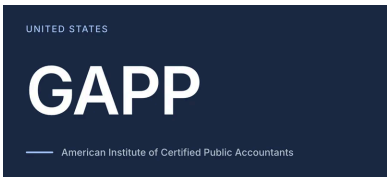
SmartSuite

Framework / Privacy / SOC Frameworks

AICPA/CICA Generally Accepted Privacy Principles (GAPP)

GAPP is the AICPA/CICA privacy framework of 2009, ten principles with measurable criteria, superseded in 2020 by the AICPA Privacy Management Framework.



What it is

Generally Accepted Privacy Principles (GAPP) is the 2009 privacy framework of the AICPA and the Canadian Institute of Chartered Accountants (CICA), built on ten privacy principles with measurable criteria, and it has been superseded: in 2020 the AICPA replaced it with the Privacy Management Framework (PMF), which the AICPA describes as an update to the former 2009 GAPP. GAPP was voluntary, so no organization is required to use it, and new privacy programs should start from the PMF.

The AICPA/CICA Privacy Task Force wrote GAPP for CPAs and CAs who advise on or audit privacy programs and for the organizations that run them. It defines privacy as the rights and obligations of individuals and organizations around the collection, use, retention, disclosure and disposal of personal information, and it organizes those obligations under Management, Notice, Choice and consent, Collection, Use, retention and disposal, Access, Disclosure to third parties, Security for privacy, Quality, and Monitoring and enforcement.

At a glance

PUBLISHER American Institute of Certified Public Accountants (AICPA) with the Canadian Institute of Chartered Accountants (CICA)	TYPE Control Framework	VERSION 2009 edition (superseded by the AICPA Privacy Management Framework, 2020)
EFFECTIVE 2009 (voluntary framework; superseded 2020)	DOMAIN Privacy	FAMILY SOC Frameworks
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

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

Why it matters

- **A complete map of a privacy program** Ten principles run from governance (Management) through the data lifecycle (Collection; Use, retention and disposal; Disclosure to third parties) to assurance (Monitoring and enforcement).
- **Criteria written to be assessed** Each principle breaks into measurable criteria, which is why auditors and SOC practitioners adopted GAPP as a privacy assessment baseline.
- **The 2009 additions still hold** Annual privacy risk assessment, incident and breach management, awareness and training and portable-media protection were added in the 2009 edition and remain in the PMF.
- **A clean path to the successor** The PMF's nine components correspond to the ten GAPP principles, so a GAPP control library converts without losing coverage.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports GAPP

Principle and Criteria Library

Load the ten GAPP principles and their criteria as controls, with owners, status and the PMF component each one maps to.

Migration Tracker

Record for each GAPP criterion whether it has been re-homed in the PMF or the Trust Services privacy criteria, with evidence and a completion date.

Annual Privacy Risk Assessment

Run the assessment GAPP added in 2009 (criterion 1.2.4) as a yearly workflow with findings, treatment decisions and approvals.

Incident and Breach Management

Log privacy incidents with discovery date, assessment, notifications and lessons learned under criterion 1.2.7.

Notice and Consent Records

Keep each privacy notice version, the purposes it states and the consent choices offered, linked to the processing activities they cover.

Assessment Reporting

Report criteria status, open gaps and migration progress to the privacy owner and to the practitioner performing the assessment.

Common framework mappings

SOC 2 (AICPA TSC 2017) | CCPA/CPRA | GDPR | ISO 27701 | NIST Privacy Framework v1.0 | SOC 2

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

CPA Canada — Generally Accepted Privacy Principles

CPA Canada's page on the GAPP framework it co-published with the AICPA.

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

Is GAPP still current?

No. The AICPA replaced GAPP in 2020 with the Privacy Management Framework (PMF), which it describes as an update to the former 2009 GAPP, made because of changes in technology, privacy laws such as the GDPR and the Trust Services Criteria. New programs should start from the PMF.

What are the ten GAPP principles?

Management; Notice; Choice and consent; Collection; Use, retention and disposal; Access; Disclosure to third parties; Security for privacy; Quality; and Monitoring and enforcement. Each principle is broken into measurable criteria that a practitioner can assess.

How does the Privacy Management Framework differ from GAPP?

The PMF has nine components: management; agreement, notice and communication; collection and creation; use, retention and disposal; access; disclosure to third parties; security for privacy; data integrity and quality; and monitoring and enforcement. Choice and consent moved into the agreement and notice component, collection gained creation, and quality became data integrity and quality.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Can an organization still be assessed against GAPP?

A practitioner can assess against any criteria a client chooses, but the AICPA no longer distributes GAPP, so current engagements use the PMF or the privacy category of the Trust Services Criteria, which SOC 2 reports use. Organizations with GAPP-based programs typically map each criterion to its PMF component and assess against that.

Who published GAPP and when?

The AICPA/CICA Privacy Task Force of the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants published it. The edition the PMF replaced is the 2009 edition, issued after a March 13, 2009 exposure draft and following an earlier 2006 edition.

License included / downloadable: No GAPP is no longer distributed by the AICPA. Its successor, the Privacy Management Framework, can be downloaded from the AICPA with a free account; neither text is included with the platform.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.