Revenue Agency
- LOA – Level of Assurance
- LOAs – Levels of Assurance
- PCTF – Pan-Canadian Trust Framework

2.3 Roles

The following roles and role definitions are applicable in the scope and context of the PCTF Verified Organization Component. These roles help to isolate the different functions and responsibilities within the end-to-end Verified Organization Trusted Processes.

Notes:

- Depending on the use case, different Organizations may assume one or multiple roles.
- Role definitions do not imply or require any particular solution, architecture, or implementation or business model.

Organization Verifier

A private or public sector Entity or other autonomous legal Entity that provides one or more Organizational Identity Validation or Organizational Identity Verification Trusted processes.

Organization Verifier is defined separately from Responsible Authority to support a wider range of potential use cases and implementation scenarios where the Responsible Authority is not directly involved in the verification process (e.g., a private business is performing verification rather than a business registry)

Responsible Authority

A private or public sector Entity or other autonomous legal Entity that provides one or more Verified Organization Trusted Processes. A Responsible Authority may be a government department, government agency, business registry, private business, or other legal autonomous Entity.

Relying Party

An Organization or Person who consumes digital Identity Information created and managed by Participants to conduct digital transactions with Subjects.

2.4 Levels of Assurance

Levels of assurance (LOAs) are used in certain contexts, including this PCTF component, to indicate the robustness of the technology and processes employed to verify the identity of an Organization. The conformance criteria for Verified Organization are profiled in terms of Levels of Assurance for identity. A level of assurance reflects the relative stringency of the conformance criteria and is used to convey a relative degree of confidence which may be accepted for use by a relying party.

Table 2 below lists the Levels of Assurance defined in existing trust frameworks and are applied to the PCTF Verified Organization Conformance Criteria.

Level of Assurance	Qualification Description
Level 1 (LOA1)	• Little or no degree of confidence required • Satisfies Level 1 Conformance Criteria
Level 2 (LOA2)	• Some (reasonable) degree of confidence required • Satisfies Level 2 Conformance Criteria
Level 3 (LOA3)	• High degree of confidence required • Satisfies Level 3 Conformance Criteria
Level 4 (LOA4)	• Very high degree of confidence required • Satisfies Level 4 Conformance Criteria

Table 2. Levels of Assurance

Note: This version of the PCTF Verified Organization Component does not define Conformance Criteria for LOAs 3 or 4. However, the PCTF acknowledges the existence of both LOA3 and LOA4 and has included them as placeholders for future versions.

3. Trusted Processes

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.

In the PCTF context, a process that is designated a trusted process is assessed according to Conformance Criteria. The integrity of a trusted 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.

A single organization may not be responsible for carrying out all the Verified Organization trusted processes.

More information on trusted processes and conformance criteria is available on diacc.ca.

3.1 Verified Organization Trusted Processes

The PCTF Verified Organization Component defines seven Trusted Processes:

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

Note: It is not expected that all trusted processes and all associated conformance criteria will apply in all circumstances or use cases, nor that they will occur in the order presented above.

3.1.1 Organizational Identity Establishment

Organizational Identity Establishment is the process of creating an Organizational Identity Record (foundational or contextual). Other parties can rely on this record for subsequent program and service delivery.

In the case of a Foundational Identity Record, the resulting record will contain sufficient Identity Information to definitively distinguish a unique Organization in a specific jurisdiction defined by that jurisdiction's authoritative record creator (i.e., Responsible Authority). A Contextual Identity Record will contain Identity Information to definitively distinguish a unique Organization in a specific Subject population. The degree of uniqueness might not be satisfactory to parties other than the Responsible Authority.

Note: Because unregistered Organizations (i.e., those without legal standing) are out of scope for this PCTF component, Organizational Identity Establishment – Contextual is dependent on the creation of a Foundational Identity Record.

Organizational Identity Establishment – Foundational

Inputs	No Identity Record – No Identity Record (Foundational) of Organizational Identity Information exists.
Outputs	Identity Record – There exists an Identity Record (Foundational) of Organizational Identity Information.
Dependencies	Organizational Identity Resolution

Organizational Identity Establishment – Contextual

Inputs	No Identity Record – No Identity Record (Contextual) of Organizational Identity Information exists.
Outputs	Identity Record – There exists an Identity Record (Contextual) of Organizational Identity Information.
Dependencies	Organizational Identity Resolution Organizational Identity Issuance (Foundational)

3.1.2 Organizational Identity Issuance

Organizational Identity Issuance is the process of creating and providing to the Organization evidence of its Identity. Foundational Evidence of Organizational Identity is issued by a Public Sector Organization Registry. Contextual Evidence of Organizational Identity is issued by public Entity (which may include a Public Sector Organization Registry when not acting in an official registrar capacity) or a private sector Entity.

Organizational Identity Issuance – Foundational

Inputs	No evidence of organizational Identity – Foundational Evidence of Organizational Identity does not exist.
Outputs	Evidence of Organizational Identity – Foundational Evidence of Organizational Identity has been issued.
Dependencies	Organizational Identity Establishment (Foundational)

Organizational Identity Issuance – Contextual

Inputs	No evidence of organizational Identity – Contextual Evidence of Organizational Identity does not exist.
Outputs	Evidence of Organizational Identity – Contextual Evidence of Organizational Identity has been issued.
Dependencies	Organizational Identity Establishment (Contextual)

3.1.3 Organizational Identity Resolution

Organizational Identity Resolution is the process of establishing an Organization as unique within a population through the use of that Organization's Identity Information. With this process, each program or service specifies the set of Organizational identity attributes required to achieve Organizational identity resolution within its jurisdiction.

Inputs	Non-unique Identity Information – A set of identity information available to uniquely identify the Organization within a population (but not yet unique to a particular Organization).
Outputs	Unique Identity Information – A set of identity information unique to a particular Organization (i.e., the Identity Information resolves to one and only one Organization).
Dependencies	Organizational Identity Validation

3.1.4 Organizational Identity Validation

Organizational Identity Information Validation is the process of confirming the accuracy of identity information about an Organization against that established by a Responsible Authority. This process involves using Contextual or Foundational Evidence of Organizational Identity to determine a claimed Identity exists and is valid.

The intent of this Trusted Process is to give Relying Parties an established method for ensuring an Organization's Identity Information is accurate and reliable for their purposes.

Notes:

- "Identity Validation" is equivalent to the term "Identity Information Validation".
- This process does not ensure that the Organization is using its own Identity Information (this is Organization Identity Verification).

Inputs	Unconfirmed Identity Information – Organizational Identity Information has not been confirmed using an Identity Record (Foundational or Contextual).
Outputs	Confirmed Identity Information – Organizational Identity Information has been confirmed using an Identity Record (Foundational or Contextual).
Dependencies	Organizational Identity Establishment

3.1.5 Organizational Identity Verification

Organizational Identity Verification is the process of confirming that the presented Organizational Identity Information relates to the Organization making the presentation. Verification is a separate process from Organizational Identity Validation and may employ different methods and require the collection of Organizational information that is not related to Identity.

The intent of the Organizational Identity Verification process is to ensure a service provider or other party knows the Identity of the Organization with which it is interacting while preventing duplicitous use of Identity Information.

Note: Since an Organization's Identity Information will be presented by persons acting on behalf of the Organization, the Verification process may also need to verify that the person is associated with the Organization.

Inputs	Unverified Identity Information – Organizational Identity Information has not been confirmed as being presented by the Organization to which it relates.
Outputs	Verified Identity Information – Organizational Identity Information has been confirmed as being presented by the Organization to which it relates.
Dependencies	Organizational Identity Validation

3.1.6 Organizational Identity Maintenance

Organizational Identity Maintenance is the process of ensuring that identity information recorded about the Organization is as accurate, complete, and up-to-date as required. This process also includes Identity notification, which is the disclosure of Identity Information when triggered by a change in Organizational Identity Information. Identity notification can also be an indication that Identity Information has been exposed to a risk factor.

Inputs	Non-current Identity Information – Organizational Identity Information is not current or under review.
Outputs	Current Identity Information – Organizational Identity Information is current.
Dependencies	Organizational Identity Verification

3.1.7 Organizational Identity Linking

Organizational Identity Linking is the process of relating two or more sets/instances of Identity Information for the same Organization.

Inputs	Unlinked Identity Information – Organizational Identity Information for the same Organization exists in multiple locations.
Outputs	Linked Identity Information – Two or more sets of Organizational Identity Information have been confirmed as being about the same Organization and subsequently linked.
Dependencies	Organizational Identity Resolution

4. Introduction to the PCTF Verified Organization Conformance Profile

This section specifies the Conformance Criteria of the PCTF Verified Organization Component, a component of the Pan-Canadian Trust Framework (PCTF).

4.1 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.

5. 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.

Notes:

- 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.

5.1 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.

6. 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”.

Notes:

- 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: 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).	X	X		
2	The Responsible Authority **SHOULD** specify to Relying Parties and other parties the Organization(s) for which its services are provided.	X	X		
3	The Responsible Authority **SHOULD** specify to Relying Parties and other parties its mandate and authority as these relate to Organizational Verification.	X			
4	The Responsible Authority **MUST** specify to Relying Parties and other parties its mandate and authority as these relate to Organizational Verification.		X		
SERVICE PROVIDERS					

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
5	The Responsible Authority **MUST** be a juridical Entity (private or public sector) (e.g., government department, public sector agency, corporation, association, etc.).	X	X		
6	A Responsible Authority **MUST** identify any Authorized Agents it employs to carry out a Verified Organization Trusted process.	X	X		
7	If a Responsible Authority relies on Authorized Agents to carry out a Verified Organization Trusted Process, that Responsible Authority **MUST**: 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.	X	X		
PRIVACY AND SECURITY					
8	The Responsible Authority **MUST** adhere to the privacy risk management practices of the PCTF and any selected Conformance Profiles.	X	X		

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.	X	X		
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.	X	X		
OIDES	**Organizational Identity Establishment**				
FOUNDATIONAL IDENTITIES					
1	The Responsible Authority that creates the Foundational Identity Record **MUST** be a Public Sector Organization Registry.		X		
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.		X		
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.		X		
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.		X		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
5	All transactions relating to the creation of a Foundational Identity Record **MUST** be confirmed with and referenceable to a relevant Event Type.		X		
6	The Responsible Authority **MUST** identify the legal name of the Organization.		X		
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.		X		

8	Creation of a Foundational Identity Record **MUST** be confirmed with and referenceable to at least two of the following pieces of information:
	
	1. Date of creation in Canada
	2. Organization Type (from relevant registry)
	    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
			X		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4

9	The Responsible Authority **MUST** record the minimum Organizational Identity Information:
	
	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
	    1. Event date (if available, in whole or in part)
	        1. Event Year, Event Month, Event Day (if available)
	    2. Place of event
	        1. At least one of: Municipality Name, Province/Territory Code, Province/Territory Name
	
	Note
	
	• 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
			X		

10	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). If additional information is collected, the Responsible Authority **MUST** identify the reason for collecting the additional information.		X		
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.	X			
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.		X		
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.	X	X		
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.	X	X		
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.	X	X		
16	The Responsible Authority **MUST** enforce access controls to ensure only Authorized Personnel can create a Contextual Identity Record for the Organization.	X	X		
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.	X	X		

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.	X			
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.		X		
20	The Responsible Authority **MUST** identify the Legal name of the Organization.	X	X		
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.	X	X		
22	The Responsible Authority **SHOULD** identify the Legal Status of the Organization.	X			
23	The Responsible Authority **MUST** identify the Legal Status of the Organization.		X		
24	The Responsible Authority **MUST** record the minimum Organizational Identity Information: 1. Assigned Identifier that uniquely distinguishes the Organization. 2. Legal name indicating the name by which an Organization is legally recognized or referred to.	X	X		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
25	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). If additional information is collected, the Responsible Authority **MUST** identify the reason for collecting the additional information.	X			
26	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). If additional information is collected, the Responsible Authority **MUST** identify the reason for collecting the additional information.		X		
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.		X		
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.		X		
3	The issued Foundational Evidence of Organizational Identity Information **MUST** be consistent with information held in the Foundational Identity Record.		X		
4	The issued Foundational Evidence of Organizational Identity Information **MUST** identify the Responsible Authority that issued the evidence.		X		

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.		X		
CONTEXTUAL IDENTITIES					
6	The issued Contextual Evidence of Organizational Identity Information **MUST** be consistent with information held in the Contextual Identity Record.	X	X		
7	The issued Contextual Evidence of Organizational Identity Information **MUST** identify the Responsible Authority that issued the evidence.	X	X		
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.	X	X		
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.	X	X		
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).	X	X		
OIDVA	**Organizational Identity Validation**				
1	Persons acting on behalf of the Organization **MUST** be able to provide proof of their identity.	X	X		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
2	The Organization Verifier **MUST** ensure the information required to validate the Organization's Identity can be: 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.	X	X		
3	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).	X	X		
4	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.	X	X		
5	The Organization Verifier **MAY** accept self-assertion of Identity Information by persons acting on behalf of the Organization.	X			
6	The Organization Verifier **MAY** accept self-assertion of additional information (e.g., addresses) by persons acting on behalf of the Organization.	X			
7	The Organization Verifier **SHOULD** request/accept Foundational Evidence of Organizational Identity or Contextual Evidence of Organizational Identity.	X			
8	The Organization Verifier **MUST** request/accept Foundational Evidence of Organizational Identity.		X		

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.	X	X		
10	Foundational Evidence of Organizational Identity **SHOULD** be validated against a Foundational Identity Record.	X			
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.		X		
12	Contextual Evidence of Organizational Identity **SHOULD** be confirmed as originating from the Responsible Authority.	X	X		
13	Foundational Evidence of Organizational Identity **SHOULD** be confirmed as originating from the Responsible Authority.	X			
14	Foundational Evidence of Organizational Identity **MUST** be confirmed as originating from the Responsible Authority.		X		
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.	X	X		
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.	X	X		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
17	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. LOA requirements should be considered when determining an acceptable level of error. For example, a higher LOA would tolerate minimal error.	X	X		
18	The Organization Verifier **SHOULD** provide a validity period for Validation results to the Relying Party.	X			
19	The Organization Verifier **MUST** provide a validity period for Validation results to the Relying Party.		X		
OIDVE	**Organizational Identity Verification**				
1	The Responsible Authority **SHOULD** undertake the Verification steps it deems necessary.	X			
2	The Responsible Authority **MUST** undertake the Verification steps it deems necessary.		X		
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.	X	X		
4	The Organization Verifier **SHOULD** confirm that Foundational Evidence of Organizational Identity originates from the relevant Public Sector Organization Registry.	X			
5	The Organization Verifier **MUST** confirm that Foundational Evidence of Organizational Identity originates from the relevant Public Sector Organization Registry.		X		
OIDMA	**Organizational Identity Maintenance**				

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
FOUNDATIONAL IDENTITIES					
1	Any change to Organizational Identity Information **MUST** result in a timely update to the Foundational Identity Record of that Organization.		X		
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.		X		
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.		X		
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.		X		
5	All transactions resulting in a change to a Foundational Identity Record **MUST** be confirmed with and referenceable to a relevant Event Type.		X		
6	All transactions resulting in a change to a Foundational Identity Record **MUST** be confirmed by the relevant Public Sector Organizational Registry.		X		
7	The Responsible Authority **SHOULD** provide subscribed or otherwise known Relying Parties notification that Foundational Evidence of Organizational Identity has been updated.		X		
CONTEXTUAL IDENTITIES					
1	Any changes to Organizational Identity Information **MUST** result in a timely update to the Contextual Identity Record of that Organization.	X	X		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
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.	X	X		
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.	X	X		
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.	X			
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.		X		
6	The Responsible Authority **MAY** provide the ability for Authorized Personnel to update a Contextual Identity Record for the Organization.	X	X		
7	The Responsible Authority **SHOULD** enforce access controls to ensure only Authorized Personnel can update a Contextual Identity Record for the Organization.	X			
8	The Responsible Authority **MUST** enforce access controls to ensure only Authorized Personnel can update a Contextual Identity Record for the Organization.		X		
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.	X	X		

Reference	Conformance Criteria	Level of Assurance (LOA)			
		LOA 1	LOA 2	LOA 3	LOA 4
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.	X	X		
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.	X	X		
12	The Responsible Authority **SHOULD** provide subscribed or otherwise known Relying Parties notification that Contextual Evidence of Organizational Identity has been updated.	X	X		
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.	X			
2	The Responsible Authority **MUST** perform an Identity Verification process to ensure that the assigned identifiers reference the same Organization before creating a link.		X		
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.		X		

7. Appendix A: Event Types

This Appendix provides a list of all relevant event types that may occur in the life of an Organization and that may result in a trigger for the Trusted Processes defined for this PCTF Component.

- Amalgamation
- Amalgamated Predecessor
- Amalgamation Successor
- Amalgamation with other corporation(s)
- Amend Appointment of Agent for Service
- Annual Return – Integrated T2 Tax Return
- Annual Return – Integrated T2 Tax Return (Foreign)
- Annual Return – Integrated T2 Tax Return or Regular Charity
- Annual Return – Standalone
- Application for Authorization to Continue in Other Jurisdictions
- Application Authorization to Continue under CO-OP Corporations Act
- Application Correction Certificate for Doc. Filed Under B.C.A.
- Application for Amendment to Extra-Provincial Licence
- Application for Authority to Cont. Corporation without S/C As CO-OP
- Application for Extra-Provincial Licence
- Application for Incorporation of a Company
- Application for Incorporation Without S/C Letter Patent
- Application for Letters Patent of Amalgamation
- Application for Letters Patent for Continuance Not Included by Letters Patent
- Application for Letters Patent for Continuance of EP Corporation
- Application for Revival Order of Dissolved Corp.
- Application for Supplementary Letters Patent
- Application for Surrender of Charter
- Application for Termination of Extra-Provincial Licence
- Application to Transfer to Other Jurisdictions Under Section 313
- Appointment of Agent for Service
- Appointment of Recognized Agent
- Arrangement
- Articles of Amalgamation
- Articles of Amendment
- Articles of Arrangement
- Articles of Continuance
- Articles of Incorporation
- Articles of Reorganization
- Articles of Revival
- Bankruptcy
- Cancellation of Letters Patent (Involuntary Dissolution)
- Cessation of Business Name
- Change Directors
- Change Registered Office
- Client Ceased Operations
- Client Created

- Client Restart Activities
- Continuance in from another jurisdiction
- Continuance out to another jurisdiction
- Corporate Business Name – Amendment
- Corporate Business Name – Cancellation
- Corporate Business Name – Cancelled for Cause
- Corporate Business Name – Name Change
- Corporate Business Name – New Registration
- Corporate Business Name – Renewal
- Corporate Business Name – Revoked for Non-Payment
- Corporate Business Name – Revoked by Request
- Corrected Extra-Provincial Licence
- Corrected Letters Patent
- Death
- Dissolution
- Deceased Client
- Dissolve Corporation (voluntary)
- Dissolve Corporation (involuntary)
- EP Limited Liability Company – Amendment
- EP Limited Liability Company – Cancellation
- EP Limited Liability Company – Cancelled for Cause
- EP Limited Liability Company – New Registration
- EP Limited Liability Company – Renewal
- EP Limited Liability Company – Revoked for Non-Payment
- EP Limited Liability Company – Revoked by Request
- EP Limited Liability Partnership – Amendment
- EP Limited Liability Partnership – Cancellation
- EP Limited Liability Partnership – Cancelled for Cause
- EP Limited Liability Partnership – New Registration
- EP Limited Liability Partnership – Renewal
- EP Limited Liability Partnership – Revoked for Non-Payment
- EP Limited Liability Partnership – Revoked by Request
- EP Limited Partnership – Cancelled for Cause
- EP Limited Partnership – Change
- EP Limited Partnership – Name Change
- EP Limited Partnership – New Registration
- EP Limited Partnership – Renewal with Name Change
- EP Limited Partnership – Renewal without Name Change
- EP Limited Partnership – Revoked for Non-Payment
- EP Limited Partnership – Revoked by Request
- EP Limited Partnership - Withdrawal
- Establish Directors
- Establish Registered Office
- Extra-Provincial Licence – Cancelled for Cause
- Forced Name Change
- Forms Partnership
- General Partnership – Amendment
- General Partnership – Cancellation
- General Partnership – Cancelled for Cause
- General Partnership – Dissolution

- General Partnership – New Registration
- General Partnership – Renewal
- General Partnership – Revoked for Non-Payment
- General Partnership – Revoked by Request
- GP Operating Name – Amendment
- GP Operating Name – Cancellation
- GP Operating Name – Cancelled for Cause
- GP Operating Name – New Registration
- GP Operating Name – Renewal
- Incorporation
- Initial Returns
- Initial Returns – EP Domestic Corporations
- Initial Returns – Foreign Corporations
- Insolvency
- Insolvency: Bankruptcy
- Insolvency: Receivership
- Insolvency: Proposal – BIA
- Insolvency: Proposal – CCAA
- Insolvency: Proposal – FDMA
- Insolvency: Proposal – WRA
- Involuntary Dissolution
- Involuntary Dissolution (Cancellations)
- Limited Liability Partnership – Amendment
- Limited Liability Partnership – Cancellation
- Limited Liability Partnership – Cancelled for Cause
- Limited Liability Partnership – New Registration
- Limited Liability Partnership – Renewal
- Limited Liability Partnership – Revoked for Non-Payment
- Limited Liability Partnership – Revoked by Request
- Limited Partnership – Cancelled for Cause
- Limited Partnership – Change
- Limited Partnership – Dissolution
- Limited Partnership – Name Change
- Limited Partnership – New Registration
- Limited Partnership – Renewal with Name Change
- Limited Partnership – Renewal without Name Change
- Limited Partnership – Revoked for Non-Payment
- Limited Partnership – Revoked by Request
- LP Operating Name – Amendment
- LP Operating Name – Cancellation
- LP Operating Name – Cancelled for Cause
- LP Operating Name – New Registration
- LP Operating Name – Renewal
- Loses/Adds Member/Partner
- Merger
- Name Change by Order of the Registrar
- New Legal Name
- Notice of Change
- Notice of Change – EP Domestic Corporations
- Notice of Change – Foreign Corporations

- Notice of Officers and Directors
- Notice of Registered Office
- Ontario Corporations under Special Act
- Out of Business
- Register Business Name
- Renew Business Name
- Reorganization
- Restated Articles of Incorporation
- Restoration
- Revival
- Revival (if voluntary dissolution)
- Revival (if involuntary dissolution)
- Sole Proprietorship – Amendment
- Sole Proprietorship – Cancellation
- Sole Proprietorship – Cancelled for Cause
- Sole Proprietorship – New Registration
- Sole Proprietorship – Renewal
- Sole Proprietorship – Revoked for Non-Payment
- Sole Proprietorship – Revoked by Request
- Voluntary Dissolution
- Voluntary Winding-Up
- Winding-Up Court Order
- Winding-Up Voluntary

8. 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 through DIACC Sustaining Member Ballot