Refresh of Key ISO/IEC Series Standards for Information Security

- A SNIA Industry Advisory

Industry advisory to SNIA members and other interested parties on a forthcoming refresh of international standards for information security

Thomas Rivera, CISSP & P.K. Gupta
Co-Chairs, SNIA Data Protection & Privacy Committee

Eric Hibbard, Chair, SNIA Security Technical Work Group

Table of Contents

Introduction

The purpose of this Advisory is to inform SNIA member companies and other interested parties of significant forthcoming changes to the ISO/IEC 27001 and ISO/SEC 27002 Information Security standards, an overview of the changes, and where to get further information.

Details of Standards

The ISO 27000 Family of Standards is a series of information security standards that provide a global framework for information security management system (ISMS) practices. Of these standards, ISO/IEC 27001 is arguably the most popular because it is currently the only standard that can provide an organization with an audited certification.

ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size, or nature.

The standard contains a set of clauses (i.e., 4 to 10) that provide requirements that are mandatory if an organization wants to be compliant with the standard. The 2013 edition of the standard also includes an annex (Annex A) that currently provides a guideline for 114 control objectives and controls.

As a framework, ISO/IEC 27001 influences the structure and content of information security policies and practices of numerous companies and organizations around the world, independently of whether they seek formal certification.

ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

ISO/IEC 27002:2013 is a supplementary standard that focuses on the information security controls that organizations might choose to implement. These controls are listed in Annex A of ISO/IEC 27001 as one or two sentence descriptions. In ISO/IEC 27002, each of the 114 controls has text that explains how each control works, what the objective is, and how the control can be implemented.

What is Changing?

After a significant effort on the part of ISO/IEC JTC 1/Subcommittee 27 (SC 27), the 3rd edition of ISO/IEC 27002 was published on 21st February 2022. In addition, ISO withdrew ISO/IEC 2702:2013 and two associated corrigenda on 22nd February 2022.

The new ISO/IEC 27002:2022, *Information Security, Cybersecurity and Privacy Protection - Information Security Controls* has been completely rewritten. The following are noteworthy:

- The control sets are now organized into four (4) categories or themes as opposed to fourteen (14) control domains. The 4 categories include Organizational, People, Physical, and Technological.
- There are a total of 93 controls, down from 114. There are 11 new controls, 24 controls that were merged from two, three, or more controls from the 2013 version to avoid control redundancy, and 58 controls from the 2013 version that were reviewed and revised to better align with the current information security and cybersecurity landscape.
- A “purpose” element has been applied to the controls within the 2022 version, as opposed to the use of a control objective for a group of controls.
- The concept of “attributes to controls” has been introduced, with the intention of enhancing the risk assessment and treatment approach. These attributes create different views or different categorizations of controls as seen from a different perspective to the control themes.

With the publication of ISO/IEC 27002:2022, ISO/IEC 27001’s Annex A is no longer synchronized with ISO/IEC 27002. To address this situation, an amendment to ISO/IEC 27001:2013 that updates Annex A to match the new controls in ISO/IEC 27002 is under development. After the amendment has been approved, a new edition of ISO/IEC 27001 will be produced from the consolidation of ISO/IEC 27001:2013, the new amendment, and existing corrigenda. Publication of the new edition of ISO/IEC 27001 could occur as early as August 2022.

With publication of ISO/IEC 27001:2022, organizations that currently hold ISO/IEC 27001:2013 based certifications will have a transition period (anticipated to be 24 months) to recertify with the new controls.

Need for the Project:

The refresh of the standard was needed to bring new features and controls that reflect the advances in business practices, technologies, applications, and services that have been developed in the digital world in recent years. The new edition will provide significant help to organizations and businesses to protect their information, and that of their customers, from a wide range of risks and threats.

Timeline (projected)

- ISO/IEC 27002:2022 corrected version published March 2022
- ISO/IEC 27001:2013/Amendment 1 approved 26th April 2022 (ISO ballot)
- ISO/IEC 27001 minor revision (ISO 8-week FDIS ballot) initiated as early as mid-June 2022
- ISO/IEC 27001:2022 published as early as August 2022
- ISO/IEC 27001:2013 based certifications expire 24 months after publication of ISO/IEC 27001:2022

SNIA Guidelines and Recommendation

Given the outsized role that ISO/IEC 27001 plays in ISMS and how organizations use it, many organizations are likely to undertake comprehensive reviews of their policies and practices. These activities are likely to have an impact on the storage industry, especially as other elements of the ISO 27000 series realigned with the new ISO/IEC 27001 and ISO/IEC 27002 (e.g., ISO/IEC 27040 covering storage security is already under revision).

It is recommended that you examine the details of the standard as it is likely to be adopted as part of the broader storage security standards published by ISO. Organizations that currently hold ISO/IEC 27001:2013 based certifications will have a transition period (anticipated to be 24 months) to recertify with the new controls.

Additional Reference Material

The documents listed below are international standards and are available to purchase from ISO using the links below:

- ISO/IEC 27001 Information technology — Security techniques (2013 version) Currently undergoing a refresh

- ISO/IEC 27002 Information technology — Information security, cybersecurity, and privacy protection (2022 version)

Usage

Disclaimer

The information contained in this publication is subject to change without notice. SNIA makes no warranty of any kind in regard to this advisory, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SNIA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this advisory. Suggestions for revisions should be directed to https://www.snia.org/feedback/.

About the Data Protection & Privacy Committee (DPPC)

The DPPC is committed to the awareness and adoption of data protection technology, and to provide education, best practices and technology guidance on all matters related to the protection and privacy of data. This charter extends the focus of the DPPC into areas of data privacy, regulatory compliance, and a more generic view of protecting data.

This mission, in collaboration with other relevant groups, such as the SNIA Security Technical Work Group, is to deliver a point of reference for customers looking to improve their management of primary data assets and reduce exposure to external threats.

If you are interested in supporting this committee, please email askdppc@snia.org

About SNIA

The Storage Networking Industry Association is a not-for-profit global organization, made up of member companies spanning the storage market. As a recognized and trusted authority for storage leadership, standards, and technology expertise worldwide, SNIA's mission is to lead the storage industry in developing and promoting vendor-neutral architectures, standards, and educational services that facilitate the efficient management, movement, and security of information.

Storage Networking Industry Association
5201 Great America Parkway, Suite 320 • Santa Clara, CA 95054 • Phone: 719-694-1380 • Fax: 719-694-1389 • www.snia.org