

AICPA/CICA Generally Accepted Privacy Principles (GAPP)

GAPP is a privacy framework that helps organizations establish, manage, and assess data protection and privacy controls.



What it is

Generally Accepted Privacy Principles (GAPP) is a comprehensive privacy framework that assists organizations in establishing, managing, and assessing data protection and privacy controls. The framework provides a structured approach for addressing privacy risks and maintaining compliance with relevant data protection laws and regulations.

Developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), GAPP is used by organizations, auditors, and compliance professionals across industries. It covers key areas including privacy governance, risk management, data lifecycle controls, and incident response. GAPP is often referenced in alignment with other regulatory and cybersecurity frameworks, such as SOC 2 and international privacy standards.

At a glance

PUBLISHER American Institute of Certified Public Accountants (AICPA)	TYPE Control Framework	VERSION 2011
EFFECTIVE 2006	DOMAIN Privacy	FAMILY SOC Frameworks
REGION United States	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.aicpa-cima.com/resources/download/privacy-management-framework>

Why it matters

- **Strengthen privacy governance** Establish clear accountability and oversight for personal data handling across organizational functions and third-party relationships.
- **Enhance regulatory alignment** Support compliance with diverse privacy regulations by providing a principles-based framework that maps to multiple legal requirements.
- **Build stakeholder trust** Demonstrate commitment to responsible data handling through transparent privacy practices that foster customer and partner confidence.
- **Improve risk management** Identify and mitigate privacy risks systematically through structured assessments and controls aligned with GAPP principles.

How SmartSuite supports GAPP

Privacy Control Library

Structure GAPP principles and criteria into a centralized privacy control library with clear ownership and accountability.

Data Inventory and Processing Records

Track personal data categories, processing purposes, retention rules, and ownership across systems and business processes.

Privacy Risk and Assessment Workflows

Manage privacy impact assessments, risk evaluations, and mitigation actions tied to GAPP privacy principles.

Vendor and Data Sharing Governance

Monitor third-party data processing, contractual obligations, and privacy assurance evidence for vendors and partners.

Privacy Incident Response Workflows

Coordinate investigation, escalation, and response workflows for privacy incidents and potential data breaches.

Privacy Control and Program Maturity Reporting

Provide dashboards showing privacy control status, open risks, incidents, and program maturity across the organization.

Common framework mappings

Official resources

Generally Accepted Privacy Principles (GAPP) Framework

Defines the privacy framework established by AICPA and CICA for managing data protection.

aicpa-cima.com/resources/download/privacy-management-framework

AICPA Privacy Management Resources

Provides resources and guidance for implementing GAPP within organizations.

aicpa-cima.com/resources/download/privacy-management-framework

CICA Privacy Framework Overview

Outlines the principles and application of the GAPP framework in privacy governance.

cpacanada.ca/en/business-and-accounting-resources/Auditing-and-assurance/Canadian-auditing-standards/publications/generally-accepted-privacy-principles

AICPA Trust Services Criteria

Describes the framework for evaluating and reporting on system controls.

aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022

Frequently asked questions

What is GAPP used for?

GAPP is used by organizations to establish, manage, and evaluate comprehensive privacy and data protection programs. It serves as a structured framework for addressing privacy risks, aligning with regulatory expectations, and supporting privacy compliance initiatives.

Is GAPP a certifiable or mandatory framework?

GAPP itself is not a certifiable or legally mandatory framework; it provides best practices and principles for privacy management. However, organizations may be assessed against GAPP criteria during audits, particularly in the context of SOC (System and Organization Controls) reporting.

What is the scope or applicability of GAPP?

GAPP applies to any organization that collects, processes, stores, or transmits personal data, regardless of industry or geography. It is designed to be adaptable to various regulatory environments and is commonly used in conjunction with international privacy laws and standards.

What are the key principles or controls required by GAPP?

GAPP is organized around ten core privacy principles, covering areas such as notice, choice, collection, use, access, disclosure, security, data quality, monitoring, and enforcement. These principles are implemented through specific organizational controls, policies, and procedures.

How do organizations implement GAPP?

Organizations implement GAPP by mapping privacy principles to internal controls and procedures, conducting data inventories, performing privacy impact and risk assessments, and establishing policy frameworks. The process also involves ongoing training, vendor due diligence, and development of incident response mechanisms.

How does GAPP relate to other privacy and cybersecurity frameworks?

GAPP can be aligned with other privacy and information security standards, such as SOC 2, ISO 27001, and GDPR. Its principles complement these frameworks by focusing specifically on privacy controls and facilitating integrated governance and audit processes.

What are the ongoing compliance requirements for GAPP?

Maintaining GAPP compliance requires continual monitoring of privacy controls, regular risk assessments, periodic reviews of policies and procedures, and documenting evidence of effective implementation. Organizations must also ensure their practices remain aligned with evolving privacy regulations and industry standards.

How would SmartSuite support GAPP?

SmartSuite enables organizations to operationalize GAPP by linking privacy controls to risk registers, policy management, and compliance dashboards. It supports evidence collection, compliance tracking, audit readiness processes, and centralized reporting, streamlining ongoing monitoring and documentation for both internal and external stakeholders.

License included / downloadable: No GAPP is published by the AICPA and CICA and requires purchase or licensed access. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/generally-accepted-privacy-principles-gapp