SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

ISO 27000-series Update for ISMS

Eric Hibbard, CISSP, CIPP/US, CISA

Samsung Technologies, Inc.

A SNIA Event

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

- The ISO/IEC 27000-series standards provide an information security framework designed to assist organization in managing cyber-attack risks and improving their information security practices. It does this by setting out information security management system (ISMS) requirements and guidance, providing a systematic approach to risk management that focuses on people, processes, and technology. At the heart of this series is the ISO/IEC 27001 standard with its ISO/IEC 27002 companion, which are used internationally by organizations seeking to certify their ISMS. With the February 2022 publication of the third edition of ISO/IEC 27002, the stage has been set for a wave of changes for the ISO/IEC 27000-series that will also impact ISO/IEC 27001 certifications.

- This session will highlight the changes for the third edition of ISO/IEC 27002 and explain the ramifications to the entire series, including anticipated timelines. The last such changes in 2013 had a significant impact on the security community and early indications are that the new ISMS requirements and guidance are non-trivial changes.

Background

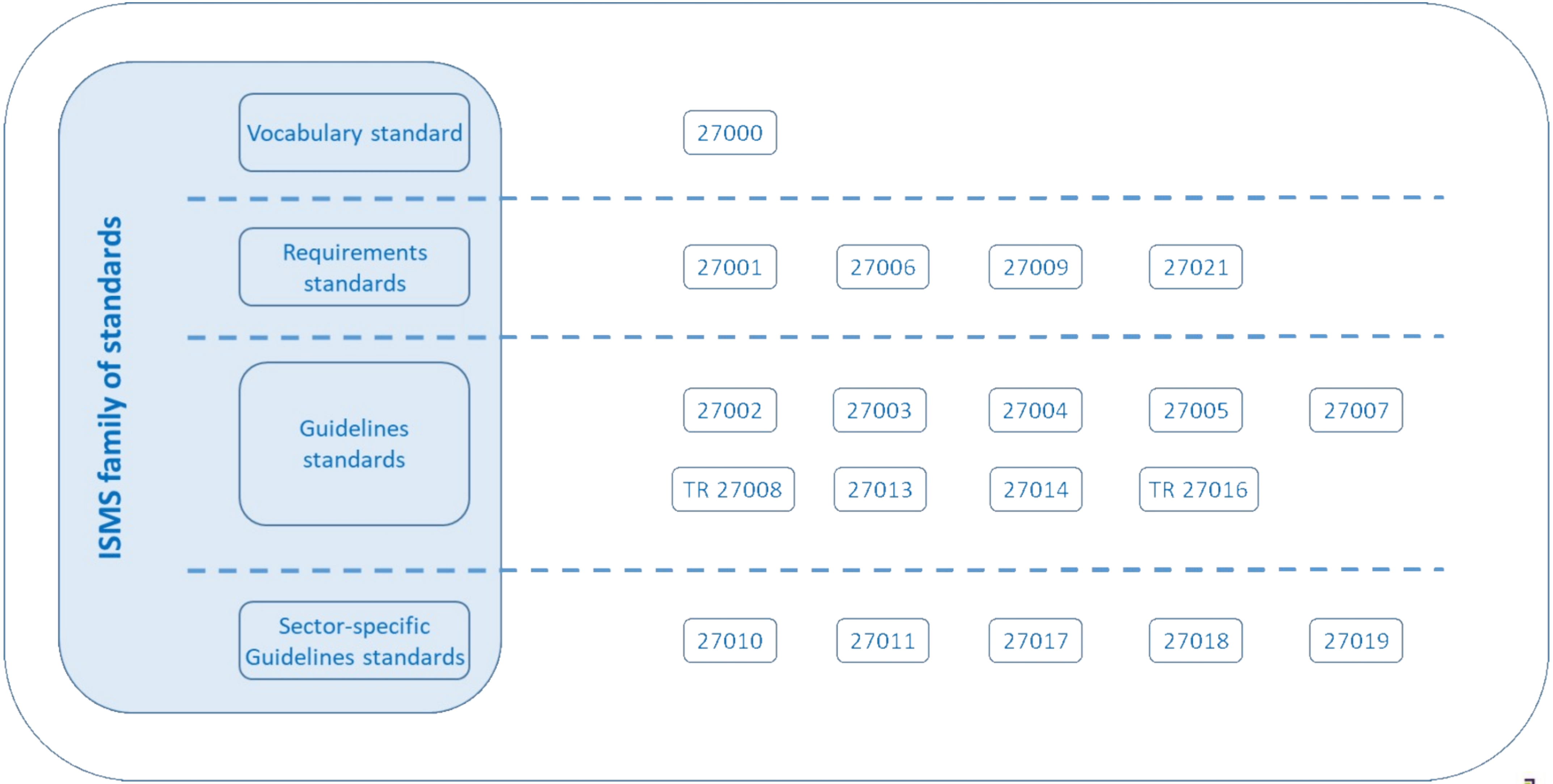
Introduction to ISO/IEC 27000-series Standards

- Provide best practice recommendations on the management of information risks through information security controls within the context of an overall information security management system (ISMS)
- They are not specific to any industry and can be applied in any business, regardless of size and industry
- The ISMS concept incorporates continuous feedback and improvements to respond to the changes in threats or vulnerabilities that occurred as a result of incidents.
- There are about 65 standards in the series
- Sometimes called the “ISMS Family of Standards” or “ISO27K” for short

Source of the ISO/IEC 27000-series Standards

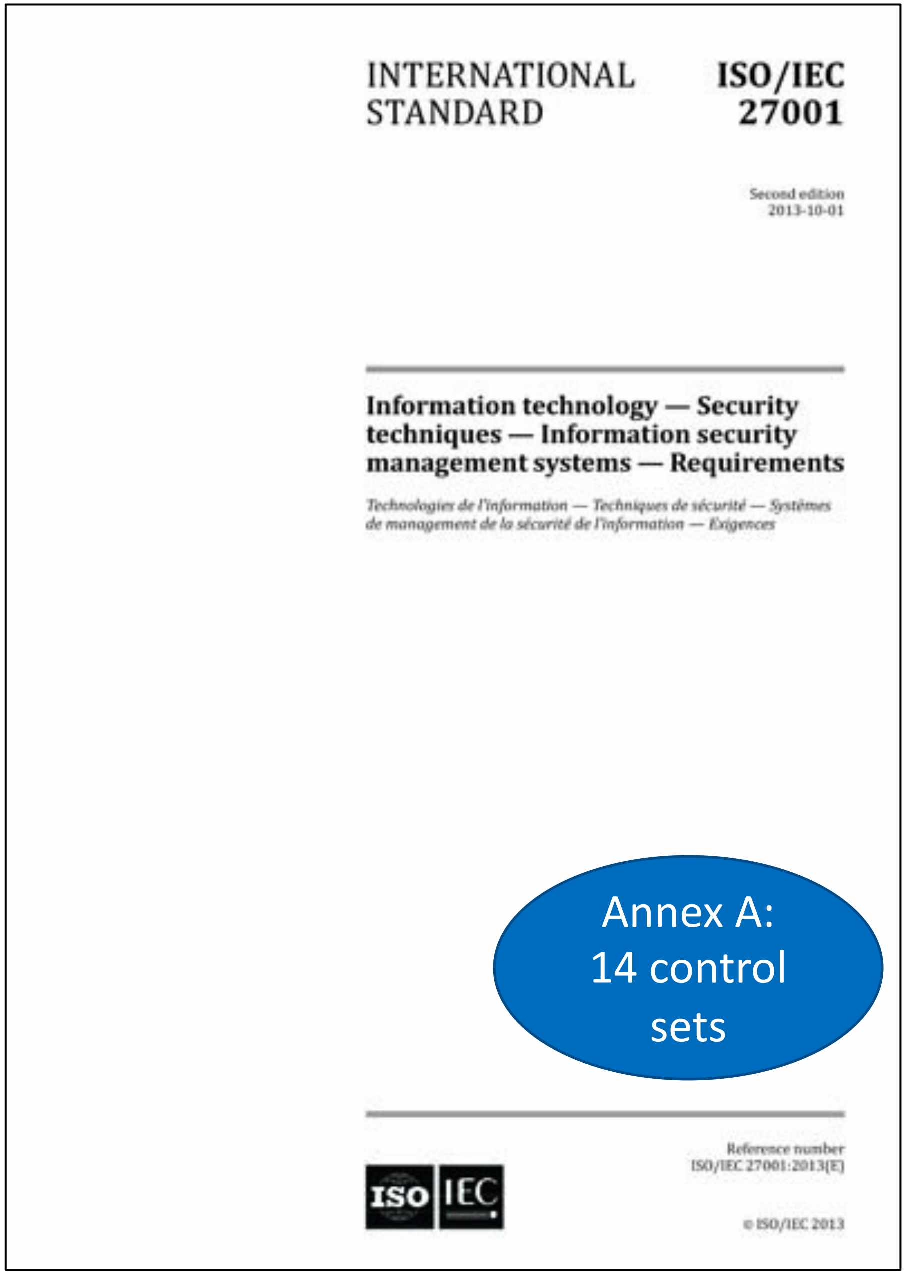
- Produced by:
  - International Organization for Standardization (ISO) and
  - International Electrotechnical Commission (IEC)
  - Working under Joint Technical Committee 1 (JTC 1) Information technology
  - With development managed by Subcommittee 27 (SC 27) Information security, cybersecurity, privacy protections
- Over 80 countries (national bodies) are members of SC 27; about 50 are voting members
- SC 27 has liaisons with about 35 internal ISO organizations
- SC 27 has liaison with about 50 external organizations

Core Standards



ISMS family of standards

Vocabulary standard	27000				
Requirements standards	27001	27006	27009	27021	
Guidelines standards	27002	27003	27004	27005	27007
	TR 27008	27013	27014	TR 27016	
Sector-specific Guidelines standards	27010	27011	27017	27018	27019



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

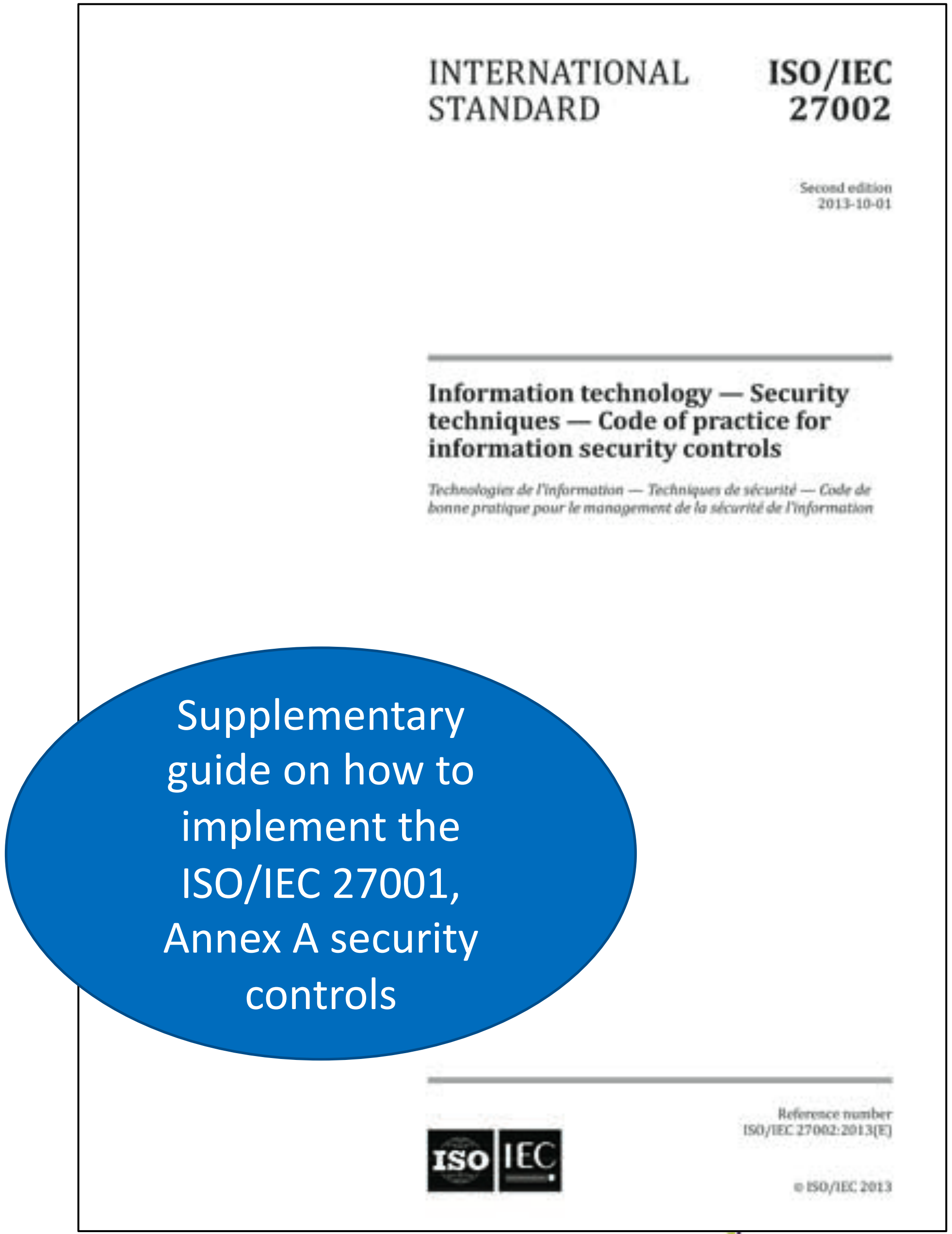
Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Annex A:
14 control
sets



INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Reference number
ISO/IEC 27002:2013(E)

© ISO/IEC 2013

Supplementary guide on how to implement the ISO/IEC 27001, Annex A security controls

ISO 27001 Certification

- Means that the organization's ISO 27001 ISMS has been certified in compliance with the standard by auditors known as certification bodies
- Once a certification body issues an ISO 27001 certificate to an organization
  - It is valid for a period of three years
  - The certification body will perform surveillance audits to evaluate if the organization is maintaining the ISMS properly, and if required improvements are being implemented in due time
- Changes to ISO/IEC 27001 (new edition) cause existing ISO 27001 certification to expire after a transition period (typically 24 months)

The Update Journey

The New ISO/IEC 27002:2022

- Published February 2022; supersedes the 2013 version
- Significant changes to the standard
- Many standards in the ISO/IEC 27000-series have specific references to ISO/IEC 27002; they are now broken

- The 14 control domains are now organized into 4 categories: Organizational, People, Physical, and Technological
- There are a total of 93 controls in the ISO/IEC 27001:2022 (21 less than ISO/IEC 27002:2013):
  - 11 controls are new;
  - 24 controls were merged from two, three, or more controls from the 2013 version
  - 58 controls from the 2013 version were reviewed and revised to better align with the current information security and cyber security environment
- There was a concentrated effort to avoid control redundancy.
- 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
  - Intention of enhancing the risk assessment and treatment approach
  - Allows the creation of different views—i.e., different categorizations of controls as seen from a different perspective to the control themes

Update Roadmap

- ISO/IEC 27001 is being updated
  - Amendment underway to replace the contents of Annex A with contents aligned with ISO/IEC 27002:2022
  - A new edition of ISO/IEC 27001 will be produced later this year; consolidation of amendment and corrigenda
- Other revisions underway
  - ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary
  - ISO/IEC 27005, Information security, cybersecurity and privacy protection — Guidance on managing information security risks
  - ISO/IEC 27006-1, Requirements for bodies providing audit and certification of information security management systems — Part 1: General
  - ISO/IEC 27006-2, Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems
  - ISO/IEC TS 27008, Information technology — Security techniques — Guidelines for the assessment of information security controls
  - ISO/IEC 27009, Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements
  - ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
  - ISO/IEC 27701, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Summary

- The major update of ISO/IEC 27002 has created issues for all documents that references specific clauses
- ISO/IEC 27001 is queued for updates
  - Annex A get a facelift
  - New edition will impact existing ISO 27001 certifications (24-month transition)
  - Full revision of ISO/IEC 27001 is planned to start in late 2022 with publication anticipated in 2025
- Several of the ISO/IEC 27000-series are undergoing revisions that are primarily focused on realigning with the new ISO/IEC 27002
- Many other ISO standards are likely to be updated to reflect changes to the ISO/IEC 27000-series

SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

Please take a moment to rate this session.

Your feedback is important to us.