Substantive Comments	52
Editorial Comments	60
Total Comments	112

Total Accepted	36
Total Rejected	76
Auditable Criteria	ALL

Disposition of Comments: Verified Person Final Recommendation V1.0

Reference	Conformance Criteria	Level of Assurance (LOA)									
BASE	**Baseline**	**L1**	**L2**	**L3**	**L4**	**Comment**	**Type**	**Final: Accepted, Deferred, or Rejected**	**Rationale**	**Final Recommendation**	**Deemed Auditable**
1	The Responsible Authority MUST provide an overall description of the program or service, including: - Type and nature of program or service; - Intended recipients of program or service; - Approximate size, characteristics and composition of the client population.	Y	Y	Y		1. Clarifying to who this should be provided would help (is it to the end-user being verified, to the regulatory body, in an audit trail that accompany the verification process?)	Substantive	Accepted	Provide specifics about what must be documented.	The Responsible Authority MUST document a current overall description of the program or service, including: • Purpose statement o What does the service do (ie authentication, proofing, verification, etc) o Who is the audience impacted (ie general public, subset, etc) o Which industries (all, healthcare, finance, etc) • Services Description o Where is the solution managed from? Specific location. o Service Description – General marketing overview or description of the service o What types of validation, authentication or technology does the service include? □ Biometrics, mobile device integrity, ID doc validation, Liveness, risk checks, OTPs, etc o Service High Level Design and/or Architecture diagram o Service User/Data Flow Diagram ~~The Responsible Authority MUST provide an overall description of the program or service, including:~~ ~~- Type and nature of program or service;~~ ~~- Intended recipients of program or service;~~ ~~- Approximate size, characteristics and composition of the client population.~~	Y
1	The Responsible Authority MUST provide an overall description of the program or service, including: - Type and nature of program or service; - Intended recipients of program or service; - Approximate size, characteristics and composition of the client population.	Y	Y	Y		2. The second and third requirements suggest that the Responsible Authority will be providing identity verification services for a single use case rather than creating a reusable digital identity that can be used in multiple use cases. Where a reusable digital identity is created, the client population is difficult to classify with any accuracy. Therefore, the second and third requirements should be altered from MUST to SHOULD.	Substantive	Rejected	They are already stated as MUST.		Y

1	The Responsible Authority MUST provide an overall description of the program or service, including: - Type and nature of program or service; - Intended recipients of program or service; - Approximate size, characteristics and composition of the client population.	Y	Y	Y		3. it would be nice to have a standard example template for this.	Editorial	Rejected	Details have been specified.		Y
2	The Responsible Authority MUST specify its business role, purpose and authority as these relate to the identification of Subjects.	Y	Y	Y		Clarifying to who this should be specified would help (is it to the end-user being verified, to the regulatory body, in an audit trail that accompany the verification process?)	Editorial	Accepted		The Responsible Authority MUST ~~specify~~ document its business role, purpose and authority as these relate to the identification of Subjects.	Y
3	The Responsible Authority SHOULD be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.	Y				~~why the difference between L1 and L2/3? What if a US entity that was certified under the NIST guidelines wanted to show conformance to the PCTF, but wasn't registered to do business in Canada?~~	Substantive	Rejected	Comment redacted		Y
4	The Responsible Authority MUST be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.		Y	Y		~~How about "The Responsible Authority SHOULD ensure subjects confirm that the data is accurate."~~	Substantive	Rejected	It is not clear which criteria this comment is directed towards.		Y
4	The Responsible Authority MUST be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.		Y	Y		This appears to duplicate Q3 but with differing LOA and its not clear how LOA affects the private entity.	Substantive	Rejected	LoA affects the RA in terms ot the rigour around trusted processes. This is clear throughout the criteria.		Y
4	The Responsible Authority MUST be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.		Y	Y		why the difference between L1 and L2/3? What if a US entity that was certified under the NIST guidelines wanted to show conformance to the PCTF, but wasn't registered to do business in Canada?	Substantive	Rejected	This criteria specifies that an RA must have a legal presence in Canada to provide tangible legal accountability for L2 & L3.		Y
5	The Responsible Authority MUST make sure that personal information is collected and managed under relevant legal authorities.	Y	Y	Y		How about "The Responsible Authority SHOULD ensure subjects confirm that the data is accurate."	Editorial	Rejected	The use of MUST is appropriate here.		Y

5	The Responsible Authority MUST make sure that personal information is collected and managed under relevant legal authorities.	Y	Y	Y		The use of "authorities" could suggest an organisation or a legislative scheme. The language should be clearer, for example, simply stating that personal information must be collected and managed in accordance with the relevant data protection regime.	Substantive	Accepted		~~The Responsible Authority MUST make sure that personal information is collected and managed under relevant legal authorities.~~ The Responsible Authority MUST provide a reference to the legal authority, policy or requirement that supports the need to collect specific personal information. For example, in Ontario, privacy requirements are covered under the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPPA).	Y
5	The Responsible Authority MUST make sure that personal information is collected and managed under relevant legal authorities.	Y	Y	Y		how would one prove this? For example, should we state that the RA have a privacy policy that speaks to the scope of service in question and that privacy policy is publicly available?	Substantive	Rejected	The rewording has addressed this concern.		Y
6	If the Responsible Authority relies on or supports another organization for carrying out the Identity establishment process, a written agreement MUST be in place.	Y	Y	Y				No Comments			Y
7	The Responsible Authority SHOULD provide Users with written notice that any false or misleading statements may result in violation of terms or conditions.	Y				is this a legal requirement in Canada? If it is, then recommend “must” for all levels. If not, then recommend “should” for all levels unless we feel strongly our rules for identity service is different and should be stronger.	Editorial	Rejected	This criteria is considered to be a best practice and reflects the TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
8	The Responsible Authority MUST provide Users with written notice that any false or misleading statements may result in violation of terms or conditions.		Y	Y		is this a legal requirement in Canada? If it is, then recommend “must” for all levels. If not, then recommend “should” for all levels unless we feel strongly our rules for identity service is different and should be stronger.	Editorial	Rejected	This criteria is considered to be a best practice and reflects the TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
8	The Responsible Authority MUST provide Users with written notice that any false or misleading statements may result in violation of terms or conditions.		Y	Y		This appears to duplicate Q7 but with differing LOA and it's not clear how LOA affects the answer	Substantive	Rejected	There is inherent assumption that L2 and L3 transactions have the potential to lead to litigation. In such a situation, it is a best practice to advise Users of their obligations in a clear manner.		Y
9	If a Responsible Authority relies on another organization to carry out a Verified Person Trusted Process subject to the Verified Person conformance criteria, the Responsible Authority MUST provide: - Documentation on written agreement for the arrangement in effect; AND - Documentation on the approved Conformance Criteria assessment;	Y	Y	Y		Type, Level of documentation unclear. There may be several scenario e.g. Another Organization could be a Biometric provider	Editorial	Rejected	The intention of this criteria is to document both the legal agreement between the two organizations, and the sum of the end-to-end process between them that results in a Verified Person record.		Y

10	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority SHOULD: - Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate - Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject	Y	Y			Suggestion - In cases where the conformance criteria includes an IF statement, consider having an option to select N/A for organizations that don't support this functionality. We think that this conformance criteria may be more appropriate as part of the Verified Relationship component, instead of Verified Person.	Editorial	Rejected	Auditors can provide the rationale for non-conformance with this profile, including when the rationale is that the RA does not handle these cases. This criteria does not attempt to assess a relationship and provide a relationship attribute as an outcome.		Y
10	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority SHOULD: - Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate - Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject	Y	Y			Is <18 defined as child, minor?	Editorial	Rejected	A minor is defined at different ages depending on jurisdiction.		Y
10	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority SHOULD: - Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate - Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject	Y	Y			“Confirm that the applicant has the legal authority to carry out request” – is this a legal requirement in Canada for identity services? I might consider changing this to “must”	Substantive	Rejected	A SHOULD is required for this criteria because it specifies an incremental improvement regardless of the baseline controls that are in place. In certain circumstances, baseline controls may be more than adequate for vulnerable subjects as well.		Y
11	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority MUST: - Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate - Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject			Y		Is it relavent to separate this question baed on LOA?	Substantive	Rejected	Question only. The increasing amount of data that may be stored in higher assurance Verified Person records justify the separation of criteria into levels of assurance.		Y

11	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority MUST: - Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate - Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject			Y		Suggestion - In cases where the conformance criteria includes an IF statement, consider having an option to select N/A for organizations that don't support this functionality. We think that this conformance criteria may be more appropriate as part of the Verified Relationship component, instead of Verified Person	Editorial	Rejected	"This criteria concerns the Trusted Process of Identity Verification using contextual evidence with a Verified Person Record as the outcome. It does not attempt to assess a relationship and provide a relationship attribute as an outcome. "		Y
11	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority MUST: - Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate - Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject			Y		Is <18 defined as child, minor?	Editorial	Rejected	Question only. The definition of child/minor depends on the jurisdiction.		Y
12	These conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.	Y	Y	Y		This does not seem like a conformance criteria that a Responsible Authority could actually confirm. It seems more like a note, assumption of informational item. Suggest removing. This might be somehting that could go in an overview statement.	Substantive	Accepted	Reworded	Organizations and individuals MUST comply with applicable legislation, policy and regulations within their jurisdiction, which are subject to change. ~~These conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.~~	Y
12	These conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.	Y	Y	Y		how do they prove this? T&Cs in contracts? Need a “should” “must” here somewhere.	Editorial	Accepted	Reworded		Y
13	The Responsible Authority SHOULD provide Users with written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.	Y	Y	Y		It apppear that this conformance criteria assumes that the Responsible Authority is managing a database of subjects. This may not be the case as it is possible that the data is transient such that subject data gets removed after the identity proofing stage is complete. Would need to discuss with author prior to suggesting any changes.	Substantive	Rejected	This criteria has been made more clear by LoA.		Y
13	The Responsible Authority SHOULD provide Users with written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.	Y	Y	Y		Is this asking that end-user are instructed to notify if any of their information changes? If this is an identity verificstion for, say, a one of purchase then it would be highly impractical.	Substantive	Accepted		***This criteria has been broken into two seperate criteria, BASE 13 and Base 14, to highlight differences in LoA.***	Y

13	The Responsible Authority SHOULD provide Users with written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.	Y								The Responsible Authority SHOULD provide Users with written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.	Y
14	The Responsible Authority MUST provide Users with written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.		Y	Y						The Responsible Authority ~~SHOULD~~ MUST provide Users with written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.	Y
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**						.			
SOUR	**Trusted Process: Establish Sources Establish Sources is the preparatory process undertaken to determine which sources of Identity Evidence can be used to validate and/or verify a Person (i.e., Subjects), and the assurance of those sources. Typically, a Digital Identity system will use a range of sources to support the requirements to identify Subjects in a given context, and to meet the target Levels of Assurance. Note: These criteria are not included in the Public Sector Profile (IMSC), as they are part of the policy and/or legislated requirements of the Relying Party.**	**L1**	**L2**	**L3**	**L4**	**Comment**	**Type**	**Final: Accepted, Deferred, or Rejected**	**Rationale**	**Final Recommendation**	**Deemed Auditable**
1	If appropriate, the Responsible Authority MUST conform to their legislated mandate for holding the information for which they are being identified as a source. The Responsible Authority MUST have appropriate security, accuracy, completeness and privacy of their Identity sources, and determine: - The provenance of the Evidence - The robustness of the processes employed in collecting and storing the Evidence - The historic performance of the source - The ability of the source to satisfy relevant regulatory authorities - The recognition of the source in law	Y	Y	Y		Would like to discuss. I'm not sure I understand this	Editorial	Rejected	Comment only, no specific change recommended.		Y

1	If appropriate, the Responsible Authority MUST conform to their legislated mandate for holding the information for which they are being identified as a source. The Responsible Authority MUST have appropriate security, accuracy, completeness and privacy of their Identity sources, and determine: - The provenance of the Evidence - The robustness of the processes employed in collecting and storing the Evidence - The historic performance of the source - The ability of the source to satisfy relevant regulatory authorities - The recognition of the source in law	Y	Y	Y		It's not clear what "recognition of the source in law" means.	Editorial	Rejected	The RA must be able to reference the legislated mandate that grants the authority to hold the information.		Y
1	If appropriate, the Responsible Authority MUST conform to their legislated mandate for holding the information for which they are being identified as a source. The Responsible Authority MUST have appropriate security, accuracy, completeness and privacy of their Identity sources, and determine: - The provenance of the Evidence - The robustness of the processes employed in collecting and storing the Evidence - The historic performance of the source - The ability of the source to satisfy relevant regulatory authorities - The recognition of the source in law	Y	Y	Y		how would an RA do this? What would be provided as evidence? I assume an RA would have a contract with their source providers and they would have done due diligence in the source provider selection. Is showing the contract sufficient?	Substantive	Rejected	This comment will be passed on the assessment component team		Y
2	If the Responsible Authority uses an external source of Identity Evidence the external source of Identity MUST either hold a recognized independent accreditation or undergo an explicit assessment by the Responsible Authority.	Y	Y	Y		Would like to discuss. I'm not sure I understand this one.	Editorial	Rejected	Comment only, no specific change recommended.		Y
2	If the Responsible Authority uses an external source of Identity Evidence the external source of Identity MUST either hold a recognized independent accreditation or undergo an explicit assessment by the Responsible Authority.	Y	Y	Y		Not clear what is meant here by "external source of identity"? What kind of accreditation is expected here? Is it specifically expected to be a PCTF-related accreditation or some other independent accreditation? If PCTF, the conformance criteria should be clear and explicit.	Substantive	Accepted		If the Responsible Authority uses an external source of Identity Evidence the external source of Identity MUST hold a recognized PCTF accreditation, or jurisdictional or domain equivalent, or undergo an explicit assessment by the Responsible Authority. ~~either hold a recognized independent accreditation or undergo an explicit assessment by the Responsible Authority.~~	Y

2	If the Responsible Authority uses an external source of Identity Evidence the external source of Identity MUST either hold a recognized independent accreditation or undergo an explicit assessment by the Responsible Authority.	Y	Y	Y		This requirement is very vague. There should be examples of independent accreditation and an explanation of what is envisaged by an explicit assessment. For example, does a passport meeting a relevant ICAO standard count as a source with independent accreditation? Does an explicit assessment have to conclude with a written paper?	Substantive	Accepted			Y
2	If the Responsible Authority uses an external source of Identity Evidence the external source of Identity MUST either hold a recognized independent accreditation or undergo an explicit assessment by the Responsible Authority.	Y	Y	Y		It seems like this might be putting a requirement on the RA specific to how they select their source providers, which might change their long standing relationships or contract language. Just highlighting this for discussion	Substantive	Rejected	Noted.		Y
3	A source of Identity Evidence MUST be assessed as Low Assurance if: it is not possible to establish the provenance of the Evidence or the processes employed in collecting and storing the Evidence employed by the source.	Y	Y	Y		Would like to discuss. I'm not sure I understand this	Editorial	Rejected	Comment only, no specific change recommended.		Y
3	A source of Identity Evidence MUST be assessed as Low Assurance if: it is not possible to establish the provenance of the Evidence or the processes employed in collecting and storing the Evidence employed by the source.	Y	Y	Y		This appears to be statement, what is the requirement?	Editorial	Rejected	Question only. The purpose of this criteria is to prevent lower quality sources of evidence from being assessed at a higher level.		Y
4	A private sector source of Identity Information MUST be assessed as Medium Assurance only if: - the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR - in the case of a statistical source, where the ongoing accuracy of the source can be demonstrated from historical performance data.	Y	Y	Y		Would like to discuss. I'm not sure I understand this	Editorial	Rejected	Comment only, no specific change recommended.		Y
4	A private sector source of Identity Information MUST be assessed as Medium Assurance only if: - the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR - in the case of a statistical source, where the ongoing accuracy of the source can be demonstrated from historical performance data.	Y	Y	Y		This appears to be statement, what is the requirement?	Editorial	Rejected	Question only. The purpose of this criteria is to specify the minimum requirements for a private sector identity source to assessed as medium assurance.		Y

4	A private sector source of Identity Information MUST be assessed as Medium Assurance only if: - the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR - in the case of a statistical source, where the ongoing accuracy of the source can be demonstrated from historical performance data.	Y	Y	Y		Also wondering how this would be proven – possibly by looking at the contracts between the RA and the Source?	Substantive	Rejected	Question only. There is no implication in this criteria that the RA is not the custodian of the source information. Regardless, the source information must meet one of the two conditions to be assessed as Medium Assurance.		Y
5	A public sector source of Identity Information MUST be assessed as Medium Assurance only if: - the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR - it is a Foundational Source of Identity (refer to definition in Overview)	Y	Y	Y		Would like to discuss. I'm not sure I understand this	Editorial	Rejected	Comment only, no specific change recommended.		Y
5	A public sector source of Identity Information MUST be assessed as Medium Assurance only if: - the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR - it is a Foundational Source of Identity (refer to definition in Overview)	Y	Y	Y		This appears to be statement, what is the requirement?	Editorial	Rejected	Question only. The purpose of this criteria is to specify the minimum requirements for a public sector identity source to assessed as medium assurance.		Y
5	A public sector source of Identity Information MUST be assessed as Medium Assurance only if: - the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR - it is a Foundational Source of Identity (refer to definition in Overview)	Y	Y	Y		The criteria where the private sector provides accurate proxy of foundational identity evidence (e.g., passport, driver license) is not clearly covered in the criteria (SOUR 4 & 5).	Substantive	Rejected	There is no intention to permit proxies of proof of identity in this criteria.		Y
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**						.			

RESO	**Trusted Process: Identity Resolution** **Identity Resolution is the process of establishing the uniqueness of a Subject within a program/service population through the use of Identity Information. A program or service defines its Identity resolution requirements in terms of Identity Attributes; that is, the program/service specifies the set of Identity Attributes that is required to uniquely identify a Subject within its population.**	L1	L2	L3	L4	Comment	Type	Final: Accepted, Deferred, or Rejected	Rationale	Final Recommendation	Deemed Auditable
1	The Responsible Authority MUST specify the population or clientele for which its services are provided.	Y	Y	Y		See discussion in line 4.	Editorial	Accepted		The Responsible Authority MUST ~~specify~~ document the population or clientele for which its services are currently provided.	Y
1	The Responsible Authority MUST specify the population or clientele for which its services are provided.	Y	Y	Y		General comment of guidance for assessors and RAs on what to provide as evidence	Editorial	Accepted			Y
2	The Responsible Authority MUST ensure that the authoritative record uniquely resolves to only one Subject within their specified population of interest.		Y	Y				No Comments			Y
3	The set of Identity Attributes MUST be sufficient to distinguish between different Subjects within an Identity context; and sufficient to describe the Subject as required by the service or program. (See section 4.1.4 of Government of Canada Directive on Identity Management (July 2019))	Y	Y	Y				No Comments			Y
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**						.			
ESTAB	**Trusted Process: Identity Establishment (Contextual)** **Identity Establishment is the process of creating contextual Identity Evidence that may be relied on by others for delivery of programs, services, and activities.** **Note: The establishment and maintenance of Foundational Evidence of Identity is out of scope, as it is the exclusive domain of the public sector; those criteria can be found in the Public Sector Profile of the Pan-Canadian Trust Framework.**	L1	L2	L3	L4	Comment	Type	Final: Accepted, Deferred, or Rejected	Rationale	Final Recommendation	Deemed Auditable
1	Any transaction relating to the creation of a Verified Person Record MUST be confirmed and reference a relevant business event or activity.	Y	Y	Y		No clear what is required	Editorial	Accepted		Any transaction relating to the creation of a Verified Person Record MUST be ~~confirmed~~ auditable and reference a relevant business event or activity.	Y

1	Any transaction relating to the creation of a Verified Person Record MUST be confirmed and reference a relevant business event or activity.	Y	Y	Y		As discussed above, digital identities can be reusable and therefore created for no particular business event or activity. An individual may create set up their Yoti digital identity for no specific reason and only use it months later. In addition, many digital identity platforms are set up so that the activities of users are not viewable by the platform. Suggest that from "...and reference" is removed.	Substantive	Rejected	A business event or activity includes pre populating a record in anticipation of future transactions.		Y
2	The Responsible Authority MUST record as part of the Verified Person Record only the necessary Identity Information required for the intended business purposes. The Responsible Authority MUST NOT record information that is not required for the business purposes for which the User has engaged them.	Y	Y	Y		Definition of what is necessary Identity information may help	Editorial	Rejected	This is too broad to be feasible.		Y
2	The Responsible Authority MUST record as part of the Verified Person Record only the necessary Identity Information required for the intended business purposes. The Responsible Authority MUST NOT record information that is not required for the business purposes for which the User has engaged them.	Y	Y	Y		As discussed above, reusable digital identity platforms are not created for a specific purpose. Therefore, it is not possible for reusable digital identity platforms to ascertain what the relevant business purpose (s) are before allowing an individual to create their digital identity. For example, X Organization collects all of the information it believes is necessary for the creation of a reusable, genuine digital identity. It should be up to the relying party to request the proportionate amount of personal data for the relying party's business purpose. Therefore, line 35 should say "The Relying Party MUST record..." and "The Relying Party MUST NOT...".	Editorial	Accepted		The Responsible Authority MUST ~~record as part of the Verified Person Record only the necessary Identity Information~~ document the necessary Identity Information required for the intended business purposes. The Responsible Authority MUST NOT record information that is not required for the business purposes for which the User has engaged them.	Y
2	The Responsible Authority MUST record as part of the Verified Person Record only the necessary Identity Information required for the intended business purposes. The Responsible Authority MUST NOT record information that is not required for the business purposes for which the User has engaged them.	Y	Y	Y		should this be captured in a policy or document? I suppose the answer here is in 3.	Editorial	Rejected	Question only. Self-redacted.		Y
3	The Responsible Authority MUST have in place policies and procedures to safeguard the Identity Attribute(s) provided by the User.	Y	Y	Y				No Comments			Y
4	The Responsible Authority MUST have in place policies and procedures to detect and respond to the misuse of the Identity Attribute(s) provided by the User.		Y	Y		Misuse by whom? Misuse by the user? Misuse by relying parties? How is misuse defined? This requirement should be much clearer as to what obligations it is attempting to impose on Responsible Authorities.	Editorial	Accepted		The Responsible Authority MUST document policies and procedures to detect and respond to the ~~misuse of the Identity Attribute(s) provided by the User.~~ use of a User's Identity Attribute(s) without their consent.	Y

Reference	Conformance Criteria	Level of Assurance (LOA)						.			
VALID	**Trusted Process: Identity Information Validation** **Identity Information Validation is the process of confirming the accuracy of Identity Information about a Subject against that established by an Authoritative Source. Identity Information Validation relies on the Evidence obtained from the Establish Sources process to determine the claimed Identity Information exists and is valid.**	**L1**	**L2**	**L3**	**L4**	**Comment**	**Type**	**Final: Accepted, Deferred, or Rejected**	**Rationale**	**Final Recommendation**	**Deemed Auditable**
1	Self-assertion of Identity Information made by a Subject SHOULD be accepted.	Y				does this require we accept that the subject says they are who they say they are?	Editorial	Rejected	Question only. This criteria conveys that a persona provided by a User should be accepted without validation to enable continuity of service.		Y
2	Identity Information MUST acceptably match (see VALID-8) the assertion provided by the User and all instances of (Foundational and/or contextual) Evidence of Identity presented by the User.		Y	Y		So we determine what is acceptable?	Editorial	Rejected	Question only. The Responsible Authority's documented risk-based approach to differences between evidence and claimed Identity Information SHOULD be taken into consideration in the context of their Level of Assurance requirements.	Identity Information MUST acceptably match ~~(see VALID-8)~~ the assertion provided by the User and all instances of (Foundational and/or contextual) Evidence of Identity presented by the User.	Y
3	The required evidence, if any, MAY include low assurance sources.	Y				Not sure what the purpose of this criteria is. Would like to discuss.	Editorial	Rejected	Comment only, no specific change recommended.		Y
3	The required evidence, if any, MAY include low assurance sources.	Y				Definition of high, medium, low assurance will help	Editorial	Rejected	These are defined outside the scope of this component. Consider TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
3	The required evidence, if any, MAY include low assurance sources.	Y				do we prescribe how many pieces of evidence is appropriate at which level similar to NIST? (Noted later that this is captured in EVID)	Substantive	Rejected	Comment self-retracted		Y
4	The required evidence MUST, at a minimum, include medium assurance sources and MAY be supported by low assurance sources		Y			Defining the medium assurance sources seems quite arbitrary	Substantive	Rejected	These are defined outside the scope of this component. Consider TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
4	The required evidence MUST, at a minimum, include medium assurance sources and MAY be supported by low assurance sources		Y			Definition of high, medium, low assurance will help	Editorial	Rejected	These are defined outside the scope of this component. Consider TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
4	The required evidence MUST, at a minimum, include medium assurance sources and MAY be supported by low assurance sources		Y			do we prescribe how many pieces of evidence is appropriate at which level similar to NIST? (Noted later that this is captured in EVID)	Substantive	Rejected	Comment self-retracted		Y

5	The required evidence MUST, at a minimum, include the use of high assurance sources MAY be supported by medium and low assurance sources.			Y		Defining the high assurance sources seems quite arbitrary	Substantive	Rejected	These are defined outside the scope of this component. Consider TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
5	The required evidence MUST, at a minimum, include the use of high assurance sources MAY be supported by medium and low assurance sources.			Y		Definition of high, medium, low assurance will help	Editorial	Rejected	These are defined outside the scope of this component. Consider TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
5	The required evidence MUST, at a minimum, include the use of high assurance sources MAY be supported by medium and low assurance sources.			Y		do we prescribe how many pieces of evidence is appropriate at which level similar to NIST? (Noted later that this is captured in EVID)	Substantive	Rejected	Comment self-retracted		Y
6	The Responsible Authority SHOULD check the Evidence to confirm that it corresponds to the claimed Identity Information, and that the Evidence is genuine and not altered.	Y						No Comments			Y
7	The Responsible Authority MUST check the Evidence to confirm that it corresponds to the claimed Identity Information, and that the Evidence is genuine and not altered.		Y	Y				No Comments			Y
8	The Responsible Authority MUST document how differences between the Evidence and the claimed Identity Information relate to their risk tolerance. For example, a specific Responsible Authority might conclude that a difference in telephone number presents a low risk to them in cases where all other evidence is identical to the claimed Identity Information. The Responsible Authority's documented risk-based approach to differences between evidence and claimed Identity Information SHOULD be taken into consideration in the context of their Level of Assurance requirements. For example, higher levels of risk are usually not acceptable for higher Levels of Assurance whereas those higher levels of risk might be acceptable in some cases where a low Level of Assurance is required.	Y	Y	Y		It's not entirely clear how this requirement is expected to be tested. It is generally challenging in the private sector to share risk assessments and levels of tolerance, and may also potentially be the same situation in a intra or inter-government situation. If the purpose of documenting differences is to share this, who is it being shared with? Generally a claim wouldn't be issued if the ecosystem didn't trust it, so there is some inherent assumption of risk assessment in issuing claims.	Substantive	Accepted	This criteria can be tested by ensuring that the RA has documented their decisions around managing risk associated with identity claim differences. These decisions are bounded by other criteria that specify acceptable differences at each level. The purpose of this specific criteria is to ensure adequate documentation.	The Responsible Authority MUST document how differences between the Evidence and the claimed Identity Information relate to their risk tolerance at each Level of Assurance. For example, a specific Responsible Authority might conclude that a difference in telephone number presents a low risk to them in cases where all other evidence is identical to the claimed Identity Information. ~~The Responsible Authority's documented risk-based approach to differences between evidence and claimed Identity Information SHOULD be taken into consideration in the context of their Level of Assurance requirements. For example, higher levels of risk are usually not acceptable for higher Levels of Assurance whereas those higher levels of risk might be acceptable in some cases where a low Level of Assurance is required.~~	Y

8	The Responsible Authority MUST document how differences between the Evidence and the claimed Identity Information relate to their risk tolerance. For example, a specific Responsible Authority might conclude that a difference in telephone number presents a low risk to them in cases where all other evidence is identical to the claimed Identity Information. The Responsible Authority's documented risk-based approach to differences between evidence and claimed Identity Information SHOULD be taken into consideration in the context of their Level of Assurance requirements. For example, higher levels of risk are usually not acceptable for higher Levels of Assurance whereas those higher levels of risk might be acceptable in some cases where a low Level of Assurance is required.	Y	Y	Y		Definition of high, medium, low assurance will help	Editorial	Rejected	These are defined outside the scope of this component. Consider TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
8	The Responsible Authority MUST document how differences between the Evidence and the claimed Identity Information relate to their risk tolerance. For example, a specific Responsible Authority might conclude that a difference in telephone number presents a low risk to them in cases where all other evidence is identical to the claimed Identity Information. The Responsible Authority's documented risk-based approach to differences between evidence and claimed Identity Information SHOULD be taken into consideration in the context of their Level of Assurance requirements. For example, higher levels of risk are usually not acceptable for higher Levels of Assurance whereas those higher levels of risk might be acceptable in some cases where a low Level of Assurance is required.	Y	Y	Y		this allows for a lot of flexibility for the RA. Would like to discuss this a bit more.	Substantive	Accepted	These decisions are bounded by other criteria that specify acceptable differences at each level. The purpose of this specific criteria is to ensure adequate documentation. Maybe skip the further elaboration stuff and refer to whomever might be working on assessor guidance? It should always be noted that this doc cannot really be properly consumed without the Overview. Perhaps the Introduction section of each Profile be revisited to make note of the fact that they should be reading and accounting for the material in the Component Overview when considering the conformance criteria - make it explicit.		Y
9	The level of risk resulting from differences between the Evidence and the claimed Identity Information (VALID-8) that is acceptable MAY be determined by the Responsible Authority.	Y					Editorial	No Comments		The level of risk resulting from differences between the Evidence and the claimed Identity Information ~~(VALID-8)~~ that is acceptable MAY be determined by the Responsible Authority.	Y

10	The level of risk resulting from differences between the Evidence and the claimed Identity Information (VALID-8) that is acceptable MUST align with the needs of regulated industry services, if applicable.		Y			The requirement is not testable, the assessment of this conformance criteria is not clear.	Editorial	Accepted		The level of risk resulting from differences between the Evidence and the claimed Identity Information ~~(VALID-8)~~ that is acceptable MUST conform with the requirements of regulated industry services, if applicable.	Y
10	The level of risk resulting from differences between the Evidence and the claimed Identity Information (VALID-8) that is acceptable MUST align with the needs of regulated industry services, if applicable.		Y			in line with the above. The use of “must” align with needs of regulated industry services, “if applicable” is giving me pause. How is this determined?	Substantive	Rejected	Reworded		Y
11	The level of risk resulting from differences between the Evidence and the claimed Identity Information (VALID-8) that is acceptable MUST be minimal and limited to, for example, minor formatting and spelling differences where it is clear that the values are semantically the same.			Y		even minor formatting and spelling differences could mean a different person entirely.	Editorial	Accepted		The level of risk resulting from differences between the Evidence and the claimed Identity Information ~~(VALID-8)~~ that is acceptable MUST be minimal and well documented. ~~and limited to, for example, minor formatting and spelling differences where it is clear that the values are semantically the same.~~	Y
12	Contextual Evidence of identity MUST be confirmed as originating from the issuing authority. If confirmation from issuing authority is not feasible, then contextual Evidence of Identity MUST be confirmed using a trained examiner.		Y	Y		Suggest more detail is provided on the type of training required. Trained resources must have proven courses/certifications on identifying fraud.	Editorial	Rejected	The definition of a Trained Examiner may vary widely based on the type of evidence being examined.		Y
12	Contextual Evidence of identity MUST be confirmed as originating from the issuing authority. If confirmation from issuing authority is not feasible, then contextual Evidence of Identity MUST be confirmed using a trained examiner.		Y	Y		Forensic document concept not clearly covered in the criteria. General feedback - some organizations establish the dynamic element of a chain of trust in the their solution's network and provides trust in the system that facilitate interaction between data providers and consumers for consented data sharing. The existing roles in this component don't account for this role entirely in a multi-party identity network and we recommend considering the addition of network operator role in this component.	Substantive	Rejected	The concept of a Chain of Trust is beyond the scope of this version.		Y
12	Contextual Evidence of identity MUST be confirmed as originating from the issuing authority. If confirmation from issuing authority is not feasible, then contextual Evidence of Identity MUST be confirmed using a trained examiner.		Y	Y		do we define “trained examiner”?	Editorial	Rejected	Question only. The definition of a Trained Examiner may vary widely based on the type of evidence being examined.		Y

13	Foundational Evidence of Identity MUST be confirmed as originating from issuing authority, who has validated the Identity Information using an authoritative record, or allows the Relying Party to validate the Identity Information at the Authoritative Source. If confirmation from originating authority or validation at source is not feasible, then Foundational Evidence of Identity MUST be confirmed using trained examiner.		Y	Y		Suggest more detail is provided on the type of training required. Trained resources must have proven courses/certifications on identifying fraud	Editorial	Rejected	The definition of a Trained Examiner may vary widely based on the type of evidence being examined.		Y
13	Foundational Evidence of Identity MUST be confirmed as originating from issuing authority, who has validated the Identity Information using an authoritative record, or allows the Relying Party to validate the Identity Information at the Authoritative Source. If confirmation from originating authority or validation at source is not feasible, then Foundational Evidence of Identity MUST be confirmed using trained examiner.		Y	Y		do we define “trained examiner”?	Editorial	Rejected	Question only. The definition of a Trained Examiner may vary widely based on the type of evidence being examined.		Y
14	The Responsible Authority MUST ensure that the sources and technology used to perform the validation process are understood, and suitable (SOUR-6).	Y	Y	Y		This seems very ambiguous. Could not find SOUR-6	Editorial	Accepted			Y
14	The Responsible Authority MUST ensure that the sources and technology used to perform the validation process are understood, and suitable (SOUR-6).	Y	Y	Y		Details on SOUR-6 conformance criteria is not present in the assessment spreadsheet. It is possible that it was intended to be SOUR-4 and SOUR-5	Editorial	Accepted		The Responsible Authority MUST ensure that the sources and technology used to perform the validation process are understood, and suitable ~~(SOUR-6)~~ as defined for public and private sources in the SOUR section of this document.	Y
15	Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking MAY employ best practices for fraudulent document detection.	Y				What is the purpose of this criteria?	Substantive	Accepted		Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking ~~MAY~~ SHOULD employ best practices for fraudulent document detection.	Y
16	Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking MUST employ best practices for fraudulent document detection.		Y	Y		How about "Where Evidence is presented in the form of physical documents that do not have an echip via ICAO 9303, then Evidence checking MUST employ best practices for fraudulent document detection. What are those best practices? Perhaps they should be detailed Can you achieve LOA3 when this is not true?	Substantive	Rejected	Reworded		Y

16	Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking MUST employ best practices for fraudulent document detection.		Y	Y		do we define “best practices for fraudulent document detection”?	Editorial	Accepted		Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking MUST employ and document a fraud detection regimen specific to the document(s) under evaluation. ~~best practices for fraudulent document detection.~~	Y
17	Where Evidence is digital (including API-based and digital certificate-based) appropriate processes SHOULD be employed to ensure the integrity of the Evidence. (e.g., Tamper-evident, cryptographically signed, machine-verification of a Credential.)	Y						No Comments			Y
18	Where Evidence is digital (including API-based and digital certificate-based) appropriate processes MUST be employed to ensure the integrity of the evidence. (e.g., Tamper-evident, cryptographically signed, machine-verification of a Credential.)		Y	Y		do we want to be more specific?	Editorial	Accepted		Where Evidence is digital (including API-based and digital certificate-based) appropriate processes MUST be employed to ensure the integrity of the evidence. (e.g., Tamper-evident, cryptographically signed, machine-verification of a Credential.) Information provided in the Credentials and Infrastructure profiles may provide further guidance for this criteria.	Y
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**						.			
EVID	**Trusted Process: Evidence Validation Evidence Validation is the process of confirming that the Evidence presented (physical or electronic) can be accepted or be admissible as a proof (i.e., beyond a reasonable doubt, balance of probabilities, and substantial likelihood).**	**L1**	**L2**	**L3**	**L4**	**Comment**	**Type**	**Final: Accepted, Deferred, or Rejected**	**Rationale**	**Final Recommendation**	**Deemed Auditable**
1	No restriction on what kind of Evidence an organization accepts.	Y				What is the purpose of this critieria?	Substantive	Rejected	Question Only: This criteria specifies that are no obligations at this level. Inclusion of this criteria gives a consolidated view of the differences by LoA.		Y
1	No restriction on what kind of Evidence an organization accepts.	Y				Unable to decipher criteria	Editorial	Accepted	This criteria specifies that are no obligations at this level.	There is no restriction on what kind of Evidence an ~~organization~~ Organization accepts.	Y
1	No restriction on what kind of Evidence an organization accepts.	Y				When reference is made to an "organisation" does this mean a Responsible Authority or a Relying Party, or both, or a different entity altogether?	Editorial	Rejected	THE PCTF defines an Organization as an Entity that consists of a person or organized body of people with a particular purpose, and whose existence is established by legal statute. Proposed change - capitalize 'Organization' to indicate a defined term.		Y

2	One instance of Evidence of Identity (contextual or foundational) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.		Y			SOUR-6 may be missing	Editorial	Accepted		One instance of Evidence of Identity (contextual or foundational) MUST be assessed to be at least a medium level of assurance per ~~SOUR-5 or SOUR-6~~ SOUR criteria.	Y
2	One instance of Evidence of Identity (contextual or foundational) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.		Y			The SOUR definitions combined with the requirement stated is not clear.	Editorial	Accepted			Y
2	One instance of Evidence of Identity (contextual or foundational) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.		Y			Details on SOUR-6 conformance criteria is not present in the assessment spreadsheet. It is possible that it was intended to be SOUR-4 and SOUR-5	Editorial	Accepted			Y
2	One instance of Evidence of Identity (contextual or foundational) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.		Y			There is currently no such thing as SOUR-6. Should this say "per SOUR-4 or SOUR-5"?	Editorial	Accepted			Y
2	One instance of Evidence of Identity (contextual or foundational) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.		Y			Where's SOUR-6?	Editorial	Accepted			Y
3	Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.			Y		Why couldn't a passport with an eChip be used? Therefore, just one evidence of identity	Substantive	Rejected	Question only. This document is not intended to redfine assurance guidelines as defined by TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
3	Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.			Y		The SOUR definitions combined with the requirement stated is not clear.	Editorial	Accepted		Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) MUST be assessed to be at least a medium level of assurance per ~~SOUR-5 or SOUR-6~~ SOUR criteria.	Y
3	Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.			Y		Details on SOUR-6 conformance criteria is not present in the assessment spreadsheet. It is possible that it was intended to be SOUR-4 and SOUR-5	Editorial	Accepted			Y
3	Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.			Y		There is currently no such thing as SOUR-6. Should this say "per SOUR-4 or SOUR-5"?	Editorial	Accepted			Y
3	Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.			Y		Where's SOUR-6?	Editorial	Accepted			Y

4	Foundational Evidence MUST originate from an Authoritative Source that is under the control of a federal, provincial or territorial government, or the local equivalent abroad; and used to maintain registration of specific vital events or to determine legal status. Acceptable Authoritative Sources, records and documents for Foundational Evidence: - Vital statistics records used in the issuance of birth certificates; -Legal status records used in the issuance of citizenship and naturalization certificates and permanent resident cards; and - Other authoritative records enabled by departmental legislation.		Y	Y		Why couldn't a passport with an eChip be used? Discuss.	Substantive	Rejected	Question only. This document is not intended to redfine assurance guidelines as defined by TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
4	Foundational Evidence MUST originate from an Authoritative Source that is under the control of a federal, provincial or territorial government, or the local equivalent abroad; and used to maintain registration of specific vital events or to determine legal status. Acceptable Authoritative Sources, records and documents for Foundational Evidence: - Vital statistics records used in the issuance of birth certificates; -Legal status records used in the issuance of citizenship and naturalization certificates and permanent resident cards; and - Other authoritative records enabled by departmental legislation.		Y	Y		The SOUR definitions combined with the requirement stated is not clear.	Editorial	Rejected	Criteria description is considered to be adequate as written. Foundational Evidence and Authoritative Source are defined in the PCTF Glossary		Y
5	Foundational Evidence of Identity Information that is incomplete or inconsistent with information provided by the User (e.g., name change) may require additional confirmation by the Authoritative Source, or additional contextual Evidence.		Y	Y		This appears to be statement, what is the requirement?	Substantive	Accepted		Foundational Evidence of Identity Information that is incomplete or inconsistent with information provided by the User (e.g., name change) ~~may~~ SHOULD require additional confirmation by the Authoritative Source, or additional contextual Evidence.	Y

6	Contextual Evidence MUST originate from an Authoritative Source that is under the control of a PCTF approved organization. Acceptable Authoritative Sources, records and documents for contextual Evidence: - Licensing and registration records or documents used in the issuance of a driver's licence; - Passport or Certificate of Indian Status; and - Accredited professional organizations used in the issuance of professional credentials.		Y	Y		GoC uses term "Supporting" rather than "Contextual". I suggest being consistent as much of the text here is from GoC TBS web page. See: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Rejected	The term 'contextual' was chosen to better align with global standards.		Y
6	Contextual Evidence MUST originate from an Authoritative Source that is under the control of a PCTF approved organization. Acceptable Authoritative Sources, records and documents for contextual Evidence: - Licensing and registration records or documents used in the issuance of a driver's licence; - Passport or Certificate of Indian Status; and - Accredited professional organizations used in the issuance of professional credentials.		Y	Y		What will happen during the transition period after the trustmark program is implemented and some organizations have not yet been certified? Does this mean a non-PCTF-approved organization would not be allowed to participate in any digital identity ecosystem? Need to better understand the semantic meaning of onboarding an org without the trustmark being in place.	Substantive	Accepted		Contextual Evidence MUST originate from an Authoritative Source that is under the control of ~~a PCTF approved~~ an Organization that is PCTF approved, or has jurisdictional or domain equivalent, or has undergone an explicit assessment by the Responsible Authority. Acceptable Authoritative Sources, records and documents for contextual Evidence may include: - Licensing and registration records or documents used in the issuance of a driver's licence; - Passport or Certificate of Indian Status; and - Accredited professional organizations used in the issuance of professional credentials.	Y
6	Contextual Evidence MUST originate from an Authoritative Source that is under the control of a PCTF approved organization. Acceptable Authoritative Sources, records and documents for contextual Evidence: - Licensing and registration records or documents used in the issuance of a driver's licence; - Passport or Certificate of Indian Status; and - Accredited professional organizations used in the issuance of professional credentials.		Y	Y		This is likely to undermine the ability of Responsible Authorities that work in an international context from participating, given that such RAs cannot be expected to limit the evidence they receive to only one country's list of aceptable Authoritative Sources. This appears to be an obligation that would be better placed on the Relying Party, rather than the Responsible Authority.	Substantive	Accepted			Y

6	Contextual Evidence MUST originate from an Authoritative Source that is under the control of a PCTF approved organization. Acceptable Authoritative Sources, records and documents for contextual Evidence: - Licensing and registration records or documents used in the issuance of a driver's licence; - Passport or Certificate of Indian Status; and - Accredited professional organizations used in the issuance of professional credentials.		Y	Y		I may be confused on the wording, but are we saying we will only consider contextual evidence if it comes from an Auth Source under the control of the PCTF? What if it's a source outside the PCTF?	Substantive	Accepted			Y
7	If contextual Evidence is accepted in conjunction with Foundational Evidence of Identity (Level 3): - Contextual evidence of identity is expected to be consistent with the information that is provided by the foundational evidence of identity. - Additional contextual evidence may be required in the case of incomplete or inconsistent identity information (e.g., name change). - An endorsement or certification may be required to verify that the contextual evidence is a true copy of an original.		Y	Y		Should the LOA2 column be blank here if the requirement refers specifically to only Level 3? Generally this is also written from a perspective of a single org with knowledge or control over the entire system. Not clear how this applies in a multi-party system with no single party having complete visibiliy to assess or enforce a decision.	Substantive	Rejected	Level 2 may use more than one piece of Identity evidence as well, although that does not alleviate the obligation to ensure that at least one of them meets the relevant L2 criteria. Evidence is assessed as part of the Evidence Validation Trusted Process. Whether that process is performed by one or more parties is not relevant to the criteria since it has previously been evaluated as a whole as a Trusted process.		Y
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**						.			
PRES	**Trusted Process: Identity Presentation** **Identity Presentation is the process of dynamically confirming that a Subject has a continuous existence over time (i. e., "genuine presence"). This process can be used to help detect fraudulent activity (past or present) and to address identity spoofing concerns.**	**L1**	**L2**	**L3**	**L4**	**Comment**	**Type**	**Final: Accepted, Deferred, or Rejected**	**Rationale**	**Final Recommendation**	**Deemed Auditable**
1	Conformance criteria for Identity Presentation will be included in a future release of the PCTF.					Does this mean identity is "Alive"?	Substantive	Rejected	Question only. No, it will not imply an 'alive' status, but it will imply a 'has been alive' status.		Y
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**									
VERIF	**Trusted Process: Identity Verification** **Identity Verification is the process of confirming that the Identity Information being presented relates to the Subject who is making the claim. It should be noted that this process may use personal information that is not related to identity.**	**L1**	**L2**	**L3**	**L4**	**Comment**	**Type**	**Final: Accepted, Deferred, or Rejected**	**Rationale**	**Final Recommendation**	**Deemed Auditable**

1	The Responsible Authority MAY undertake the verification steps it deems necessary, if any.	Y				What is the purpose of this critieria?	Substantive	Rejected	Question only. Where there is no content to which a criteria applies, or the criteria does not express a requirement, the criteria is considered satisfied. Criteria may be used in this way to achieve a commonality of understanding.		Y
2	The Responsible Authority MUST ensure that interactions within a given context can be linked to the Subject who is making the claim.		Y	Y		might want to add language around the RA ensuring the transaction can be linked, but also ensuring privacy is in place to degree the PCTF wants to enforce privacy.	Substantive	Rejected	From the Privacy Component: "The handling of Subject-Specific Personal Information, and Service-Specific Information, by a Disclosing Organization is subject to relevant privacy legislation and regulations and is not generally deemed to fall within the scope of the requirements of the PCTF until that data is processed for the purpose of sharing via the Digital Identity Ecosystem"		Y
3	The Responsible Authority MUST, at a minimum, verify the Subject remotely, and MAY use one of the following methods: - knowledge-based verification - contextual data The verification MUST provide sufficient assurance that only the identifiable Subject in question would be able to successfully complete the verification process.		Y					No Comments			Y
4	The Responsible Authority MUST use at least one of the following methods to ensure the Identity Information relates to the User and the Subject: - Biological (e.g., photo ID), biometric (e.g.: fingerprint), or behavioural - characteristic confirmation - Face-to-face verification in person (or equivalent) - Physical possession confirmation If the above methods are not feasible then alternative methods MUST be defined and documented in an exception process which MAY include: - Confirmation by a trusted referee (e.g., guarantor, notary, certified agent) as determined by program-specific criteria - Additional safeguards - Compensating factors			Y		If using biometrics: must be certified to ISO 30107-3 Level 2 for Presentation Attack Detection (PAD) Photo ID: Algorirthm must be tested by NIST FRVT 1:1 Fingerprint: Algorithm must be tested by NIST FpVTE 2012 Must be trained/certified resource in matching faces or fingerprints	Substantive	Rejected	It is the intention of the conformance criteria to specify what what must be done and to refrain from specifying the how. This approach best supports industry innovation. This would be up to the documented policy for the ecosystem in question and it's required elsewhere that policy and procedure for things like this be documented.		Y

4	The Responsible Authority MUST use at least one of the following methods to ensure the Identity Information relates to the User and the Subject: - Biological (e.g., photo ID), biometric (e.g.: fingerprint), or behavioural - characteristic confirmation - Face-to-face verification in person (or equivalent) - Physical possession confirmation If the above methods are not feasible then alternative methods MUST be defined and documented in an exception process which MAY include: - Confirmation by a trusted referee (e.g., guarantor, notary, certified agent) as determined by program-specific criteria - Additional safeguards - Compensating factors			Y		Define Compensating Factors	Editorial	Rejected	Compensating Factors is a term widely used in industry. For a common definition, consult TBS Guideline on Identity Assurance https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML		Y
5	In addition to the conditions specified in BASE-10, private and government organizations MAY include Evidence of Identity requirements for a parent or guardian as part of the Evidence of Identity requirements for a child, minor or other vulnerable Subject. For example, the passport of a parent could be used as contextual Evidence of Identity for the child.	Y	Y	Y		Suggestion - We think that this conformance criteria fits better in the Verified Relationship component, instead of Verified Person	Substantive	Rejected	This criteria concerns the Trusted Process of Identity Verification using contextual evidence with a Verified Person Record as the outcome. It does not attempt to assess a relationship and provide a relationship attribute as an outcome.		Y
5	In addition to the conditions specified in BASE-10, private and government organizations MAY include Evidence of Identity requirements for a parent or guardian as part of the Evidence of Identity requirements for a child, minor or other vulnerable Subject. For example, the passport of a parent could be used as contextual Evidence of Identity for the child.	Y	Y	Y		we should be sure to align with Canadian laws and regs here.	Editorial	Rejected		In addition to the conditions specified in ~~BASE-10~~ the BASE section concerning vulnerable subjects, private and government organizations MAY include Evidence of Identity requirements for a parent or guardian as part of the Evidence of Identity requirements for a ~~child,~~ minor or other vulnerable Subject. For example, the passport of a parent could be used as contextual Evidence of Identity for the child."	Y
Reference	**Conformance Criteria**	**Level of Assurance (LOA)**						.			

MAINT	**Trusted Process: Identity Maintenance** **Identity Maintenance is the process of ensuring that Identity Information is as accurate, complete, and up-to-date as is required. This process deals with events that may impact the previously performed Identity Information Validation and Identity Verification (e. g., Evidence used to establish the Verified Person has changed, expired or been revoked, which invalidates the Verified Person Record).**	L1	L2	L3	L4	Comment	Type	Final: Accepted, Deferred, or Rejected	Rationale	Final Recommendation	Deemed Auditable
1	The Responsible Authority MAY deem the Subject to be no longer verified if any one of the following are true: - Any contextual Evidence changes. - The status of the Foundational Evidence changes. This could include immigration, marriage, death or the status changes that impact the previous Identity Information Validation and Identity Verification processes. - The elapsed time since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the Relying Party.	Y						No Comments			Y
2	The Responsible Authority MUST deem the Subject to be no longer verified if any one of the following are true: - Any contextual Evidence changes. - The status of the Foundational Evidence changes. This could include immigration, marriage, death or the status changes that impact the previous Identity Information Validation and Identity Verification processes. - The elapsed time since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the Relying Party.		Y	Y		bullet 3 – this would need to be captured in the RA/RP contract language. Does PCTF want to establish it's own baseline?	Substantive	Rejected	Stipulating contractual components is outside the scope of the PCTF.	The Responsible Authority MUST not represent a Subject as verified to an RP if the RA becomes aware of any of the following for a Subject: ~~deem the Subject to be no longer verified if any one of the following are true:~~ - Any contextual Evidence changes. - The status of the Foundational Evidence changes. This could include immigration, marriage, death or the status changes that impact the previous Identity Information Validation and Identity Verification processes. - The elapsed time since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the ~~Relying Party~~ Responsible Authority.	Y

3	The Responsible Authority MAY perform additional checks to re-validate or re-verify the Subject. In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes. In all cases, sufficient checks MUST be performed to ensure that the full Identity Resolution, Identity Information Validation, and Identity Verification requirements are upheld, for the Level of Assurance in question.	Y						No Comments			Y
4	The Responsible Authority SHOULD perform additional checks to re-validate or re-verify the Subject. In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes. In all cases, sufficient checks MUST be performed to ensure that the full Identity Resolution, Identity Information Validation, and Identity Verification requirements are upheld, for the Level of Assurance in question.		Y			similar comment about the frequency	Substantive	Rejected	There are no other comments regarding frequency, so this comment lacks context. If the intent was to imply that a frequency for re-validation of the Subject is needed, it is the responsibility of Relying Parties to make determinations based on their own risk management approach.		Y
5	The Responsible Authority MUST perform additional checks to re-validate or re-verify the Subject. In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes. In all cases, sufficient checks MUST be performed to ensure that the full Identity Resolution, Identity Information Validation, and Identity Verification requirements are upheld, for the Level of Assurance in question.			Y		Why the difference between SHOULD or MUST, either it is done or it is not done.	Editorial	Rejected	SHOULD means that the requirement is expected to be met, except in limited cases where the applicant documents valid reasons or circumstances to ignore the requirement. The full implications of such an exception must be understood and carefully weighed before choosing to not adhere to the conformance criteria as described.		Y
5	The Responsible Authority MUST perform additional checks to re-validate or re-verify the Subject. In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes. In all cases, sufficient checks MUST be performed to ensure that the full Identity Resolution, Identity Information Validation, and Identity Verification requirements are upheld, for the Level of Assurance in question.			Y		similar comment about the frequency	Substantive	Rejected	There are no other comments regarding frequency, so this comment lacks context. If the intent was to imply that a frequency for re-validation of the Subject is needed, it is the responsibility of Relying Parties to make determinations based on their own risk management approach.		Y

6	When the Responsible Authority becomes aware of any changes to Identity Information resulting from Birth or Death events it SHOULD correct or update the Subject's record(s) (in accordance with applicable legislation or regulations)	Y				Suggestion - We think that this conformance criteria fits better in the Verified Relationship component, instead of Verified Person	Substantive	Rejected	This criteria concerns the Trusted Process of Identity Maintenance triggered by death or birth events and produces an updated Verified Person Record as the outcome. It does not attempt to assess a relationship and provide a relationship attribute as an outcome.		Y
6	When the Responsible Authority becomes aware of any changes to Identity Information resulting from Birth or Death events it SHOULD correct or update the Subject's record(s) (in accordance with applicable legislation or regulations)	Y				Are there examples of when this “should” vs a “must” given privacy requirements	Substantive	Rejected	Question only. The need to respect privacy is consistent across all assurance levels. It is the intended assurance of accuracy of the Verified Person records that determine the need for 'SHOULD' or 'MUST' in this case.		Y
7	When the Responsible Authority becomes aware of any changes to Identity Information resulting from Birth or Death events it MUST correct update the Subject's record(s) (in accordance with applicable legislation or regulations)		Y	Y		Suggestion - We think that this conformance criteria fits better in the Verified Relationship component, instead of Verified Person	Substantive	Rejected	This criteria concerns the Trusted Process of Identity Maintenance triggered by death or birth events and produces an updated Verified Person Record as the outcome. It does not attempt to assess a relationship and provide a relationship attribute as an outcome.		Y
8	Any changes to Foundational Identity information MUST be confirmed by a foundational authority for the related event for: - Name change - Death		Y	Y				No Comments			Y
9	Birth and Death events SHOULD result in notification to Relying Parties.		Y	Y		Why should a birth event result in notification to RP?	Substantive	Rejected	Question only. There are circumstances where an RP may be relying on Verified Person attributes to make business decisions. An example would be whether or not a Subject has any dependents.		Y