PORTAGE CYBERTECH
A CONVERGE COMPANY

WHITE PAPER

THE PCTF
AND GOVERNMENT ORGANIZATIONS

Table of Contents

The PCTF for Government Organizations: A Clear Picture

What the PCTF Is and Why It’s Important

Why Government Organizations Should Align with the PCTF

How to Align with the PCTF: A Practical Overview

One Framework, 10 Components

1. Model
2. Glossary
3. Assessment
4. Authentication
5. Notice & Consent
6. Verified Person
7. Verified Organization
8. Credentials (Relationships & Attributes)
9. Infrastructure (Technology & Operations)
10. Privacy

How Portage CyberTech Can Help You Align With the PCTF

Why Governments May Struggle with the PCTF

Meet Portage™: A National Thought Leader on Privacy and Trust

Our Trust-Based Process, Platforms, and Ecosystems

How to Start Aligning with the PCTF Today

The PCTF for Government Organizations: A Clear Picture

The PCTF creates a framework for building trust and privacy into digital services and ecosystems that serve Canadian citizens. It is a public-private partnership with specific value to Canada's government organizations.

What the PCTF Is and Why It's Important

The Pan-Canadian Trust Framework (PCTF) is a framework that sets process and technical standards that preserve privacy and establish trust between public and private sector parties that are offering digital services and building digital ecosystems for Canadian citizens.

It was published by the Digital Identification and Authentication Council of Canada (the DIACC), a non-profit coalition of public and private sector organizations. The DIACC is committed to developing Canadian frameworks for digital identification and authentication, and to help Canadians participate securely within digital economies.

PCTF is a framework that sets process and technical standards that preserve privacy and establish trust between public and private sector parties that are offering digital services and building digital ecosystems for Canadian citizens.

The DIACC commissioned and published the PCTF to meet several emerging needs.

- To set shared definitions, processes, and evaluation criteria for a wide range of trust and privacy topics that are emerging in the field of cybersecurity and risk.
- To give Canada a trust framework for digital identities, ecosystems, and transactions similar to frameworks created by other nations and industries.
- To help public and private sector organizations comply with Canadian principles, business interests, technical models and regulations.
- To establish an innovative, secure, and privacy-respecting Canadian digital identity ecosystem that supports open government principles.
- To create paths for safe and secure cross-border transactions and service delivery, and to ensure Canada's participation in the global economy.

While the PCTF was designed to provide guidance for both the public and private sector, it solves a few specific, timely needs for Canada's government organizations.

Why Government Organizations Should Align with the PCTF

Over the past two years, government organizations have been forced to accelerate their digital transformations, and to move many of their services online. These digital services — and the digital ecosystems of which they are part — are both necessary for the lives of their citizens and are also at high risk for cyberattack and fraud.

Government organizations need to offer their digital services, and to build new digital ecosystems, in a manner that is both convenient, easy-to-use, and reliable for their citizens, while also protecting their citizens' data and preventing potential misuse. To do so — without retrenching into closed corporate networks that sacrifice cost effectiveness and user experience — organizations need to find a way to establish digital identities for the end users of their digital services and ecosystems.

Further, government organizations need to follow an approach to trust and privacy that can be shared between themselves, other organizations, and the private sector partners, and that can establish levels of assurance (in identities, credentials, and federation arrangements) they need to participate in trusted digital ecosystems.

> **Government organizations need to offer their digital services, and to build new digital ecosystems, in a manner that is both convenient, easy-to-use, and reliable for their citizens, while also protecting their citizens' data and preventing potential misuse.**

The PCTF addresses each of these challenges. It gives government organizations a framework for weaving trust and privacy into their digital services and ecosystems. It also sets national standards that other government organizations and private sector partners can align with to build digital ecosystems with a unified approach to trust.

Ultimately, the PCTF is valuable to every C-level technology leader and to anyone responsible for building digital services and ecosystems and driving digital transformation in government agencies.

By aligning to the PCTF's standards, government organizations will:

- Minimize business and cyber risk from multiple angles
- Improve the efficiency and reliability of their operations
- Comply with current and future best practices in digital identity
- Lay the foundation for modern security strategies like Zero Trust
- Meet the expectations of citizens, business partners, IT and businesses managers, and other stakeholders for secure, trustable digital services and ecosystems

For the rest of this whitepaper, we will outline a practical understanding of what the PCTF recommends, walk through each of its 10 components in detail, and discuss the ways that Portage can help government organizations align with this new framework.

How to Align with the PCTF: A Practical Overview

The PCTF sets new standards for building trust into digital services and ecosystems. It provides a framework of 10 components that all government organizations can choose to align with in whole or in part.

One Framework, 10 Components

At its core, the Pan-Canadian Trust Framework (PCTF) is a comprehensive framework that:

1. Defines core processes and associated criteria for building various elements of trust into digital ecosystems

2. Provides assessment criteria so organizations can make sure they're compliant with the framework's definitions, processes, and best practices

The PCTF's framework is made up of 10 components. Each component tackles a different element of online trust, and each includes its own definitions, processes, best practices, and assessment criteria. The 10 components are:

1. Model	2. Glossary	3. Assessment	4. Authentication	5. Notice & Consent
6. Verified Person	7. Verified Organization	8. Credentials	9. Infrastructure	10. Privacy

While these components make up a unified, end-to-end framework, the PCTF is modular in nature. A government organization can use one or more components as they deem necessary to fill gaps in their existing digital ecosystems, or they can align with this full framework to build comprehensive trust into their digital services.

A government organization can use one or more components as they deem necessary to fill gaps in their existing digital ecosystems, or they can align with this full framework to build comprehensive trust into their digital services.

To help you better understand how the PCTF works, and which elements might be most relevant to you, let's look at each of these 10 components in greater detail.

Component 1: Model

What This Component Is
Provides a complete overview of the PCTF framework. This component explains the PCTF's goals and objectives, and offers an introduction to each component and the criteria and processes that each component encompasses.

Why It Matters for Government Organizations
It outlines a high-level, easy-to-understand picture of the PCTF, what it seeks to achieve, what functional areas it touches, and the processes needed to bring the framework to life.

What You Have to Do
This component does not provide any concrete, actionable steps to improve trust in your digital ecosystems; it is mostly a non-normative document. Instead, it's simply a good idea to read this component to better understand the PCTF as a whole, and to quickly identify the components that are practically relevant for your organization.

Component 2: Glossary

What This Component Is
Provides definitions for every major term used within the PCTF framework. While many of these terms will be familiar, the framework sometimes uses its own specific, nuanced, and contextual definition for each term that can differ from its general understanding.

Why It Matters for Government Organizations
It establishes a shared and consistent understanding of terms used by the PCTF. Many of these terms are used differently by different groups. This glossary ensures all government organizations and private partners work from the same understanding.

What You Have to Do
This component also does not provide any concrete, actionable steps you have to take. Instead, it's a good idea to read through this component to better understand how the PCTF defines key terms related to trust and privacy, and to make sure you understand exactly what the PCTF recommends in each of the following components.

Component 3: Assessment

What This Component Is
Outlines how to examine and evaluate your own digital processes and services, or those of your business partners and other stakeholders. Helps you identify where these processes and services may already be compliant with the PCTF's components and where you or your partners and stakeholders may have gaps to fill.

Why It Matters for Government Organizations
It provides a maturity model for government organizations that seek to follow the PCTF's recommendations. It also provides a shared benchmark between government organizations and private partners to evaluate each other's alignment with the PCTF.

What You Have to Do
This component provides guidance on how to utilize and interpret the assessment criteria that are included in every other component. You can use it to define levels of assurance for digital transactions within your ecosystem, and to better understand and mitigate the potential risks carried by these transactions.

Component 4: Authentication

What This Component Is

Defines processes and criteria to follow to authenticate the people and organizations using digital services. Also defines processes and criteria that can be used to identify the risks that end users bring to digital ecosystems.

Why It Matters for Government Organizations

It provides standards that government organizations can follow to maintain the integrity of their login and authentication processes. These standards create a baseline level of assurance that a user is the same user each time they log into a service.

What You Have to Do

Create repeatable and consistent login and authentication processes, and to create assurance that end users can engage in authorized transactions with your digital services and ecosystems. You can use its eight Trusted Processes to build assurance into every stage of authentication.

Component 5: Notice & Consent

What This Component Is

Specifies under what conditions a digital service provider must seek consent from end users to collect and share their personal information. Also specifies what data must be retained pertaining to the user's decision(s) in this process.

Why It Matters for Government Organizations

It compliments and ensures compliance with existing privacy legislation and regulations. It also ensures that citizens and other end users of digital services are able to give informed, authorized, and transparent consent to data sharing.

What You Have to Do

Create statements about your collection, use, disclosure, and retention of your end users' data. You can also create processes to ensure your users have the authority to give and manage their consent, and that their consent is informed and valid (freely given, specific, informed, and unambiguous).

Component 6: Verified Person

What This Component Is

Provides processes and criteria for verifying the identities of individual persons who act as end users of digital services. Defines how to ensure these people are real, unique, and identifiable as the person that they say they are within digital ecosystems.

Why It Matters for Government Organizations

It prevents fraud and misuse of digital services by showing how to verify that individuals are real, unique, and identifiable. It also shows how to verify that the end user is an individual, and to use this verification to grant access to digital services and ecosystem with a certain increased level of confidence.

What You Have to Do

Create consistent and reliable processes to both ensure the real-world identity of individuals and to create and maintain digital records of their identity. You can follow its guidelines to define what evidence you can collect that can accurately identify an individual as the person they are presenting as.

Component 7: Verified Organization

What This Component Is

Provides processes and criteria for verifying the organizations who act as end users for digital services. Defines how to ensure they actually exist and are identifiable as the organizations that they say they are within digital ecosystem.

Why It Matters for Government Organizations

It prevents fraud and misuse of digital services by showing how to verify the existence and identity of other government or private sector partners. It also helps establish that the persons and processes that claim to represent that entity are connected to it. Overall, it is a fundamental pre-requisite to making these connections in digital ecosystems with high levels of assurance.

What You Have to Do

Implement seven Trusted Processes to manage the digital identities of organizations, including the evidence required to verify them. You can follow these processes and criteria for establishment, issuance, resolution, validation, verification, maintenance, and linking of the identity of an organization.

Component 8: Credentials (Relationships & Attributes)

What This Component Is

Provides processes and criteria to better understand the individuals and organizations who use digital services, and to verify their relationships with each other — all to enhance the ability to trust them in digital ecosystems.

Why It Matters for Government Organizations

It plays a critical role for the framework, and sets standards for creating, issuing and managing digital credentials. This helps government organizations minimize or eliminate reliance on self-asserted attributes of end users — or of the relationship between them and their representatives or delegates — in order to enhance authentication, and to reduce administrative burden pre and post completion.

What You Have to Do

Identify what entities can issue, endorse or revoke credentials within your digital ecosystem, to construct connections between your services and specific credential issuing entities, and to ensure the full-lifecycle integrity and reliability of any credentials used across the ecosystem.

Component 9: Infrastructure (Technology & Operations)

What This Component Is
Provides guidance to assess privacy and trust within a digital ecosystem's operational policies, plans, technology, and technology operations. Also helps define what infrastructure can meet the recommendations of each PCTF component.

Why It Matters for Government Organizations
It outlines the policies and technologies that government organizations should implement and perform to align with the other components of the framework. These recommendations are tool-agnostic and do not force specific technology purchases.

What You Have to Do
Evaluate and select technologies with the right characteristics and capabilities to drive your digital trust services and ecosystems, and to set up operational processes for compliant security, data oversight and governance, auditability, and support for those technologies.

It gives government organizations privacy-respecting practices to handle digital identities and data for each end users at each digital touchpoint.

Component 10: Privacy

What This Component Is
An all-encompassing component that provides guidance and standardized criteria, assessments, and certifications on how to handle an end user's personal data. Offers guidance on how to create the right privacy policies across digital ecosystems.

Why It Matters for Government Organizations
It gives government organizations privacy-respecting practices to handle digital identities and data for each end users at each digital touchpoint. These practices extend existing data privacy regulations that organizations may already comply with.

What You Have to Do
Ensure your digital services and ecosystem is protecting the privacy of your end users at every stage. You can follow its processes to properly collect personal information, manage changes to it, and to design privacy into every stage of development of your digital services and ecosystems.

How Portage Can Help You Align With the PCTF

Many government organizations lack the resources to align with the PCTF on their own. Portage CyberTech worked with the DIACC and others to draft the PCTF, and aligns its consultations, tools, and services with the framework.

Why Government Organizations May Struggle with the PCTF

Trust and privacy are not new concepts, but establishing them in the digital world creates new challenges. To establish trust online, government organizations must create effective technical and business processes that replace in-person social conventions. To protect privacy online, they must find a way to lock down millions of records that can be linked, inspected, and downloaded in seconds, often by one laptop, while meeting the service expectations of citizens.

While the PCTF tries to make establishing trust and protecting privacy online as simple and actionable as possible, these challenges still represent emerging areas of risk that many government organizations are only now beginning to tackle.

As such, many government organizations lack the tools, teams, and expertise they need to fully understand the PCTF, to assess their compliance against its standards, and to follow its recommendations. Even leaders in privacy and trust may require outside assistance to scope and implement one or more of the PCTF's components.

That's where Portage can help.

To establish trust online, government organizations must create effective technical and business processes that replace in-person social conventions.

Meet Portage: A National Thought Leader on Privacy and Trust

Portage CyberTech provides tools, services, and consultation that build privacy and trust into digital services and ecosystems. Portage provides thought leadership on these topics and has worked directly with a range of government organizations.

Portage also has a unique history with the PCTF. The DIACC contracted Portage to draft the initial version of the PCTF prior to its review by, and contributions from, other public and private organizations. Portage has remained involved with the PCTF, and has worked with the DIACC to incorporate feedback and expand the framework.

At Portage, we align our tools, services, and consultative advice with the PCTF, and provide custom solutions that help government organizations achieve compliance with this end-to-end framework or any of its individual components. Here's how.

Our Trust-Based Processes, Platforms, and Ecosystems

To start, our expert consultants will help you understand where the PCTF applies to your organization and your digital services. We will help you identify the gaps that might exist in your approach to privacy and trust, as well as the specific processes and tools that must be implemented to fill those gaps.

From there, we will begin to define the roles and systems that will move you into compliance with the PCTF, and define how big of an effort it will take to align with this framework. We will help you break down and prioritize the PCTF's recommendations into a project plan that captures quick wins towards greater trust and compliance, and work with you to set up governance to maintain each improvement you build.

In addition, we will work with you to define ecosystems of digital trust that help you outsource some of your authentication, verification, and credentialing to other public and private sector organizations. By identifying and partnering with the right private sector services, we will ensure you don't have to build everything in the PCTF.

From there, we offer end-to-end technology solutions for achieving compliance with the PCTF through our Digital Trust Matrix of tools and services. Each of these services can either be selected modularly or deployed together to build a single, unified, end-to-end trust system. Our tools and services include:

- Ongoing strategy formation, consultation, and guidance
- The CitizenOne platform for identity & access management
- The TrustBuilder platform for verified credentials
- The 1CRM platform for customer and business management
- Seamless digital experiences produced using Drupal

How to Start Aligning to the PCTF Today

The PCTF is here to stay. It's being rapidly adopted by public and private sector organizations, and it's set a new standard for privacy and trust in digital services.

At Portage we remain at the forefront of this framework and this emerging area of cybersecurity and business risk. Together, we can better secure your digital services, maintain compliance with key regulations, and give your users confidence that you respect their data privacy.

Take the next step to work with Portage and to bring the PCTF to life in your government organization. Reach out for a no-obligation consultation today.

www.portagecybertech.com