DIACC-CP-03-01 GUIDANCE FOR AUDITS OF SERVICES AGAINST PCTF

Version 2.1
Reference: DIACC-CP-03-01
Status: Final version
Date: 2024-01-02
Editor: DIACC Certification Program Management Office (CPMO)

This document describes the Audit approach to determine conformity of services against DIACC Pan-Canadian Trust Framework (PCTF). It is based on ISO standards (ISO/IEC 17021; ISO/IEC 17065; ISO/IEC 19011, ISO/IEC 27001, ISO/ IEC 27006, ISO/IEC 29115) and industry best practices.

Table of Contents

Guidance for audits of Services against PCTF

1. Introduction

The DIACC Certification provides assurance that Services conform to specified requirements in the DIACC Pan-Canadian Trust Framework (PCTF).

The DIACC Certification is based on a third-party conformity assessment performed by DIACC Auditors and with an independent quality assurance review by the Independent Review Committee (IRC).

This document provides guidance on performing audits of services against PCTF.

The definitions used in this document are available in Exhibit A.

2. Audit Overview

The DIACC Certification Trustmark is granted to Operators whose Service demonstrates conformity against the PCTF.

The DIACC Certification Trustmark has a three-year cycle and is subject to annual audits. If necessary, unscheduled audits may apply.

3. Networks

Network and Network Elements can be granted the Certification Trustmark as a specific type of service as defined in Exhibit A, see definition of Network.

An Operator providing a Network[1] or Network Element is audited as a Service according to this guidance, but with a specified scope and responsibilities for the audited entity.

The scope of the Audit for a Network will depend on the architecture of the Network, as well as the responsibility of the Network operator and the entities that jointly deliver, integrate, and contribute to the Network.

For a Network to be assessed there needs to be a designated authoritative entity for the Network. The authoritative entity is responsible for the governance of the Network. Depending on the setup of the Network and its architecture the Audit of the Network will differ. The following is a non-exhaustive list of models that can be audited.

3.1 A self-governed Network

[1] See definition of Network in Exhibit A.

For this type of Network there is a governance framework for the Network that one entity (the Network operator) is responsible for, and that the entity enforces.

This Network type is defined and assessed as follows:

- The scope and applicability of PCTF components and conformance criteria is defined by the Network operator.
- The scope as well as the applicability is validated for completeness by the Auditor.

The Network operator can then be audited with the following scope:

1. All processes and technology provided by the Network operator.
2. Fulfillment of all governance requirements and processes defined in the Network architecture.
3. The governance processes performed by the Network operator.
4. All applicable PCTF components and conformance criteria.

Each Network Element is audited with the following scope:

1. All governance requirements and processes for a Network Element defined by the Network operator.
2. All applicable PCTF components and respective conformance criteria.

3.1.1 Responsibilities

- Network Operator: Responsible for the governance of the network and conformance against PCTF criteria for the services the Operator provides.
- Network Elements: Responsible for conformance against PCTF criteria for the Network Element as well as governance as part of the Network Element.
- Auditor: Validation of applicability and completeness of PCTF component criteria defined by the Network Operator and Elements, as well as validation of governance requirements and processes defined in the Network architecture.

Example of Networks of this type would be a federated identity service with a defined federation operator. A specific example would be Incommon Federation (https://incommon.org/federation/).

3.2 A regulated Network

For this type of Network there is a, for the Network, externally defined governance framework or a regulation for the Network that is enforced jointly by the different parties in the Network.

This Network is audited as follows:

1. All Network Elements are audited separately with the following scope:
    a. Fulfillment of all governance requirements and processes defined in the Network architecture
    b. The governance processes performed by the specific Network Element.
2. The scope and applicability of PCTF components and conformance criteria is defined by the Network Element.

3. The scope as well as the applicability is validated for completeness by the Auditor.
4. All applicable PCTF components and respective conformance criteria

3.2.1 Responsibilities

- Network Elements: Responsible for conformance against PCTF criteria for the Network Element as well as governance as part of the Network Element as required in the externally defined framework or regulation.

- Auditor: Validation of applicability and completeness of PCTF component criteria for the Network Elements as well as validation of fulfillment of governance requirements and processes defined in the Network architecture.

Example of Networks of this type would be a regulated Identity Wallet framework with entities providing identity services, attribute services, wallet applications or relying parties

4. Key aspects of the Audit

a. The Audit must be performed on an operational Service, with at least three (3) months of operational records.
b. The conformance criteria must be used as a reference when conformity is determined and must include the normative requirements of the applicable PCTF Components. Please see the available conformance criteria at https://diacc.ca/trust-framework/
c. The Audit must follow the approach of an information security audit or similar, such as using ISO/IEC 19011 Auditing Management Systems for auditing of Information Security Management Systems.
d. The Audit is technically a Point in Time audit, which means that the Auditor conducts an Audit once per year, which provides assurance of the service operations over a one-year period.
e. The DIACC Certification Trustmark is granted for a three-year cycle and is subject to annual audits and, if necessary, unscheduled audits.
f. Annual surveillance audits are required to maintain the DIACC Certification Trustmark.
g. Unscheduled audits may be required if Significant Changes have been implemented to the Certified Service.

5. Audit activities

During the audit, information relevant to the Service objectives, scope and criteria should be obtained by appropriate sampling and Certified by the Auditor to become Audit evidence. In this regard, the Audit may entail the examination and evaluation of the Operator's information technology infrastructure, systems, policies, and operations related to the provision of a Service that seeks conformity against PCTF.

Methods to obtain information may include, but are not limited to:

a. Documentation reviews relevant to the scope of the Audit and application for Certification against the applicable PCTF Component.
b. Review of organisational policies and practices.
c. Review records, systems logs.
d. Examination and test of the system that is the object of the audit, including system documentation, system functionality.
e. Observation of processes and activities.
f. Interview management personnel; technical or managerial personnel; trained personnel.
g. Onsite visits according to the level of assurance (LOA2 and anything above). In the case that the mobility is restricted due to health or other force majeure reasons, the DIACC Accredited Auditor must find a remote technological equivalent.

6. Considerations for Operators

The Operator of the Service must:

a. Be aware that the Audit must be performed to operational Services that have been operational (in live production) for at least three (3) months before getting audited.

b. Provide unrestricted access to those parts of its business, premises, systems, records, and supporting documents, covered by the proposed scope of audit.

c. Demonstrate that the Service meets the applicable PCTF Component conformance criteria, by providing the necessary evidence.

d. Ensure that the External Providers integrated into its Service are in scope of the audit, by for example having in place appropriate processes and contractual arrangements with the external providers that are integrated with its Service, which must enforce the external providers to follow the specific requirements and provide the necessary evidence for the audit.

e. For a Network Operator, ensure that all Network Elements that integrated to the Network are in scope of the audit, by for example having in place appropriate processes, governance framework, and contractual arrangements with the Network Element, which must enforce the Network elements to follow the specific requirements and provide the necessary evidence for the audit.

f. Consider that the Auditor is required to keep the Audit Records for three years.

7. Considerations for Auditors

The Auditor must:

a. Follow this document as the key guidance for the Audit.
b. Follow the Conflict of Interest policy as specified in the DIACC-CP-01-01 Eligibility criteria for auditors, also available at the Exhibit B of this document.
c. Ensure that the Service to be audited is operational for at least three (3) months.
d. Create an audit plan based on the agreed scope.
e. Determine whether the claims provided during the application are materially correct and conform with the specified requirements addressed in the applicable PCTF Component conformance criteria. Through the validation of the claims, the Auditor will determine conformity against the applicable PCTF components conformance criteria and confirmation of truthfulness of the Service object of Certification.

8. Types of Audits during the Certification Trustmark cycle

8.1. Overview

The DIACC Certification Trustmark has a three-year cycle in which the Operator of the Service must go through different types of audits:

- Year 1 - Initial Audit before the Certification is granted and the applicable DIACC Certification Trustmark is issued.
- Year 2 and 3 - Annual surveillance Audits to maintain the DIACC Certification Trustmark.
- Unscheduled audits due to Significant Changes to the Service.

8.1.1 Initial Audit

The initial Audit is a full Audit that must be performed against 100% of the applicable criteria.

8.1.2 Annual surveillance audits

Annual surveillance audits must be conducted by the Auditor in the first and second years following the DIACC Certification Trustmark issuance.

Year 2 - Annual surveillance Audit against 50% of the applicable criteria, including consideration of risks and changes to the service.

Year 3 - Annual surveillance audits against the other 50% of the applicable criteria, including consideration of risks and changes to the service.

8.1.3 Unscheduled audits

The Service Operator is obliged by the Certification Agreement to notify the Certification Program Management Office (CPMO) of any changes to the Certified Service.

The Auditor and CPMO will evaluate if the changes apply as Significant Changes [2] and if so, it will determine if there is a need for an unscheduled audit.

In the event, it is more than six months away from the annual surveillance Audit an unscheduled Audit may be required.

8.1.4 Recertification Audit

At the end of the third year, prior to the expiration of the Certification Trustmark, a full Audit must be conducted.

8.1.5 Changes to the PCTF Components

The CPMO will notify the Service Operator of any changes to the PCTF Components conformance criteria applicable to the Certification Trustmark.

If the changes are material, the implementation of the new requirements and applicable Audit must take place in a 15-month period after the DIACC TFEC notification of the new release.

To avoid the possible requirement of unscheduled audits, it is suggested that the implementation of the new requirements and related audits are aligned with the annual schedules of the granted Trustmark.

9. Planning the audit

The Audit objectives should describe what is to be accomplished and may include:

a. Determination of the conformity of the service, or parts of it, with PCTF conformance criteria.
b. Determination of the effectiveness of the service systems to ensure that they are achieving specified objectives.

[2] See definition of Significant Changes in Exhibit A

c. as applicable, identification of areas for potential improvement of the service.
d. For Networks and Network elements, scope and applicability to be validated for completeness.

The Audit scope should describe the extent and boundaries of the audit.

The Audit plan should be appropriate to the objectives and the scope of the audit, it may include or refer to the following:

a. The Audit objectives;
b. The Audit criteria;
c. The Audit scope, including identification of the organisational and functional units, processes, systems and network elements to be audited;
d. The dates and sites where the on-site Audit activities will be conducted;
e. The roles and responsibilities of the Audit team members.

10. Performing audits during the three-year cycle of Certification Trustmark

10.1 Initial Audit activities

The purpose of the initial Audit is to evaluate the implementation, including the effectiveness of the service systems and processes, in relation to the applicable PCTF Component(s) being audited.

The initial Audit is a full audit that must be performed against 100% of the applicable criteria.

The initial Audit may include onsite visits according to the level of assurance (LOA2 and anything above). In the case that the mobility is restricted due to health or other force majeure reasons, the Auditor must find a remote technological equivalent.

The initial Audit may include the Audit of the following:

a. Information and evidence about conformity to all requirements of the applicable PCTF Components conformance criteria.
b. Performance monitoring, measuring, reporting, and reviewing against key performance objectives and targets (consistent with the expectations in the applicable PCTF Components conformance criteria).

c. The service systems ability and its performance regarding meeting of applicable PCTF Components conformance criteria.
d. Operational control of the service Operator processes.
e. Internal quality assurance and management review.
f. Service operator policies.

10.2 Annual surveillance audit activities

The aim of the annual surveillance audits is to maintain confidence that the Certified Service continues to fulfil PCTF requirements between recertification audits.

Year 2 - Annual surveillance Audit against 50% of the applicable criteria, including consideration of risks and changes to the service and addressing minor non-conformities if applicable.

Year 3 - Annual surveillance Audit against the other 50% of the applicable criteria, including consideration of risks and changes to the service. These actions shall be implemented and Certified prior to the expiration of Certification Trustmark.

Annual surveillance audits include activities so that representative areas and functions covered by the scope of the service are monitored on an annual basis and take into account changes to the Certified Service and performance of its related systems.

Each annual surveillance Audit includes the following activities, if applicable:

a. Review of remedial actions taken on minor non-conformities identified during the previous audit.
b. Effectiveness of Service with regard to achieving the Certification objectives.
c. Progress of planned activities aimed at continual improvement.
d. Continuing operational control.
e. Review of any changes.
f. Risk-based approach.

Annual surveillance audits are usually on-site audits, according to the level of assurance (LOA2 and anything above). In the case that the mobility is restricted due to health or other force majeure reasons, the Auditor must leverage a remote technological equivalent.

At the end of Year 3 of the Trustmark cycle, the Service is expected to undergo a new initial audit, essentially a full Audit to start a new cycle.

10.3 Recertification Audit activities

At the end of the third year, prior to the expiration of the Certification Trustmark, a full Audit must be conducted.

The recertification Audit is a full Audit that must be performed against 100% of the applicable criteria.

The recertification Audit may include an on-site Audit according to the level of assurance (LOA2 and anything above). In the case that the mobility is restricted due to health or other force majeure reasons, the Auditor must leverage a remote technological equivalent.

The recertification Audit includes the following activities, if applicable:

a. A review of remedial actions taken on minor non-conformities identified during the previous audit.
b. Effectiveness of Service with regard to achieving the Certification objectives and its continued relevance and applicability to the scope of Certification.
c. Progress of planned activities aimed at continual improvement and enhancement of overall performance.
d. Continuing operational control.
e. Review of any changes.
f. Risk-based approach

11. Finding of non-conformity

11.1 Minor non-conformity

A minor non-conformity means a single identified gap or a concern in meeting a requirement of the conformance criteria in scope, which, in the Auditor's judgment, would not in itself raise significant doubt as to the capability of the Service Operator to achieve its objectives.

In order to mitigate the risk of the minor non-conformity found during the audit, the Auditor and Applicant should work together and agree on a clear remediation plan with specific corrective actions and deadlines for completion.

Minor non-conformities must be remediated before the next annual surveillance Audit.

Corrective actions must be appropriate to the impact of the problems encountered.

During and after the audit, the Auditor must ensure the following:

a. Identify non-conformities.
b. Determine the causes of non-conformity.
c. Propose correcting non-conformities.
d. Evaluate the need for actions to ensure that non-conformities do not recur.
e. Determine and implement the actions needed in a timely manner.

f. Record the results of remedial actions taken.
g. Review the effectiveness of corrective actions.

After the DIACC Certification Trustmark is granted to a Service, the CPMO will follow up with the Operator to make sure it takes the necessary actions and measures to remediate the identified minor non-conformities.

11.2 Reporting minor non-conformities

11.2.1 The Auditor's report of the initial Audit must include all minor non-conformities found and the prescribed corrective actions with corresponding deadlines for completion.

11.2.2 In the annual surveillance audits, the Auditor must include the completed remediation report for the minor non-conformities.

11.3 Major non-conformity

A major non-conformity is an absence of, or the repeated failure to implement and maintain, one or more of the required applicable conformance criteria, or a situation that would, on the basis of objective evidence, raise significant doubt as to the capability of the Service Operator to achieve its objectives.

A major non-conformity must be addressed before an Audit can be completed and the application will be paused until the major non-conformity is remediated.

The Applicant has a period of twelve months to maintain the application. Within that time frame, the Applicant must address the major non-conformity issues and demonstrate that it has completed the remediation plan that the Auditor has proposed.

12. Audit Report

The work carried out by the Auditor must be covered by a comprehensive Audit Report, using the DIACC provided template.

The Audit Report must include at least the following elements:

a. The name of the Service Operator.
    - In addition, for a Network: the role of the audited entity in the Network, i.e., Network operator, Network Element, or other roles depending on Network architecture.
b. The name of the Service, Network or Network Element.
c. Scope of the audit.
    - For a Network, the validated applicable requirements for the audited entity.

- For a Network, the Network architecture, and the roles of all the Network elements.
- If applicable reference to any externally defined or regulated network.

d. The date of receipt of the evidence provided by the applicant.
e. Period of time (dates) of performance of the audit. The duration of the Audit must be recorded in the Audit report.
f. The date of issue of the report.
g. Names of the audit team members who have performed the audit, clearly identifying who was the Lead Auditor.
h. Information on environmental conditions during the audit, if relevant.
i. Clear determination whether there is conformity or not against the applicable PCTF component and specific Level of Assurance. This may include a statement on the conformity and the effectiveness of the Service conforming its capability to meet applicable requirements and expected outcomes.
j. Audit methods, procedures used, and standards followed to perform the audit.
k. Minor non-conformities (as applicable).
l. Remedial actions and timeline to mitigate the minor non-conformities found.
m. Recommendation to confirm the Certification of a Service and its corresponding issuance of Trustmark.
n. Signature of Lead Auditor that supervised the audit.
o. Signature of the client.

13. References

a. ISO/IEC 17021 Conformity Audit—Requirements for bodies providing audit and certification of management systems.
b. ISO/IEC 19011 Guidelines for auditing management systems.
c. ISO/IEC 27006 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems.
d. ISO/IEC 29115 Information technology — Security techniques — Entity authentication assurance framework.
e. NIST 800-63-3 Conformance Criteria (63A, 63B and 63C)
https://www.nist.gov/system/files/documents/2020/07/02/800-63A%20Conformance%20Criteria_0620.pdf
https://www.nist.gov/system/files/documents/2021/04/27/800-63C%20Conformance%20Criteria_042621.pdf
f. TDIF annual Audit requirements
https://www.digitalidentity.gov.au/sites/default/files/2021-06/tdif-07-annual-assessment- release-4-v1.1.pdf

Revision history

Version	Release Date	Changes
2.1	2024-01-02	Adjustments in terminology
2.0	2022-11-16	Incorporated audit of Networks Adjustments to fulfill ISO 17065 requirements
1.0	2022-03-14	New Document

Exhibit A – Definitions

Term	Meaning
Applicant	Operator seeking Certification of its Service against applicable PCTF Components.
Audit	Third-party assessment or inspection or examination, of an organisation, and/or a process and/or a system, to ensure compliance with PCTF Components requirements.
Audit Records	Evidence of the Audit reports and other technical information created and/or obtained by a DIACC Auditor in relation to the DIACC PCTF audits/assessments.
Audit Report	Report provided by the Auditor, which informs conformity of a Service against the applicable DIACC PCTF Component conformance criteria.
Auditor	DIACC-accredited Auditor qualified to perform audits against PCTF Components.
DIACC PCTF Components	DIACC Pan-Canadian Trust Framework Components are available at https://diacc.ca/trust-framework/
Network	A Network is an identity solution that is dependent on elements and services provided by different entities. A Network will consist of governance, processes and technologies across the different entities that jointly deliver and integrate with the Network. There are different network architectures, such as federations, wallet solutions, proxies, agents, and brokers, not excluding other architectures.

Network Element	A Network Element or just Element is a separate part or separate service in a Network. A Network element that is provided by a separate entity can be separately audited against the PCTF. Examples of Network elements are federation operators, issuers, attribute providers, wallet providers or relying parties.
Service	Identity solution that supports identity proofing, authentication and/or credential management and/or other related functionalities. A Service, in the context of the PCTF, requires a User to be authenticated to access the Service. Examples: applying for employment insurance; registering a business; applying for a loan; making online purchases. Services applicable for Audit against the PCTF, include Networks and Network Elements.

Significant Changes	Significant Changes to the Certified Service may include: 1. Changes relating to the legal, commercial, organisational status or ownership. 2. Changes relating to the scope of operations under the Certified Service. 3. Major changes to the Certified Service management system and processes. 4. Change of external providers (external service components; subcontracted services). 5. Change of type of authenticator. 6. Access control change. 7. Privacy policy change. 8. Addition of new functionalities. 9. Other changes as applicable.
Trustmark	Any sign or mark of conformity that an entity has fulfilled the applicable requirements, including DIACC trademarks, trade names, symbols, logos, which DIACC grants the right to use to identify the Certification of a Service.
Independent Review Committee (IRC)	The IRC has delegated authority from the DIACC Board of Directors (BOD) to perform a quality review of the audit findings.
Certification	Demonstration that specified requirements from DIACC PCTF relating to a Service are fulfilled. The DIACC Certification process includes a third-party Audit against the applicable DIACC PCTF Components, conducted by a DIACC Accredited Auditor.

DIACC Certification Program (DCP)	A DIACC run program that verifies Services and Networks against the Pan-Canadian Trust Framework (PCTF), indicating that specific assurance requirements and best practices are met.

Exhibit B - Conflicts of Interest Policy (COI Policy) regarding a Service to be audited.

1. Purpose

DIACC Auditors are expected to conduct their services with objectivity and impartiality. The Auditor team members are obligated to disclose ethical, legal, financial and other conflicts of interest involving the Operators of the Service (s) to be audited.

The purpose of this Conflicts of Interest Policy (COI Policy) is to prevent any conflict of interest or the appearance of a conflict of interest from affecting any decision-making involving the audit of a Service.

The Auditor must adopt this COI Policy.

2. Potential Conflicts

A conflict of interest may include any of the following situations:

a. Financial conflict;
b. Direct or indirect gain (of any sort) arising from access to confidential information;
c. Family/personal relationships and bias;
d. Contractual or affiliation relationships;
e. Be the designer, implementer, developer, operator or maintainer of the Service to be audited. This does not preclude the possibility of exchange of information (e.g., explanations of findings or clarifying requirements) between the Auditor and its clients.
f. Provide consultancy regarding the Service to be audited, including:
    - Recommendations, readiness, gap analysis of a Service to be audited;
    - Participate in the designing, development, installing, maintaining of a Service to be audited.
g. State or imply that Audit performance would be simpler, easier, faster or less expensive if a specified consultancy entity were used.

3. Duty to disclose

The Auditor must disclose any matter that could reasonably affect the outcome of the Audit and decision-making process, any conflict or potential conflict, to the applicable clients and the DIACC.

4. Cooling period

The conflict of interest cooling period shall be two years from the conclusion of all related consultancy performed to the Service to be audited (as specified in item 2 above).
To ensure that the cooling period is complied, the organisation that has provided consultancy to the Service to be audited, shall not perform an Audit to that Service within two years following the end of the consultancy.