Professional Perspective

Updated ISO Standards Require Enhanced Information Governance

Chuck Ragan, Redgrave LLP & Tom Seymour, Redgrave Data

Bloomberg Law

Updated ISO Standards Require Enhanced Information Governance

Contributed by Chuck Ragan, Redgrave LLP & Tom Seymour, Redgrave Data

In October 2022, the International Organization for Standardization (ISO) released a revised ISO 27001 on information security, cybersecurity, and privacy protection requirements for information security management systems (ISMS).

This is the first revision to ISO 27001 since 2013, and several of the updates signal an increased recognition of the critical role information governance plays in information security management. Interestingly, many of the themes found in new ISO 27001 controls are consistent with the guidelines ISO set forth earlier in 2022 when it promulgated ISO 24143 on Information Governance.

The modifications to the body of ISO 27001 are modest, but the Annex of information security controls was substantially restructured, with the total number of controls being reduced (from 114 to 93, largely through consolidation) and 11 new controls added.

This article focuses on several of the new controls aimed at data masking, managing data in the cloud, enhanced monitoring, and deleting information to align with data minimization requirements. These new controls are likely to impact data privacy and cybersecurity policies and procedures, as well as information governance programs and initiatives.

A Family of Standards

ISO, according to its website, "was founded with the idea of answering a fundamental question: 'what's the best way of doing this?'" Traditionally, when an organization is certified as complying with an ISO, it means "that consumers can have confidence that their products are safe, reliable and of good quality." ISO standards are important for any organization devoted to ensuring the quality and safety of their products and operations—whether automotive, healthcare, industrial equipment, energy, or technology.

ISO 27001 is one of a family of standards regarding information security management systems. ISO 27000 is the parent of the family and contains definitions for vocabulary used throughout the family.

The 27000 family of standards "enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties," according to the ISO website. ISO also released an update to family member ISO 27002 related to information security controls earlier this year, which includes guidelines that will be instructive for implementation of revised ISO 27001.

The information security management landscape has evolved significantly since ISO 27001 was last revised in 2013. At that time, migration of enterprise systems and applications to the cloud was only beginning to gain traction; the General Data Protection Regulation (GDPR) did not come into effect until five years later, with comprehensive state privacy regulations, including the California Consumer Privacy Act (CCPA) following shortly thereafter.

Security controls have not kept pace with these developments. For example, the most recent Ponemon-IBM Data Breach Survey, which tracks the costs—including redress for exposing personal data—of data breaches, found that costs associated with cloud-originated breaches were higher than on-premises incidents. In addition, the survey reported that 45% of cybersecurity incidents originated in the cloud, but 43% of responding organizations had not started or were only in the early stages of applying practices to secure their cloud environments.

Significant Added Controls

Against that background, it is not surprising to see in the 2022 ISO 27001 revision, new controls promulgated for managing data in the cloud, data masking, enhanced monitoring, and deleting information to align with data minimization requirements. The table below highlights several of the new controls and the types of information governance initiatives companies can undertake.

Control	Description	Supporting Information Governance Initiatives
5.23	**Acquiring cloud services, managing data in the cloud, and exiting from a cloud service provider arrangement:** Control 5.23 requires processes for acquisition, use, management, and exit from cloud services in accordance with the organization's security requirements.	• Inventory cloud service arrangements, and identify systems that store sensitive information • Update processes for contracting with cloud service providers to include requirements related to the identification, management, retention, and disposition of information, generally and specifically sensitive information • Audit cloud service providers and other business partners for compliance with information security requirements
8.10	**Information deletion to align with data minimization requirements in recent data privacy regulations:** Control 8.10 states that information stored in information systems, devices, or in other media shall be deleted when no longer needed.	• Conduct audits and assessments to identify information that is no longer needed or past its prescribed retention period • Collaborate between business, IT, and legal to identify data that must be preserved for legal or regulatory requirements • Retire legacy systems and databases no longer needed • Remediate caches of hardware devices, storage infrastructure, or disaster recovery data that have been preserved but are no longer needed, such as laptops, mobile phones, storage servers, backup tapes, etc.
8.11	**Data masking:** Control 8.11 requires masking data in accordance with an organization's topic-specific policies, in combination with access controls, to reduce the likelihood of exposure of sensitive information in the event of a breach.	• Identify where sensitive information exists, leveraging earlier initiatives where possible • Evaluate enabling technologies • Use data pseudonymization or anonymization where possible
8.12	**Data leakage:** Control 8.12 requires that measures be applied to systems, networks, and other devices that process, store, or transmit sensitive information.	• Align with efforts to identify and inventory systems that process, store, or transmit sensitive information so that appropriate measures can be applied
5.22 7.4 8.16	**Monitoring:** Several controls in the revised ISO 27001 require enhanced monitoring. Control 5.22 requires monitoring, review, and change management of supplier services and seems to assume that existing suppliers have some security practices in place. Control 7.4 requires continuous monitoring for unauthorized physical access. Control 8.16 requires monitoring of networks, systems, and applications for anomalous behavior with appropriate actions taken to evaluate potential security incidents.	• Align with efforts to identify and inventory systems that process, store, or transmit sensitive information so that appropriate measures can be applied • Align with audit and quality assurance practices to monitor not only for security but also for compliance with information governance policies

In combination, an organization's need to conform with these new controls should lead to stronger collaboration among IT, security, and legal personnel responsible for data privacy and discovery on data minimization, data masking, and security arrangements with cloud service providers and other business partners. Organizations should establish procedures to ensure these issues are addressed in all service level agreements, reviewed periodically, and updated as necessary.

The same forces—the need to delete data no longer needed defensibly and without exposing personal data—should drive more cooperation and coordination between and among the above-named groups as well as the information governance and records management teams responsible for defensible disposition projects.

Revised Requirements in ISO 27001

As noted above, there are some modest adjustments to the requirements in the body of the revised ISO 27001. These include enhancements regarding:

- **Interested Parties**: Interested parties, which are defined in the parent ISO 27000 as persons or organizations "that can affect, be affected by, or perceive [themselves] to be affected by a decision or activity." As a bookend to the need to shore up security with cloud service providers and business partners, the revised ISO 27001 requires an organization to determine the relevant requirements of interested parties.
- **Top Management Review**: As with its predecessor, revised ISO 27001 requires top management, which the parent ISO 27000 defines as the "person or group of people who directs and control an organization at the highest level," to review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. It also adds a requirement that top management's review include consideration of changes in the needs and expectations of interested parties that are relevant to the ISMS.
- **Planning New Processes**: The predecessor ISO 27001 required that an organization establish an ISMS, maintain it, and continually improve it. Clause 4.4 of the 2022 update adds a requirement that the organization include the processes needed to meet the requirements of the ISO; Clause 6.3 adds a requirement that changes to an ISMS be carried out in a planned way; and Clause 8.1 on operationalizing an ISMS added a requirement that in planning to implement changes to the ISMS, the organization should establish criteria for the processes and implement the processes in accordance with the criteria.

Conclusion

Complying with the revised standard will not be optional. Security threats continue to evolve and become more sophisticated, and regulators have proposed new rules that will require organizations to provide more transparency about their efforts to manage and protect against cyber incidents. See, e.g., SEC Fact Sheet, Public Company, Cybersecurity; Proposed Rules; New York State, Department of Financial Services, Press Release, Nov. 9, 2022.

The revised ISO 27001 does not affect current certifications. Entities that certify an organization's compliance with ISO 27001 will begin to measure organizations against the revised ISO 27001 by no later than Oct. 31, 2023, and organizations have until Oct. 31, 2025, to transition to the revised ISO 27001. The 2022 update of ISO 27002 aligns with the controls listed in the Annex of the revised ISO 27001 and should provide reasonable guidance on implementing the new controls.

If compliance with the new international standards and proposed domestic regulations is to be achieved, it will require top management commitment, adequate resources, diligence, cross-functional collaboration among diverse stakeholders responsible for technology, data privacy, discovery, security, and information governance within an organization, oversight of governing bodies—such as boards—and guidance from knowledgeable professionals.