SECURITY

Revisions released around internationally recognized information security standards

Image by vectorjuice via Freepik

July 15, 2022

Christopher Denton

With standards bodies represented from more than 160 countries, the International Organization for Standardization, more commonly referred to ISO, is often seen as a gold standard for certifications. What many might not know is that the ISO seeks to update standards around its frameworks every five to seven years after a comprehensive review. The process takes several years to complete.

A review of ISO 27002 began in March 2018 and the draft international standard (DIS) was released in January 2021. After much review, the full standard was released on February 15, 2022 and supersedes ISO 27002:2013.

What is ISO 27002 all about?

Most organizations have heard of ISO 27001, which is a standard designed to manage and monitor information security management systems while mitigating risk. While ISO 27001 is a standard that an organization can be certified against, ISO 27002 is supplementary guidance and a set of best practices for controls that can be implemented as part of an ISO 27001 program.

Up until the update earlier this year, ISO 27002 provided a normative set of controls that aligned with Annex A of ISO 27001.

What Changed?

While the overall structure of ISO 27002 has changed greatly since the previous release in 2013, the intent of the guidance remains the same and is now even more focused on supporting ISO 27001.

Some of the key differences of ISO 27002:2022 from ISO 27002:2013 are:

1. A reduction in the total control count: Previously 114, the control count in the new guidance is only 93.

2. An introduction of several new controls: To be precise, 11 new controls were introduced to address the ever-changing IT landscape. They include:

- 5.7 Threat intelligence
- 5.23 Information security for use of cloud services
- 5.30 ICT readiness for business continuity
- 7.4 Physical security monitoring
- 8.9 Configuration management
- 8.10 Information deletion
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.16 Monitoring activities
- 8.23 Web filtering
- 8.28 Secure coding

3. Redundant/similar controls were merged: This is most visible with information security policies, asset management, media, access control, logging, and change control.

4. Reorganization of controls: The controls throughout the guidance were reorganized into four categories instead of the 14 domains that existed previously.

- Clause 5: Organizational
- Clause 6: People
- Clause 7: Physical
- Clause 8: Technological

In addition, every control within ISO 27002:2022 contains a purpose for applying the control, and attributes that allow them to be organized and filtered in such a way that is useful to the organization, as is outlined here:

- Control types: Preventive, Detective, and Corrective
- Information security properties: Confidentiality, Integrity, and Availability
- Cybersecurity concepts: Identify, Protect, Detect, Respond, and Recover
- Operational capabilities: Governance, Asset Management, Information Protection, Human Resource Security, Physical Security, System And Network Security, Application Security, Secure Configuration, Identity and Access Management, Threat and Vulnerability Management, Continuity, Supplier Relationships Security, Legal and Compliance, Information Security Event Management, and Information Security Assurance
- Security Domains: Governance and Ecosystem, Protection, Defense, And Resilience

Connectivity to ISO 27017/27018/27701

If your organization already complies with ISO 27017, 27018, and/or 27701, you might wonder what these updates mean for you.

The updates made to ISO 27002:2022 do not prevent organizations from being assessed against these other supplements and standards; however, some work is needed to map them to ISO 27002:2022 until those standards are also updated.

You should keep an eye open for updates to those standards but, generally, you will have time to comply with any revisions without risking the loss of your certification.

Looking Ahead

Stay in contact with your certification body for updates. As mentioned at the start of this article, reviews take substantial lengths of time, so organizations should not be surprised that new guidance is likely to emerge.

Furthermore, if your organization is currently assessing against ISO 27001:2013, continue to do so while preparing for the 11 new controls. This will ensure that the transition is not as drastic.

If you are just at the beginning of your journey with ISO, consider adopting the ISO 27002:2022 controls using Annex B as a guide in order to be as proactive as you can in securing one of your organization's most valuable assets — its information.

This article originally ran in *Today's Cybersecurity Leader*, a monthly cybersecurity-focused eNewsletter for security end users, brought to you by *Security* magazine. Subscribe here.

Christopher Denton, CISA, ISO Practice Lead at Marcum LLP, a national accounting and advisory services firm, can be reached at christopher.denton@marcumllp.com for any questions or comments.

Design, CMS, Hosting & Web Development :: ePublishing