

Summary of Major Changes Made to Generally Accepted Privacy Principles

Principle	Criteria	Summary of Change
Management	1.2.3 Personal Information Identification and Classification	New criterion that requires (1) identification of the types of personal information and sensitive personal information and the related processes, systems and third parties involved in the handling of such information and (2) that such information is covered by the entity's privacy and security policies.
Management	1.2.4 Risk Assessment	New criterion that requires an entity to use a risk assessment process to establish a risk baseline and to at least annually identify new or changed risks to personal information.
Management	1.2.6 Infrastructure and Systems Management	Expanded criterion that now restricts the use of personal information in process and systems testing.
Management	1.2.7 Privacy Incident and Breach	New criterion that requires a documented privacy incident and breach management program to be implemented and sets forth the minimum requirements for

		such a program.
Management	1.2.10 Privacy Awareness and Training	New criterion that requires an entity to provide a privacy awareness program on its privacy policies and related matters, and specific training for selected personnel. This requirement was previously covered by other criteria, which have now been moved combined into one criterion.
Collection	4.2.4 Information Developed about Individuals	New criterion that requires an entity to inform individuals if the entity develops or acquires additional information about them for its use.
Use, Retention, and Disposal		Principle was modified to include the disposal of personal information.
Use, Retention, and Disposal	5.2.3 Disposal, Destruction and Redaction of Personal Information	New criterion that requires personal information which is no longer retained, to be anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.
Access	6.2.7 Escalation of Complaints and Disputes	This criterion was removed due to duplication in 10.2.2 Dispute

		Resolution and Recourse.
Security for Privacy Principle	8.2.1. The Information Security Program	The criterion was modified to require the security program to address certain matters and to include references to ISO/IEC 27002:2005, Information technology—Security techniques—Code of practice for information security management.
Security for Privacy Principle	8.2.6 Personal Information on Portable Media	New criterion that requires personal information stored on portable media or devices to be protected from unauthorized access.
Monitoring and Enforcement	10.2.5 Ongoing Monitoring	New criterion that requires that an entity to have ongoing procedures for monitoring the effectiveness of controls over personal information, based on a risk assessment, and for taking timely corrective actions.