PCTF Infrastructure (Technology & Operations)

Document Status: Final Recommendation V1.2

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 Infrastructure (Technology & Operations) Component 3

1.1 Purpose and Anticipated Benefits 3

1.2 Scope 3

1.2.1 In-Scope 4

1.2.2 Out-of-Scope 4

1.3 Relationship to the PCTF 4

2. Infrastructure (Technology & Operations) Conventions 5

2.1 Terms and Definitions 6

2.2 Abbreviations 6

3. Conformance Criteria coverage 6

3.1 Policy and plans 7

3.2 Technology criteria 8

3.3 Technology Operations criteria 8

4. Introduction to the PCTF Infrastructure (Technology & Operations) Conformance Profile 9

4.1 Conformance Criteria Keywords 9

4.2 Infrastructure Conventions 10

5. Infrastructure Component Conformance Criteria 10

6. References 64

7. Revision History 65

1. Introduction to the PCTF Infrastructure (Technology & Operations) 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 Purpose and Anticipated Benefits

The objective of the PCTF Infrastructure (Technology & Operations) Component is to identify the operational policies, plans, technology and technology operations requirements to support implementation of the principles of the PCTF Profiles in the context of a Digital Identity Ecosystem.

A process that has been certified is a Trusted Process that can be relied on by other participants of the PCTF. The PCTF Conformance Criteria are intended to complement existing privacy legislation and regulations; DIACC-certified participants in the Digital Identity Ecosystem are expected to meet the applicable legislated requirements and regulations in their jurisdictions.

The PCTF Infrastructure (Technology & Operations) Component defines:

- The formal policy and plan artifacts that form the basis of a conforming technology installation and its technology support operations.
- The high-level technology and technology tool capabilities required to support a technology infrastructure delivering service to a Digital Identity Ecosystem.
- The technology support operational tools and characteristics to support an installed technology infrastructure delivering service to a Digital Identity Ecosystem.

1.2 Scope

This section defines the scope of the PCTF Infrastructure (Technology & Operations) Component. In-scope requirements are identified at a high level to illustrate scope, and detailed requirements are elaborated in the PCTF Infrastructure (Technology & Operations) Conformance Profile.

1.2.1 In-Scope

This PCTF component will specify conformance criteria that provide general requirements and guidelines regarding the trustworthiness of the IT infrastructure that enables implementation and delivery of the trusted processes defined in other PCTF components. The component's primary subject areas are the security and integrity of technical components. Within these areas of interest, the component's scope includes:

- IT security (as a general consideration).
- Oversight of data collection, validation, storage, and accessibility.
- Audit and logging.
- Prevention of, and response to, IT events that compromise the trustworthiness of the Digital Identity Ecosystem.
- Policies and plans supporting the trustworthy management of technology and technology operations.

1.2.2 Out-of-Scope

The scope of this PCTF component does not include:

- The suitability of specific products to support a given trusted process.
- The suitability of standards, processes, technologies, or technology protocols that may be specific to, or mandated by, an individual Digital Identity Ecosystem.
- Mandating the use of a specific set of standard practices or frameworks to govern technology operations (e.g. IT Infrastructure Library <<ITIL>>, Control Objectives for Information Technology <<COBIT>>).

1.3 Relationship to the PCTF

The PCTF 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.

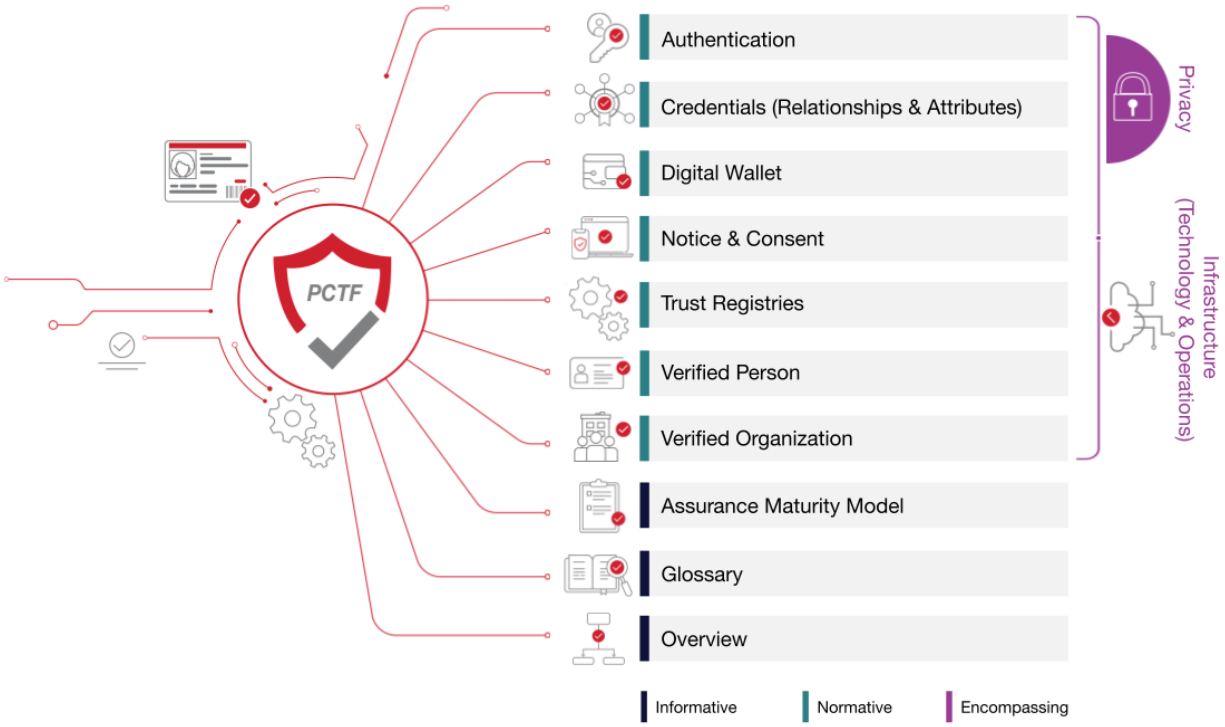

Figure 1. Components of the Pan-Canadian Trust Framework

PCTF 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.

2. Infrastructure (Technology & Operations) Conventions

This section describes and defines key terms and concepts used in the PCTF Infrastructure (Technology & Operations) Component. This information is provided to ensure consistent use and interpretation of terms throughout this component.

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 and the PCTF Glossary are capitalized throughout this document.
- Hypertext Links – hypertext links may be embedded in electronic versions of this document for reader reference. 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.

Conformance Criteria

Requirements developed for each of the PCTF Components and used as the basis to assess compliance.

Digital Identity Ecosystem

An interconnected ecosystem for the exchange and verification of digital Identity Information, involving public and private sector Organizations that comply with a common Trust Framework for the management and use of digital identities, and the Subjects of those digital identities.

Personal Information

Any factual or subjective information, recorded or not, about an identifiable individual (Source: PIPEDA in Brief, Office of the Privacy Commissioner of Canada - What is personal information?).

2.2 Abbreviations

The following abbreviations appear throughout this PCTF component:

- DIACC – Digital ID & Authentication Council of Canada
- COBIT - Control Objectives for Information Technology
- ENISA - European Union Agency for Cybersecurity
- FEDRAMP - Federal Risk and Authorization Management Program
- ITIL - IT Infrastructure Library
- NIST - National Institute of Standards and Technology
- PCTF – Pan-Canadian Trust Framework

3. Conformance Criteria coverage

Conformance criteria are elaborated in detail in the PCTF Infrastructure (Technology & Operations) Conformance Profile. Requirements were designed to reflect the capabilities and characteristics found in technology operations and governance standards (e.g., ITIL, COBIT) without being so prescriptive that a specific standard is required.

Similarly, public sector standards bodies and their implementation guidance were drawn upon to help define some of the detailed requirements in the Conformance Criteria. These include National Institute of Standards and Technology (NIST) and Federal Risk and Authorization Management Program (FEDRAMP) in the US, European Union Agency for Cybersecurity (ENISA) in Europe, and various Federal Government Directives in Canada. The approach was to derive inspiration from some of the common guidance for technology implementation and management while ensuring that the PCTF Conformance Criteria were generic enough to co-exist in any public or private sector domain.

It is worth noting that the PCTF Infrastructure (Technology & Operations) Conformance Criteria are described in a generic fashion, focusing more on the capabilities required to operate a trusted infrastructure as a platform for the delivery of other conforming services within the PCTF. It is expected that organizations wishing to participate in a specific Digital Identity Ecosystem will have additional specific technology and technology operations requirements imposed upon them by the Digital Identity Ecosystem. The identification of a required specific technology product, protocol, or third-party operational standard in an individual Digital Identity Ecosystem is not within the scope of this profile.

The Criteria are organized into three broad categories. These are:

- Policies and Plans - capture the key formal artifacts that elaborate the organization's consistent approach to instantiating and managing the technology and system components that fulfill the role that organization is playing in the Digital Identity Ecosystem.
- Technology – identifies the characteristics and capabilities of required technology components.
- Operations – identifies the characteristics and capabilities required of the operational framework and toolset utilized to play a defined role within a Digital Identity Ecosystem.

3.1 Policy and plans

The foundation of the technology component of an enterprise architecture is a comprehensive set of organization policies and plans clearly mapped to the business objectives identified in the business components of the enterprise architecture. This profile identifies requirements for formal artifacts and their continuous management in the areas of:

- Risk assessment;
- Audit and accountability;
- Security assessment;
- Disaster or contingency planning;

- Identification and authentication;
- Systems and communication protection;
- Incident response;
- System and information integrity;
- Configuration management;
- Information management;
- System maintenance;
- Technical access control;
- Physical access control; and,
- Personnel security.

At a high level, the most important takeaway from this set of criteria is the need for orderly planning that starts with the identification of objectives in policy statements, supported by formal plans that govern the implementation and operation of technology.

3.2 Technology criteria

These criteria focus on identifying the generic tools and technology capabilities required to support an operating infrastructure delivering PCTF conforming services. Specific technology products or protocols are not identified as these tend to vary depending on the specific trusted process being delivered in an individual Digital Identity Ecosystem. It is expected that organizations will have additional specific requirements in this area imposed by the Digital Identity Ecosystem in which they wish to operate.

Also, the capabilities that are specific to other PCTF trusted processes (i.e., Authentication, Privacy, Verified Person, etc.) are not elaborated in this Profile. Those criteria are identified in the subject matter-specific PCTF Conformance Profiles. There are several cross-references to other Conformance Profiles where appropriate.

3.3 Technology Operations criteria

The third category of Conformance Criteria identifies the technology operations and support capabilities required to operate a PCTF conforming infrastructure. Aligned with the policies and plans identified earlier, these capabilities represent the ongoing technology, support and operational characteristics required to deliver on the enterprise capabilities identified in the policies and plans associated with a comprehensive enterprise architecture.

4. Introduction to the PCTF Infrastructure (Technology & Operations) Conformance Profile

This document specifies the Conformance Criteria of the PCTF Infrastructure (Technology & Operations) Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the PCTF, including contextual information and the PCTF goals and objectives, please see the PCTF Model Overview.

The Conformance Criteria for the Infrastructure Component specify the characteristics of the technology and technology operations supporting the implementation of systems delivering service compliant with PCTF Profiles. The criteria are expressed in generic terms, recognizing that specific technologies or technology characteristics (e.g., protocols) are likely to be mandated, and will vary, within each individual Digital Identity Ecosystem.

Note: These conformance criteria do not replace existing policy or regulation; organizations are expected to comply with relevant legislation, policy, and regulations in their jurisdiction.

4.1 Conformance Criteria Keywords

The following keywords are used in the conformance criteria to indicate their precedence and/or general rigidity, and are to be interpreted as:

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

4.2 Infrastructure Conventions

Each PCTF component includes conventions that ensure consistent use and interpretation of terms and concepts appearing in the component. The PCTF Infrastructure (Technology & Operations) 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

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 Infrastructure Component Overview and the PCTF Glossary apply. Key terms and concepts described and defined in this section, or the PCTF Infrastructure 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. Infrastructure Component Conformance Criteria

The Conformance Criteria listed below are organized into three broad categories. These are:

- **POL** – policy and plan requirements that define and support the technology architecture under which the system components participating in the Digital Identity Ecosystem operate.
- **TECH** – technology-related requirements
- **OPS** – technology operations

For ease of use, the Criteria are numbered within their section and may be referred to using these identifiers (e.g., the first criterion in the POL section may be referenced as POL-1).

Criteria scope may be assumed to apply only to the technology or system components leveraged by an organization in its provision or consumption of service within a Digital Identity Ecosystem.

Notes:

- Assurance levels associated with the individual criteria below do not correspond to traditional authentication, identity, and credential assurance levels. Instead, they are intended to indicate a level of technology and infrastructure maturity in support of those assurances. For example, an organization supporting a Level 2 Identity Assurance process should meet all of the criteria listed as appropriate for Level 2 below.
- Level 4 is out of scope for this version. Reference is retained as a placeholder for future development.

Note: It is important to note that these represent capabilities to be addressed and should not be interpreted as individual policy or plan artifacts. Many of these capabilities are typically combined and addressed in a single artifact.

Reference	**Conformance Criteria**				
POL	**Requirements relating to the technology policies and plans required to support the infrastructure leveraged to service the Digital Identity Ecosystem.**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Any policies, plans, or artifacts that are required in any other criteria of this profile **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements.	X	X	X	
2	Business capability and service architecture **MUST** be formalized and documented.	X	X	X	
3	A Risk Assessment policy **MAY** be developed, documented, and disseminated within the organization.	X			
4	A Risk Assessment policy **MUST** be developed, documented, and disseminated within the organization.		X	X	

5	A Risk Assessment policy **MAY** address, but is not limited to the following: • Context and priorities for managing risk (including security and privacy risk). This can include evaluation of risk at organizational level, business process level, and/or system level. • Categorization of system(s) and the information processed, stored, and transmitted by the system(s) based on an analysis of the impact of loss. • Identification of key risk factors, including but not limited to: impact of loss; threats, vulnerabilities, and likelihood of occurrence.	X			
6	A Risk Assessment policy **SHOULD** address, but is not limited to the following: • Context and priorities for managing risk (including security and privacy risk). This can include evaluation of risk at organizational level, business process level, and/or system level. • Categorization of system(s) and the information processed, stored, and transmitted by the system(s) based on an analysis of the impact of loss. • Identification of key risk factors, including but not limited to: impact of loss; threats, vulnerabilities, and likelihood of occurrence.		X	X	

7	A Risk Assessment plan **MAY** address, but is not limited to, the following: • A plan for designing system controls to mitigate risk to acceptable levels. • A plan to create/maintain implementation guide(s) and standard operating procedure(s) for operating controls. • A plan to assess controls to determine if they are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying entity's requirements (including security and privacy requirements). • Plans to monitor, and report on, the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation conducting risk assessments and impact analysis.	X			

8	A Risk Assessment plan **SHOULD** address, but is not limited to the following: • A plan for designing system controls to mitigate risk to acceptable levels. • A plan to create/maintain implementation guide(s) and standard operating procedure(s) for operating controls. • A plan to assess controls to determine if they are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying Entity's requirements (including security and privacy requirements). • Plans to monitor, and report on, the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation conducting risk assessments and impact analysis.		X	X	
9	An Audit and Accountability policy **MAY** be developed, documented, and disseminated within the organization.	X			
10	An Audit and Accountability policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
11	An Audit and Accountability plan **MAY** be developed, documented, and disseminated within the organization.	X			
12	An Audit and Accountability plan **MUST** be developed, documented, and disseminated within the organization.		X	X	

13	An Audit and Accountability plan **MAY** address and detail, but is not limited to, the following: • Data owners; • Auditable events; • Content of audit records; • Audit storage capacity; • Response to audit processing failures; • Audit review, analysis, and reporting processes; • Protection of audit information; • Audit record retention and disposal.	X			
14	An Audit and Accountability plan **SHOULD** address and detail, but is not limited to, the following: • Data owners; • Auditable events; • Content of audit records; • Audit storage capacity; • Response to audit processing failures; • Audit review, analysis, and reporting processes; • Protection of audit information; • Audit record retention and disposal.		X	X	
15	A Security Assessment policy **MAY** be developed, documented, and disseminated within the organization.	X			
16	A Security Assessment policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
17	A Security Assessment plan **MAY** be developed, documented, and disseminated within the organization.	X			
18	A Security Assessment plan **MUST** be developed, documented, and disseminated within the organization.		X	X	

19	A Security Assessment plan **MAY** detail, but is not limited to, the following: • The security controls under assessment; • Assessment tools; • Roles and responsibilities; • Security assessment procedures; • Assessment review, analysis, and reporting.	X			
20	A Security Assessment plan **SHOULD** detail, but is not limited to, the following: • The security controls under assessment; • Assessment tools; • Roles and responsibilities; • Security assessment procedures; • Assessment review, analysis, and reporting.		X	X	
21	An IT Contingency policy **MAY** be developed, documented, and disseminated within the organization.	X			
22	An IT Contingency policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
23	An IT Contingency plan **MAY** be developed, documented, and disseminated within the organization.	X			
24	An IT Contingency plan **MUST** be developed, documented, and disseminated within the organization.		X	X	

25	An IT Contingency plan **MAY** detail, but is not limited to, the following: • Essential missions and business functions and associated contingency requirements; • Recovery objectives, restoration priorities, and metrics; • Contingency roles, responsibilities, and assigned individuals with contact information; • Maintenance of essential missions and business functions despite an information system disruption, compromise, or failure; • Full information system restoration, including system data and personal information, without deterioration of the security safeguards originally planned and implemented.	X			
26	An IT Contingency plan **SHOULD** detail, but is not limited to, the following: • Essential missions and business functions and associated contingency requirements; • Recovery objectives, restoration priorities, and metrics; • Contingency roles, responsibilities, and assigned individuals with contact information; • Maintenance of essential missions and business functions despite an information system disruption, compromise, or failure; • Full information system restoration, including system data and personal information, without deterioration of the security safeguards originally planned and implemented.		X	X	

27	An Identification and Authentication policy **MAY** be developed, documented, and disseminated within the organization.	X			
28	An Identification and Authentication policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
29	An Identification and Authentication plan **MAY** be developed, documented, and disseminated within the organization.	X			
30	An Identification and Authentication plan **MUST** be developed, documented, and disseminated within the organization.		X	X	
31	An Identification and Authentication plan **MAY** detail, but is not limited to, the following: • Roles, and responsibilities; • Identification and authentication of organizational users; • Identification and authentication of non-organizational users; • Identification and authentication of devices; • Identifier management; • Authenticator management and feedback.	X			
32	An Identification and Authentication plan **SHOULD** detail, but is not limited to, the following: • Roles, and responsibilities; • Identification and authentication of organizational users; • Identification and authentication of non-organizational users; • Identification and authentication of devices; • Identifier management; • Authenticator management and feedback.		X	X	

33	A System and Communication Protection Policy **MAY** be developed, documented, and disseminated within the organization.	X			
34	A System and Communication Protection Policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
35	A System and Communication Protection Plan **MAY** be developed, documented, and disseminated within the organization.	X			
36	A System and Communication Protection Plan **MUST** be developed, documented, and disseminated within the organization.		X	X	
37	A System and Communication Protection plan **MAY** detail, but is not limited to, the following: • Application partitioning; • Information in shared resources; • Denial of service protection; • Boundary protection; • Transmission confidentiality and integrity; • Protection of information at rest; • Session termination; • Cryptographic key management; • Cryptographic protection; • Collaborative computing devices; • Session authenticity; • Process isolation.	X			

38	A System and Communication Protection plan **SHOULD** detail, but is not limited to, the following: • Application partitioning; • Information in shared resources; • Denial of service protection; • Boundary protection; • Transmission confidentiality and integrity; • Protection of information at rest; • Session termination; • Cryptographic key management; • Cryptographic protection; • Collaborative computing devices; • Session authenticity; • Process isolation.		X	X	
39	An Incident Response policy **MAY** be developed, documented, and disseminated within the organization.	X			
40	An Incident Response policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
41	An Incident Response plan **MAY** be developed, documented, and disseminated within the organization.	X			
42	An Incident Response plan **MUST** be developed, documented, and disseminated within the organization.		X	X	

43	An Incident Response plan **MAY** detail, but is not limited to, the following: • A roadmap for implementing incident response capability; • Unique requirements of the organization, which relate to mission, size, structure, and functions; • Reportable incidents; • Metrics for measuring the incident response capability within the organization; • The resources and management support needed to effectively maintain the incident response capability; • The procedures necessary for identification, containment, eradication, recovery, reporting, and plan revision.	X			
44	An Incident Response plan **SHOULD** detail, but is not limited to, the following: • Roles and responsibilities; • A roadmap for implementing incident response capability; • Unique requirements of the organization, which relate to mission, size, structure, and functions; • Reportable incidents; • Metrics for measuring the incident response capability within the organization; • The resources and management support needed to effectively maintain the incident response capability; • The procedures necessary for identification, containment, eradication, recovery, reporting, and plan revision.		X	X	

45	A System and Information Integrity policy **MAY** be developed, documented, and disseminated within the organization that: • Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; • Is consistent with applicable laws, regulations, policies, standards, and guidelines; • Designates an organization-defined official to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; • Review and update the current system and information integrity related policies and procedures at a defined frequency or due to defined events. **Note:** Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, orders in council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.	X			

46	A System and Information Integrity policy **MUST** be developed, documented, and disseminated within the organization that: • Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; • Is consistent with applicable laws, regulations, policies, standards, and guidelines; • Designates an organization-defined official to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; • Review and update the current system and information integrity related policies and procedures at a defined frequency or due to defined events. **Note:** Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, orders in council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.		X	X	
47	A System and Information Integrity plan **MAY** be developed, documented, and disseminated within the organization.	X			
48	A System and Information Integrity plan **MUST** be developed, documented, and disseminated within the organization.		X	X	

49	A System and Information integrity plan **MAY** detail, but is not limited to, the following: • Identification, reporting and correction of system flaws; • Testing of software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Installation of security-relevant software and firmware updates within a defined period of time; • Incorporation of flaw remediation into the organizational configuration management process.	X			
50	A System and Information integrity plan **MUST** detail, but is not limited to, the following: • Identification, reporting and correction of system flaws; • Testing of software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Installation of security-relevant software and firmware updates within a defined period of time; • Incorporation of flaw remediation into the organizational configuration management process.		X	X	
51	A Configuration Management policy **MAY** be developed, documented, and disseminated within the organization.	X			
52	A Configuration Management policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
53	A Configuration Management plan **MAY** be developed, documented, and disseminated within the organization.	X			

54	A Configuration Management plan **MUST** be developed, documented, and disseminated within the organization.		X	X	
55	A Configuration Management plan **MAY** detail, but is not limited to the following: • Roles, responsibilities, and configuration management processes and procedures; • Processes for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; • The configuration items, and any related baselines to be managed under the plan.	X			
56	A Configuration Management plan **SHOULD** detail, but is not limited to the following: • Roles, responsibilities, and configuration management processes and procedures; • Processes for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; • The configuration items, and any related baselines to be managed under the plan.		X	X	
57	An Information Management and Privacy Protection policy **MAY** be developed, documented, and disseminated within the organization.	X			
58	An Information Management and Privacy Protection policy **MUST** be developed, documented, and disseminated within the organization.		X	X	

59	An Information Management and Privacy Protection plan **MAY** be developed, documented, and disseminated within the organization.	X			
60	An Information Management and Privacy Protection plan **MUST** be developed, documented, and disseminated within the organization.		X	X	
61	An Information Management and Privacy Protection plan **MAY** detail, but is not limited to, the following: • Roles and responsibilities; • Data definitions; • Information management and privacy protection principles; • Governing authorities and frameworks; • Breach reporting.	X			
62	An Information Management and Privacy Protection plan **SHOULD** detail, but is not limited to, the following: • Roles and responsibilities; • Data definitions; • Information management and privacy protection principles; • Governing authorities and frameworks; • Breach reporting.		X	X	
63	A System Maintenance policy **MAY** be developed, documented, and disseminated within the organization.	X			
64	A System Maintenance policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
65	A System Maintenance plan **MAY** be developed, documented, and disseminated within the organization.	X			

66	A System Maintenance plan **MUST** be developed, documented, and disseminated within the organization.		X	X	
67	A System Maintenance plan **MAY** detail, but is not limited to, the following: • Scheduling, documenting and reviewing maintenance records; • The use of automated maintenance activities; • Inspection, restriction, usage, and update of maintenance tools; • Non-local maintenance activities; • Timeliness of maintenance.	X			
68	A System Maintenance plan **SHOULD** detail, but is not limited to, the following: • Scheduling, documenting and reviewing maintenance records; • The use of automated maintenance activities; • Inspection, restriction, usage, and update of maintenance tools; • Non-local maintenance activities; • Timeliness of maintenance.		X	X	
69	A Technical Access Control policy **MAY** be developed, documented, and disseminated within the organization.	X			
70	A Technical Access Control policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
71	A Technical Access Control plan **MAY** be developed, documented, and disseminated within the organization.	X			
72	A Technical Access Control plan **MUST** be developed, documented, and disseminated within the organization.		X	X	

73	A Technical Access Control plan **MAY** detail, but is not limited to, the following: • Account management; • Access enforcement; • Information flow enforcement; • Separation of duties; • Least privilege; • Unsuccessful login attempts; • Remote access; • Wireless access; • System notifications; • Session management; • Security and privacy attributes; • Use of external systems; • Data mining protection.	X			
74	A Technical Access Control plan **SHOULD** detail, but is not limited to, the following: • Account management; • Access enforcement; • Information flow enforcement; • Separation of duties; • Least privilege; • Unsuccessful login attempts; • Remote access; • Wireless access; • System notifications; • Session management; • Security and privacy attributes; • Use of external systems; • Data mining protection.		X	X	
75	A Physical Access Control policy **MAY** be developed, documented, and disseminated within the organization.	X			
76	A Physical Access Control policy **MUST** be developed, documented, and disseminated within the organization.		X	X	

77	A Physical Access Control plan **MAY** be developed, documented, and disseminated within the organization.	X			
78	A Physical Access Control plan **MUST** be developed, documented, and disseminated within the organization.		X	X	
79	A Physical Access Control plan **SHOULD** detail, but is not limited to, the following: • Authorization; • Control management; • Monitoring; • Visitor Access; • Asset monitoring and tracking; • Alternative work sites.	X			
80	A Physical Access Control plan **SHOULD** detail, but is not limited to, the following: • Authorization; • Control management; • Monitoring; • Visitor Access; • Asset monitoring and tracking; • Alternative work sites.		X	X	
81	A Personnel Security policy **MAY** be developed, documented, and disseminated within the organization.	X			
82	A Personnel Security policy **MUST** be developed, documented, and disseminated within the organization.		X	X	
83	A Personnel Security plan **MAY** be developed, documented, and disseminated within the organization.	X			
84	A Personnel Security plan **MUST** be developed, documented, and disseminated within the organization.		X	X	

85	A Personnel Security plan **MAY** detail, but is not limited to, the following: • Personnel screening; • Personnel termination; • Personnel transfer; • Access agreements including non-disclosure, acceptable use, conflict of interest, etc.; • External personnel security.	X			
86	A Personnel Security plan **SHOULD** detail, but is not limited to, the following: • Personnel screening; • Personnel termination; • Personnel transfer; • Access agreements including non-disclosure, acceptable use, conflict of interest, etc.; • External personnel security.		X	X	
Reference	**Conformance Criteria**				
TECH	**Technology requirements required by organizations servicing the Digital Identity Ecosystem**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Tools and techniques **MAY** be in place that provide malicious code protection mechanisms at information system entry and exit points (e.g., firewalls, gateways, host intrusion detection systems) to detect and eradicate malicious code.	X			
2	Tools and techniques **SHOULD** be in place that provide malicious code protection mechanisms at information system entry and exit points (e.g., firewalls, gateways, host intrusion detection systems) to detect and eradicate malicious code.		X		

3	Tools and techniques **MUST** be in place that provide malicious code protection mechanisms at information system entry and exit points (e.g., firewalls, gateways, host intrusion detection systems) to detect and eradicate malicious code.			X	
4	Malicious code protection tools **MAY** update malicious code protection mechanisms in alignment with policy.	X			
5	Malicious code protection tools **SHOULD** update malicious code protection mechanisms in alignment with policy.		X		
6	Malicious code protection tools **MUST** update malicious code protection mechanisms in alignment with policy.			X	
7	The information system **SHOULD** ensure the confidentiality and integrity of Digital Identity information at rest and in transit. Please refer to the PCTF Privacy Conformance Profile for additional related requirements in this area.	X			
8	The information system **MUST** ensure the confidentiality and integrity of Digital Identity information at rest and in transit. Please refer to the PCTF Privacy Conformance Profile for additional related requirements in this area.		X	X	
9	The information system **MAY** ensure the authenticity of communication sessions (e.g., unique randomized session identifiers, session identifier invalidation upon logout, proper application of approved encryption certificates based on enterprise policy).	X			
10	The information system **SHOULD** ensure the authenticity of communication sessions (e.g., unique randomized session identifiers, session identifier invalidation upon logout, proper application of approved encryption certificates based on enterprise policy).		X		

11	The information system **MUST** ensure the authenticity of communication sessions (e.g., unique randomized session identifiers, session identifier invalidation upon logout, proper application of approved encryption certificates based on enterprise policy).			X	
12	The information system **MAY** invalidate session identifiers upon user logout or other session termination. Please also refer to the Session Termination section of the PCTF Authentication Conformance Profile for additional context.	X			
13	The information system **SHOULD** invalidate session identifiers upon user logout or other session termination. Please also refer to the Session Termination section of the PCTF Authentication Conformance Profile for additional context.		X		
14	The information system **MUST** invalidate session identifiers upon user logout or other session termination. Please also refer to the Session Termination section of the PCTF Authentication Conformance Profile for additional context.			X	
15	The organization **MAY** issue public key certificates in accordance with organization-defined certificate policy or obtain public key certificates from a well-known public trust anchor certificate authority.	X			
16	The organization **MUST** issue public key certificates in accordance with organization-defined certificate policy or obtain public key certificates from a well-known public trust anchor certificate authority.		X	X	
17	The information system **MAY** terminate the network connection associated with a user session, or system-to-system communication session, at the end of the session or after a predefined period of inactivity.	X			

18	The information system **SHOULD** terminate the network connection associated with a user session, or system-to-system communication session, at the end of the session or after a predefined period of inactivity.		X		
19	The information system **MUST** terminate the network connection associated with a user session, or system-to-system communication session, at the end of the session or after a predefined period of inactivity.			X	
20	The organization **MAY** employ integrity verification tools to detect unauthorized changes to software, firmware, and information.	X			
21	The organization **SHOULD** employ integrity verification tools to detect unauthorized changes to software, firmware, and information.		X	X	
22	Tools **MAY** be in place to monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	X			
23	Tools **SHOULD** be in place to monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.		X		
24	Tools **MUST** be in place to monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.			X	

25	Monitoring and alarming tools, devices, and techniques **MAY** be employed that will monitor the information system to: • Detect attacks and indicators of potential attacks; • Detect unauthorized local, network, and remote connections; • Detect inbound and outbound communications traffic for unusual or unauthorized activities or conditions; • Mitigate the potential for insider threats and data exfiltration. Additional guidance can be found in the Threat Monitoring section of the PCTF Authentication Conformance Profile.	X			
26	Monitoring and alarming tools, devices, and techniques **SHOULD** be employed that will monitor the information system to: • Detect attacks and indicators of potential attacks; • Detect unauthorized local, network, and remote connections; • Detect inbound and outbound communications traffic for unusual or unauthorized activities or conditions; • Mitigate the potential for insider threats and data exfiltration. Additional guidance can be found in the Threat Monitoring section of the PCTF Authentication Conformance Profile.		X		

27	Monitoring and alarming tools, devices, and techniques **MUST** be employed that will monitor the information system to: • Detect attacks and indicators of potential attacks; • Detect unauthorized local, network, and remote connections; • Detect inbound and outbound communications traffic for unusual or unauthorized activities or conditions; • Mitigate the potential for insider threats and data exfiltration. Additional guidance can be found in the Threat Monitoring section of the PCTF Authentication Conformance Profile.			X	
28	Boundary protection tools, devices, and techniques **MAY** be employed that will: • Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; • Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and • Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	X			

29	Boundary protection tools, devices, and techniques **SHOULD** be employed that will: • Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; • Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and • Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.		X		
30	Boundary protection tools, devices, and techniques **MUST** be employed that will: • Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; • Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and • Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.			X	
31	The organization **MAY** employ tools and techniques to protect against or limit the effects of denial of service attacks.	X			
32	The organization **SHOULD** employ tools and techniques to protect against or limit the effects of denial of service attacks.		X		

33	The organization **MUST** employ tools and techniques to protect against or limit the effects of denial of service attacks.			X	
34	The information system **MAY** uniquely identify and authenticate non-organizational users, or processes acting on behalf of non-organizational users, where authentication is appropriate.	X			
35	The information system **SHOULD** uniquely identify and authenticate non-organizational users, or processes acting on behalf of non-organizational users, where authentication is appropriate.		X		
36	The information system **MUST** uniquely identify and authenticate non-organizational users, or processes acting on behalf of non-organizational users, where authentication is appropriate.			X	
37	The organization **MAY** ensure that unencrypted static authenticators are not embedded in applications or access scripts, or stored on function keys. Additional guidance can be found in the credential issuance and authentication sections of the PCTF Authentication Conformance profile.	X			
38	The organization **MUST** ensure that unencrypted static authenticators are not embedded in applications or access scripts, or stored on function keys. Additional guidance can be found in the credential issuance and authentication sections of the PCTF Authentication Conformance profile.		X	X	

39	The organization **MAY** employ automated tools to determine if password authenticators are sufficiently strong to satisfy the requirements of the organization's security policy. Additional guidance can be found in the credential issuance and authentication sections of the PCTF Authentication Conformance profile.	X			
40	The organization **SHOULD** employ automated tools to determine if password authenticators are sufficiently strong to satisfy the requirements of the organization's security policy. Additional guidance can be found in the credential issuance and authentication sections of the PCTF Authentication Conformance profile.		X	X	
41	The organization **MAY** implement tools to defend against authentication replay and secret guessing attacks to gain network access. Additional guidance can be found in the Threat Mitigation section of the PCTF Authentication Conformance Profile.	X			
42	The organization **SHOULD** implement tools to defend against authentication replay and secret guessing attacks to gain network access. Additional guidance can be found in the Threat Mitigation section of the PCTF Authentication Conformance Profile.		X		

43	The organization **MUST** implement tools to defend against authentication replay and secret guessing attacks to gain network access. Additional guidance can be found in the Threat Mitigation section of the PCTF Authentication Conformance Profile.			X	
44	The organization **MAY** analyze changes to the information system to determine potential security impacts prior to change implementation.	X			
45	The organization **SHOULD** analyze changes to the information system to determine potential security impacts prior to change implementation.		X		
46	The organization **MUST** analyze changes to the information system to determine potential security impacts prior to change implementation.			X	
47	The organization **MAY** have automated intrusion detection and alerting technology in place for all technology components used in the delivery or consumption of digital identity	X			
48	The organization **SHOULD** have automated intrusion detection and alerting technology in place for all technology components used in the delivery or consumption of digital identity		X		
49	The organization **MUST** have automated intrusion detection and alerting technology in place for all technology components used in the delivery or consumption of digital identity			X	
50	The organization **MAY** proactively assess and maintain the adequacy of systems and services, including system resource levels and the currency of hardware and operating system patch levels.	X			

51	The organization **MUST** proactively assess and maintain the adequacy of systems and services, including system resource levels and the currency of hardware and operating system patch levels.		X	X	
52	The information system **MAY** have security safeguards to protect its memory from unauthorized code execution.	X			
53	The information system **SHOULD** have security safeguards to protect its memory from unauthorized code execution.		X	X	
54	The information system **MAY** deploy cryptographic tools and other data protection methods and technology to ensure privacy is maintained during information exchanges. Additional guidance can be found in the PCTF Privacy Conformance Profile.	X			
55	The information system **SHOULD** deploy cryptographic tools and other data protection methods and technology to ensure privacy is maintained during information exchanges. Additional guidance can be found in the PCTF Privacy Conformance Profile.		X		
56	The information system **MUST** deploy cryptographic tools and other data protection methods and technology to ensure privacy is maintained during information exchanges. Additional guidance can be found in the PCTF Privacy Conformance Profile.			X	
57	Cryptographic tools used to ensure privacy is maintained during information exchanges **MAY** meet an industry-recognized validation standard (e.g., FIPS 140-2 or equivalent).	X			

58	Cryptographic tools used to ensure privacy is maintained during information exchanges **SHOULD** meet an industry-recognized validation standard (e.g., FIPS 140-2 or equivalent).		X	X	
	Conformance Criteria				
OPS	**Operational requirements for organizations servicing the Digital Identity Ecosystem.**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	There **MAY** be an operational standard requiring developers to follow a documented development process that explicitly addresses security requirements, identifies the technology standards and toolsets to be used, and identifies the specific work tool configurations to be used.	X			
2	There **SHOULD** be an operational standard requiring developers to follow a documented development process that explicitly addresses security requirements, identifies the technology standards and toolsets to be used, and identifies the specific work tool configurations to be used.		X		
3	There **MUST** be an operational standard requiring developers to follow a documented development process that explicitly addresses security requirements, identifies the technology standards and toolsets to be used, and identifies the specific work tool configurations to be used.			X	
4	The organization **MAY** manage the system components using its defined system development life cycle that incorporates security concerns.	X			
5	The organization **SHOULD** manage the system components using its defined system development life cycle that incorporates security concerns.		X		

6	The organization **MUST** manage the system components using its defined system development life cycle that incorporates security concerns.			X	
7	The organization **MAY** have formal information retention and disposition schedules subject to monitoring and audit to ensure compliance with its information management plan.	X			
8	The organization **SHOULD** have formal information retention and disposition schedules subject to monitoring and audit to ensure compliance with its information management plan.		X		
9	The organization **MUST** have formal information retention and disposition schedules subject to monitoring and audit to ensure compliance with its information management plan.			X	
10	Formal technology governance systems and processes (e.g., Governance Risk and Compliance/GRC or Integrated Risk Management/IRM) **MAY** be in place that include ongoing monitoring and activity audit controls.	X			
11	Formal technology governance systems and processes (e.g., Governance Risk and Compliance/GRC or Integrated Risk Management/IRM, governance task and workflow management, change management) **SHOULD** be in place that include ongoing monitoring and activity audit controls.		X	X	
12	The organization **MAY** periodically test restoration/recovery of information system components as per requirements defined in the contingency plan.	X			
13	The organization **SHOULD** periodically test restoration/recovery of information system components as per requirements defined in the contingency plan.		X		

14	The organization **MUST** periodically test restoration/recovery of information system components as per requirements defined in the contingency plan.			X	
15	Full testing, evaluation, and update of the contingency plan **MAY** be performed on a regular (e.g., biennial or annual preferred) basis.	X			
16	Full testing, evaluation, and update of the contingency plan **SHOULD** be performed on a regular (e.g., biennial or annual preferred) basis.		X		
17	Full testing, evaluation, and update of the contingency plan **MUST** be performed on a regular (e.g., biennial or annual preferred) basis.			X	
18	Comprehensive automated backup procedures **MAY** be in place. This capability includes backup of: • User-level information; • System-level information; • System and security documentation.	X			
19	Comprehensive automated backup procedures **SHOULD** be in place. This capability includes backup of: • User-level information; • System-level information; • System and security documentation.		X		
20	Comprehensive automated backup procedures **MUST** be in place. This capability includes backup of: • User-level information; • System-level information; • System and security documentation.			X	

21	Backups of critical system software and operational data **MAY** be stored in a facility that is physically separate from the operational system.	X			
22	Backups of critical system software and operational data **SHOULD** be stored in a facility that is physically separate from the operational system.		X	X	
23	Processes and procedures **MAY** be in place to protect the confidentiality, integrity, and availability of backup information at storage locations in alignment with governance and risk management policy.	X			
24	Processes and procedures **MUST** be in place to protect the confidentiality, integrity, and availability of backup information at storage locations in alignment with governance and risk management policy.		X	X	
25	There **MAY** be a program of continuous vulnerability testing of system and software components leveraged in the delivery of services to the Digital Identity Ecosystem.	X			
26	There **SHOULD** be a program of continuous vulnerability testing of system and software components leveraged in the delivery of services to the Digital Identity Ecosystem.		X		
27	There **MUST** be a program of continuous vulnerability testing of system and software components leveraged in the delivery of services to the Digital Identity Ecosystem.			X	
28	Vulnerability scanning techniques, and tools that readily update the vulnerabilities to be scanned, **MAY** be employed and operated in an automated fashion.	X			
29	Vulnerability scanning techniques, and tools that readily update the vulnerabilities to be scanned, **SHOULD** be employed and operated in an automated fashion.		X	X	

30	The organization **MAY** conduct regular penetration testing of all components leveraged in the delivery of services to the Digital Identity Ecosystem.	X			
31	The organization **SHOULD** conduct regular penetration testing of all components leveraged in the delivery of services to the Digital Identity Ecosystem.		X		
32	The organization **MUST** conduct regular penetration testing of all components leveraged in the delivery of services to the Digital Identity Ecosystem.			X	
33	Remote access methods **MAY** be controlled and monitored.	X			
34	Remote access methods **SHOULD** be controlled and monitored.		X		
35	Remote access methods **MUST** be controlled and monitored.			X	
36	Remote access **MAY** be routed through managed network access control points.	X			
37	Remote access **SHOULD** be routed through managed network access control points.		X		
38	Remote access **MUST** be routed through managed network access control points.			X	
39	There **MAY** be automated systems (e.g., provisioning, rights assignment and management) to support the management of information system accounts.	X			
40	There **SHOULD** be automated systems (e.g., provisioning, rights assignment and management) to support the management of information system accounts.		X	X	
41	Processes **MAY** be in place to automatically disable inactive accounts after a defined period of inactivity based on information system control policy.	X			

42	Processes **SHOULD** be in place to automatically disable inactive accounts after a defined period of inactivity based on information system control policy.		X		
43	Processes **MUST** be in place to automatically disable inactive accounts after a defined period of inactivity based on information system control policy.			X	
44	There **MAY** be a system record automatically created for account creation, modification, enabling, disabling, and removal actions.	X			
45	There **SHOULD** be a system record automatically created for account creation, modification, enabling, disabling, and removal actions.		X		
46	There **MUST** be a system record automatically created for account creation, modification, enabling, disabling, and removal actions.			X	
47	Controls **MAY** be in place to require system accounts to log out after a specified period of inactivity.	X			
48	Controls **SHOULD** be in place to require system accounts to log out after a specified period of inactivity.		X		
49	Controls **MUST** be in place to require system accounts to log out after a specified period of inactivity.			X	
50	Privileged user accounts **MAY** be established and administered using a role-based access scheme.	X			
51	Privileged user accounts **SHOULD** be established and administered using a role-based access scheme.		X		
52	Privileged user accounts **MUST** be established and administered using a role-based access scheme.			X	

53	Monitoring and alarming technology components **MAY** be configured to generate real-time notifications and initiate processes for timely threat mitigation.	X			
54	Monitoring and alarming technology components **SHOULD** be configured to generate real-time notifications and initiate processes for timely threat mitigation.		X		
55	Monitoring and alarming technology components **MUST** be configured to generate real-time notifications and initiate processes for timely threat mitigation.			X	
56	Automated or manual processes **MAY** be in place to terminate shared/group account credentials when members leave the group.	X			
57	Automated or manual processes **SHOULD** be in place to terminate shared/group account credentials when members leave the group.		X		
58	Automated or manual processes **MUST** be in place to terminate shared/group account credentials when members leave the group.			X	
59	Automated processes **MAY** be in place to enforce a limit of unsuccessful login attempts and lock the account/node until released by an administrator or administrative process (e.g., forced password reset).	X			
60	Automated processes **SHOULD** be in place to enforce a limit of unsuccessful login attempts and lock the account/node until released by an administrator or administrative process (e.g., forced password reset).		X		
61	Automated processes **MUST** be in place to enforce a limit of unsuccessful login attempts and lock the account/node until released by an administrator or administrative process (e.g., forced password reset).			X	

62	The system **MAY** prevent system access after a defined period of inactivity and require that the user reestablishes access using established identification and authentication procedures. Additional guidance can be found in the PCTF Authentication Profile.	X			
63	The system **SHOULD** prevent system access after a defined period of inactivity and require that the user reestablishes access using established identification and authentication procedures. Additional guidance can be found in the PCTF Authentication Profile.		X		
64	The system **MUST** prevent system access after a defined period of inactivity and require that the user reestablishes access using established identification and authentication procedures. Additional guidance can be found in the PCTF Authentication Profile.			X	
65	If information systems allow concurrent sessions, processes **MAY** be in place to limit the number of concurrent sessions for each defined account type as per the organization's established security and access policy.	X			
66	If information systems allow concurrent sessions, processes **SHOULD** be in place to limit the number of concurrent sessions for each defined account type as per the organization's established security and access policy.		X		

67	If information systems allow concurrent sessions, processes **MUST** be in place to limit the number of concurrent sessions for each defined account type as per the organization's established security and access policy.			X	
68	Organizations **MAY** assign account managers for information system accounts and establish formal conditions for group and role membership granting access authorizations.	X			
69	Organizations **SHOULD** assign account managers for information system accounts and establish formal conditions for group and role membership granting access authorizations.		X		
70	Organizations **MUST** assign account managers for information system accounts and establish formal conditions for group and role membership granting access authorizations.			X	
71	Documented processes **MAY** be in place that require approvals for account creation and have automated procedures to monitor information system account usage.	X			
72	Documented processes **SHOULD** be in place that require approvals for account creation and have automated procedures to monitor information system account usage.		X		
73	Documented processes **MUST** be in place that require approvals for account creation and have automated procedures to monitor information system account usage.			X	

74	The organization **MAY** adhere to the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. This includes: • Configuration of software products to reflect the most restrictive mode consistent with operational requirements; • Restricted access to Digital Identity data using configurations that provide explicit access to only that data required by the individual or system that requires it; and • Network and communication device configurations restricting access to only those system components or services that are required.	X			

75	The organization **SHOULD** adhere to the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. This includes: • Configuration of software products to reflect the most restrictive mode consistent with operational requirements; • Restricted access to Digital Identity data using configurations that provide explicit access to only that data required by the individual or system that requires it; and • Network and communication device configurations restricting access to only those system components or services that are required.		X		

76	The organization **MUST** adhere to the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. This includes: • Configuration of software products to reflect the most restrictive mode consistent with operational requirements; • Restricted access to Digital Identity data using configurations that provide explicit access to only that data required by the individual or system that requires it; and • Network and communication device configurations restricting access to only those system components or services that are required.			X	
77	The organization **MAY** maintain availability of information in the event of the loss of cryptographic keys by users.	X			
78	The organization **SHOULD** maintain availability of information in the event of the loss of cryptographic keys by users.		X	X	
79	The information system **MAY** implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to Digital Identity information during transmission.	X			
80	The information system **SHOULD** implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to Digital Identity information during transmission.		X		

81	The information system **MUST** implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to Digital Identity information during transmission.			X	
82	The organization **MAY** authorize external connections between information systems based on formal security agreements as defined in the organization's security policy.	X			
83	The organization **SHOULD** authorize external connections between information systems based on formal security agreements as defined in the organization's security policy.		X		
84	The organization **MUST** authorize external connections between information systems based on formal security agreements as defined in the organization's security policy.			X	
85	For each individual external connection between information systems, the interface characteristics, security requirements, and the nature of the information communicated **MAY** be documented.	X			
86	For each individual external connection between information systems, the interface characteristics, security requirements, and the nature of the information communicated **SHOULD** be documented.		X		
87	For each individual external connection between information systems, the interface characteristics, security requirements, and the nature of the information communicated **MUST** be documented.			X	
88	Change history for the agreement and/or interface characteristics **MAY** be maintained for external connections between information systems.	X			

89	Change history for the agreement and/or interface characteristics **SHOULD** be maintained for external connections between information systems.		X	X	
90	Internal connections between information system components **MAY** be documented, capturing the interface characteristics, security requirements, and the nature of the information communicated.	X			
91	Internal connections between information system components **SHOULD** be documented, capturing the interface characteristics, security requirements, and the nature of the information communicated.		X		
92	Internal connections between information system components **MUST** be documented, capturing the interface characteristics, security requirements, and the nature of the information communicated.			X	
93	Change history for the interface characteristics, security requirements, and the nature of the information communicated **MAY** be maintained for internal connections between information system components.	X			
94	Change history for the interface characteristics, security requirements, and the nature of the information communicated **SHOULD** be maintained for internal connections between information system components.		X	X	
95	Processes **MAY** be in place to ensure approved authorizations for controlling the flow of information within the system and between interconnected systems based on the organization's security policy.	X			
96	Processes **SHOULD** be in place to ensure approved authorizations for controlling the flow of information within the system and between interconnected systems based on the organization's security policy.		X		

97	Processes **MUST** be in place to ensure approved authorizations for controlling the flow of information within the system and between interconnected systems based on the organization's security policy.			X	
98	The organization **MAY** employ automated mechanisms to make security alerts and advisory information available to authorized security personnel.	X			
99	The organization **SHOULD** employ automated mechanisms to make security alerts and advisory information available to authorized security personnel.		X	X	
100	The organization **MAY** receive information system security alerts, advisories, and directives from recognized external authorities (for example, vendors, business partners, supply chain partners, external security authorities etc.) on an ongoing basis and generate internal security alerts, advisories, and directives as deemed necessary.	X			
101	The organization **SHOULD** receive information system security alerts, advisories, and directives from recognized external authorities (for example, vendors, business partners, supply chain partners, external security authorities etc.) on an ongoing basis and generate internal security alerts, advisories, and directives as deemed necessary.		X	X	

102	The organization **MAY:** • Identify, report, and correct information system flaws; • Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Install security-relevant software and firmware updates within a time period, after release, defined by the organization's security policy; and • Incorporate flaw remediation into the organizational configuration management process.	X			
103	The organization **SHOULD:** • Identify, report, and correct information system flaws; • Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Install security-relevant software and firmware updates within a time period, after release, defined by the organization's security policy; and • Incorporate flaw remediation into the organizational configuration management process.		X		

104	The organization **MUST:** • Identify, report, and correct information system flaws; • Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Install security-relevant software and firmware updates within a time period, after release, defined by the organization's security policy; and • Incorporate flaw remediation into the organizational configuration management process.			X	
105	Formal technology change management processes **MAY** be in place to evaluate and manage risk associated with technology evolution.	X			
106	Formal technology change management processes **SHOULD** be in place to evaluate and manage risk associated with technology evolution.		X		
107	Formal technology change management processes **MUST** be in place to evaluate and manage risk associated with technology evolution.			X	
108	The organization **MAY** define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	X			
109	The organization **SHOULD** define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.		X		
110	The organization **MUST** define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.			X	

111	Technology change management processes **MAY:** • Determine the types of changes to the information system that are configuration-controlled; • Review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; • Document configuration change decisions associated with the information system; • Implement approved changes to the information system; • Retain records of changes to the information systems for the time period specified in the change control policy; and • Coordinate and provide oversight for configuration change control activities through a formally constituted change control governance body.	X			

112	Technology change management processes **SHOULD:** • Determine the types of changes to the information system that are configuration-controlled; • Review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; • Document configuration change decisions associated with the information system; • Implement approved changes to the information system; • Retain records of changes to the information systems for the time period specified in the change control policy; and • Coordinate and provide oversight for configuration change control activities through a formally constituted change control governance body.		X	X	
113	Activity monitoring and audit trail facilities **MAY** be in place to provide a record of all digital identity-related transactions within the Digital Identity Ecosystem.	X			
114	Activity monitoring and audit trail facilities **SHOULD** be in place to provide a record of all digital identity-related transactions within the Digital Identity Ecosystem.		X		
115	Activity monitoring and audit trail facilities **MUST** be in place to provide a record of all digital identity-related transactions within the Digital Identity Ecosystem.			X	
116	Records of all digital identity-related transactions within the Digital Identity Ecosystem **MAY** be protected from alteration and limited access policies enforced.	X			

117	Records of all digital identity-related transactions within the Digital Identity Ecosystem **SHOULD** be protected from alteration and limited access policies enforced.		X		
118	Records of all digital identity-related transactions within the Digital Identity Ecosystem **MUST** be protected from alteration and limited access policies enforced.			X	
119	Audit information and audit tools **MAY** be protected from unauthorized access, modification, and deletion.	X			
120	Audit information and audit tools **SHOULD** be protected from unauthorized access, modification, and deletion.		X		
121	Audit information and audit tools **MUST** be protected from unauthorized access, modification, and deletion.			X	
122	The information system **MAY** have mechanisms in place that protect against an individual (or process acting on behalf of an individual) falsely denying having performed actions to be covered by non-repudiation.	X			
123	The information system **SHOULD** have mechanisms in place that protect against an individual (or process acting on behalf of an individual) falsely denying having performed actions to be covered by non-repudiation.		X		
124	The information system **MUST** have mechanisms in place that protect against an individual (or process acting on behalf of an individual) falsely denying having performed actions to be covered by non-repudiation.			X	

125	Audit records **MAY** be securely retained for the time period identified in the organization's information retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	X			
126	Audit records **SHOULD** be securely retained for the time period identified in the organization's information retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		X		
127	Audit records **MUST** be securely retained for the time period identified in the organization's information retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.			X	
128	Audit records **MAY** be generated for Digital Identity transactions containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	X			
129	Audit records **SHOULD** be generated for Digital Identity transactions containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.		X		

130	Audit records **MUST** be generated for Digital Identity transactions containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.			X	
131	Audit records **MAY** be generated for the execution of privileged system functions.	X			
132	Audit records **SHOULD** be generated for the execution of privileged system functions.		X		
133	Audit records **MUST** be generated for the execution of privileged system functions.			X	
134	Processes **MAY** be in place to ensure that only authorized personnel can execute privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.	X			
135	Processes **SHOULD** be in place to ensure that only authorized personnel can execute privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.		X		
136	Processes **MUST** be in place to ensure that only authorized personnel can execute privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasure.			X	
137	Information system account usage **MAY** be monitored for atypical usage and atypical usage patterns reported and/or accounts disabled dependent on risk associated with observed atypical usage.	X			
138	Information system account usage **SHOULD** be monitored for atypical usage and atypical usage patterns reported and/or accounts disabled dependent on risk associated with observed atypical usage.		X		

139	Information system account usage **MUST** be monitored for atypical usage and atypical usage patterns reported and/or accounts disabled dependent on risk associated with observed atypical usage.			X	
140	Processes **MAY** be in place to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	X			
141	Processes **SHOULD** be in place to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.		X		
142	Processes **MUST** be in place to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.			X	
143	The organization **MAY** have clearly identified data and information stewards.	X			
144	The organization **SHOULD** have clearly identified data and information stewards.		X	X	
145	The organization **MAY** have a documented API standard.	X			
146	The organization **SHOULD** have a documented API standard.		X	X	

6. References

This Profile was influenced by the standards or standard bodies listed below. Each of the cited organizations includes a document repository containing multiple documents pertaining to the establishment and operation of a technical infrastructure required to support the delivery of service, in this case, to a Digital Identity Ecosystem.

Note: Where applicable, only the version or release number specified herein applies to this PCTF component.

PCTF Component Conformance profiles (public versions to be published in their final state at www.diacc.ca) were referenced in their draft state:

- Authentication Conformance Profile
- Credentials (Relationships & Attributes) Conformance Profile
- Notice & Consent Conformance Profile
- Privacy Conformance Profile
- Verified Organization Conformance Profile
- Verified Person Conformance Profile

Government of Canada. *GoC Treasury Board Directive on Service and Digital*. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601

Government of Canada. *GoC PCTF Public Sector Profile V1.1*. https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_1

United States Department of Commerce. National Institute of Standards and Technology. *Digital Identity Guidelines (NIST Special Publication 800-63 – 5 documents).* 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html

United States Department of Commerce. National Institute of Standards and Technology. *Assessing Security and Privacy Controls (NIST Special Publication 800-53 Rev. 5).* September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

ISACA. *Control Objectives for Information Technology (COBIT)*. www.isaca.org

Axelos. *IT Infrastructure Library (ITIL).* www.axelos.com

International Standards organization (ISO). *Evaluation criteria for IT security*. https://www.iso.org/standard/50341.html

US Federal Government, *Federal Risk and Authorization Management Program (FedRAMP). See link to document repository*. www.fedramp.gov

European Union Agency for Cybersecurity (ENISA). *See link to document repository*. https://www.enisa.europa.eu/

7. Revision History

Version	Date	Author	Comment
0.01	2019-12-15	PCTF Editing Team	Initial framework draft
0.02	2020-02-14	PCTF Editing Team	Initial content-complete draft
0.03	2020-03-03	PCTF Editing Team	Adjustments based on further research and review of PCTF component drafts
0.04	2020-03-30	PCTF Editing Team	Final adjustments for publication of Draft
0.05	2020-06-05	PCTF Editing Team	Updates based on TFEC member input
0.06	2020-06-29	PCTF Editing Team	Updates as a result of a short supplemental TFEC review period
1.0	2020-07-08	PCTF Editing Team	TFEC approved as Draft Recommendation V1.0
1.1	2020-09-18	PCTF Editing Team	Updates per comments received during Draft Recommendation public review period
1.0	2020-09-30	PCTF Editing Team	TFEC approved as Candidate for Final Recommendation V1.0
1.1	2022-08-09	PCTF Editor and Infrastructure Design Team	Final Recommendation V1.1 to incorporate alpha testing feedback
1.1	2022-09-14	PCTF Editor and Infrastructure Design Team	TFEC approved as Final Recommendation V1.1
1.1.1	2023-01-19	PCTF Editor and Infrastructure Design Team	Updates per comments received during Final Recommendation V1.1 public review period

1.2	2023-02-01	PCTF Editor and Infrastructure Design Team	TFEC approves as Candidate for Final Recommendation V1.2
1.2	2023-04-19	PCTF Editor and Infrastructure Design Team	Approved as Final Recommendation V1.2 through DIACC Sustaining Member Ballot