Fill the GAPP: generally accepted privacy principles are little-known, but mighty useful.

Print

Title Annotation: *GAPPNEWS*
Author: *Harden, Stuart H.*
Date: *Oct 1, 2007*
Words: *1211*
Publication: *California CPA*
ISSN: *1530-4035*

No, it's not a misprint.

Although many CPAs have spent much of their professional life dealing with GAAP (generally accepted accounting principles), this article concerns GAPP--generally accepted privacy principles.

WHAT IS GAPP?

We are all familiar with privacy concerns: the rights and obligations of individuals and organizations with respect to the collection, use, disclosure and retention of personal information. We have all submitted personal information to organizations. We have been provided with privacy notices by organizations that collect our data and have received assurance that our personal information will be kept confidential and only shared with others in certain disclosed instances. We have been informed that we can opt not to have our information shared with others.

Still, how can we be assured that our information is safe?

Developed as a joint project of the AICPA and the Canadian Institute of Chartered Accountants, GAPP is a tool for all CPAs.

CPAs in public practice will be able to offer clients a range of services, including privacy strategic and business planning; privacy gap and risk analysis; privacy policy design and implementation; and independent verification of privacy controls, which includes attestation engagements. And CPAs in industry can enhance their value to their employers by offering privacy advisory services and performing internal assessments against something they can measure--GAPP.

UNDERLYING PRINCIPLES

There are 10 generally accepted privacy principles:

1. Management: The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.

2. Notice: The entity provides notice about its privacy policies and procedures and identifies the

purposes for which personal information is collected, used, retained and disclosed.

3. Choice and Consent: The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.

4. Collection: The entity collects personal information only for the purposes identified in the notice.

5. Use and Retention: The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.

6. Access: The entity provides individuals with access to their personal information for review and update.

7. Disclosure to Third Parties: The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. Security for Privacy: The entity protects personal information against unauthorized access.

9. Quality: The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.

10. Monitoring and Enforcement: The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

GAPP may be used by organizations for privacy policy design and implementation, performance measurement, benchmarking, and monitoring and auditing of privacy programs. In managing a privacy program, GAPP may be used in strategizing (planning); diagnosing (risk analysis); implementing (developing solutions); sustaining (monitoring) and auditing (evaluation by internal or external auditors).

AIDS IN APPLYING THE PRINCIPLES

Included with GAPP are aids to understand and implement the principles. For example, guidance is provided in the use of GAPP to develop a vision, perform strategic planning, and in resource allocation, all of which are essential elements of strategizing.

[ILLUSTRATION OMITTED]

Detailed criteria are included for each of the 10 principles:

* Subheadings for each principle. For example, management criteria includes subheadings that consider establishment of privacy policies; communication of policies to internal personnel; assigning responsibility and accountability for the policies; review and approval of policies; assessing consistency of policies with laws and regulations; assessing consistency of policies with internal procedures; qualifications of internal personnel; and addressing changes in the business and regulatory environment.

* For each subheading, explanations are provided. For example, when communicating policies to internal personnel, suggestions are made regarding periodic communication (such as through a website or newsletter), obtaining confirmation from personnel as to their understanding of and compliance with the policies, and education and training of personnel as to policies/procedures.

* Additional considerations are provided to clarify the criteria. For example, it is clarified that the person accountable for privacy should be from the entity.

PRACTITIONER SERVICES

Appendices C and D to GAPP, which are included only with the CPA/CA Practitioner Version, provide information to practitioners who are asked to provide some form of assurance or consulting services in connection with an entity's privacy policies and procedures.

Appendix C observes that practitioners can provide various privacy services including advising clients on system weaknesses, assessing risk and recommending a course of action using GAPP as a benchmark. It is observed that, in the United States, such services are covered by the Standards for Consulting Services.

Assurance services may also be provided. In the United States, such services are covered by Standards for Attestation Services. GAPP provides the necessary accepted criteria against which to measure assertions (similar to the function of GAAP in financial statement assertions) and allow for attestation engagements to be performed. Attestation standards provide for examinations, reviews and agreed-upon procedures engagements.

Examination (audit) engagements result in a high level of assurance. The scope of the audit should include all 10 principles, but may be limited to only certain aspects of personal information or certain business segments. The scope of the audit should normally be no broader than the scope of the privacy notice. The report should ordinarily cover a period of time (not less than two months); however, an initial report can be a point-in-time report.

Appendix D includes example audit reports. The standard report includes:

* A statement that an examination has been performed of the entity's controls over the collection of personal information and its compliance with its commitments in its privacy notice;

* A statement that the examination was performed in accordance with attestation standards (in the United States); and

* An opinion whether, in all material respects, the entity maintained effective controls over privacy of personal information in conformity with its privacy notice and GAPP, and complied with the commitments in its privacy notice.

The report may also refer to management's assertions regarding privacy and an example report is provided for those situations where management's report accompanies the practitioner's report. Examples are also provided for management's assertion and practitioner reports issued under Canadian attestation standards.

Appendix C does not recommend that reviews be performed due to the difficulty in conveying the limited assurance resulting from a review engagement. Agreed-upon procedure engagements

are encouraged, however, due to the wide range of user needs in the privacy area.

BRINGING IT ALL TOGETHER

Most organizations encounter challenges in managing privacy on a local, national or international basis, and most are faced with a number of differing privacy laws and regulations.

GAPP has referenced significant domestic and international privacy regulations, and has brought together these complex privacy requirements into a single privacy objective that can be used by any organization.

Stuart H. Harden, CPA, CFE is a director in the litigation and forensic consultants group of Hemming Morse, Inc. in San Francisco. You can reach him at hardens@hemming.com.

BY STUART H. HARDEN, CPA

RELATED ARTICLE: GAPP INFO

Want More?

Find more GAPP resources at http://infotech.aicpa.org/Resources/Privacy/Generaly+Accepted+Privacy+Principles/.