

HCIA - Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 1 Part 3

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Information Security Standards and Specifications



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

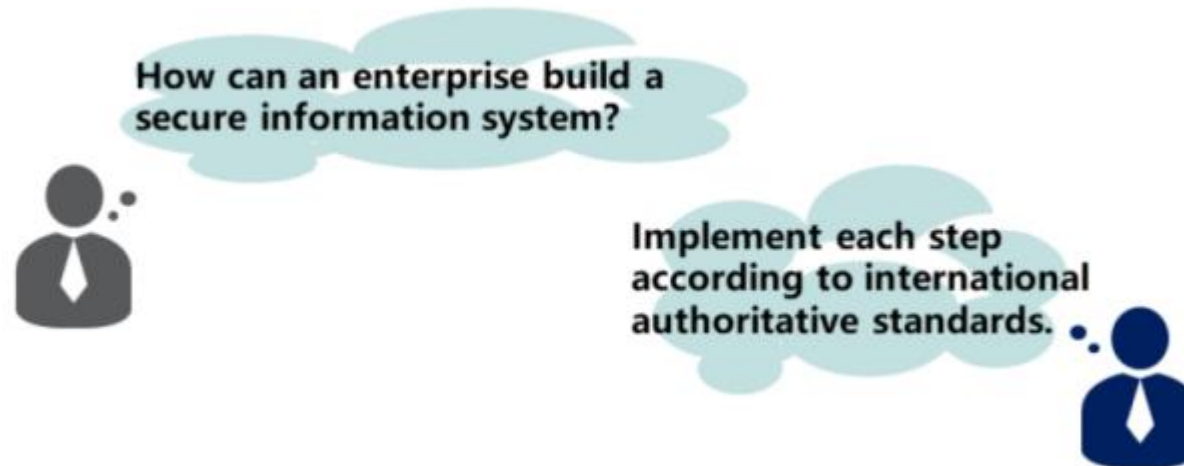
- In the process of information security system construction, enterprises comply with international standards and specifications to develop their own information security specifications and improve operations.
- This document describes and analyzes several international information security standards to help better understand information security.

- **Upon completion of this course, you will be able to describe:**
 - ❑ **Common information security standards.**
 - ❑ **Significance of information security standards.**
 - ❑ **Main points of common information security standards.**

- 1. Information Security Standards and Specifications**
- 2. ISO 27001 ISMS**
- 3. Graded Protection of Information Security**
- 4. Other Standards**

Significance of Information Security Standards

Standards are normative documents that are jointly formulated, approved by recognized authorities, and used throughout the industry to achieve the best security.



Information Security Standards Organizations

- **International organizations related to information security standardization:**
 - ❑ International Organization for Standardization (ISO)
 - ❑ International Electrotechnical Commission (IEC)
- **Chinese security standards organizations:**
 - ❑ China Information Security Standardization Technical Committee
 - ❑ Cyber and Information Security Technical Committee (TC8) of China Communications Standards Association (CCSA)
- **Other standards organizations:**
 - ❑ International Telecommunication Union (ITU)
 - ❑ Internet Engineering Task Force (IETF)

- International information security standardization began in the middle of the 1970s, rapidly developed in the 1980s and drew global attention in the 1990s. At present, there are nearly 300 international and regional organizations establishing standards or technical rules.
- ISO is a global non-governmental organization and plays a crucial role in international standardization. It has published international standards and related documents for most fields (including monopolized industries such as military, oil, and shipping).



- IEC was the first international organization established for the preparation and publication of international standards for all electrical, electronic and related technologies.
- ITU is the United Nations specialized agency for information and communication technologies. It allocates global radio spectrum and satellite orbits, develops global telecommunication standards, works to improve telecommunication infrastructure in the developing world, and promotes global telecommunication development.
- IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.



Common Information Security Standards and Specifications



- The Information Security Management System (ISMS), based on the BS7799 standard developed by the British Standards Institution (BSI), has been widely recognized as the international standard.

- Plan (Establish an ISMS)
- Do (Implement and operate ISMS)
- Check (Monitor and review ISMS)
- Action (Maintain and improve ISMS)



Plan : ISMS planning and preparation

- **Establish security policy, objectives, processes and procedures relevant to managing risks and improving information security to deliver results in accordance with an organizations over all policies and objectives.**

Do : ISMS document development Implement and operate the ISMS policy, controls, processes and procedures.

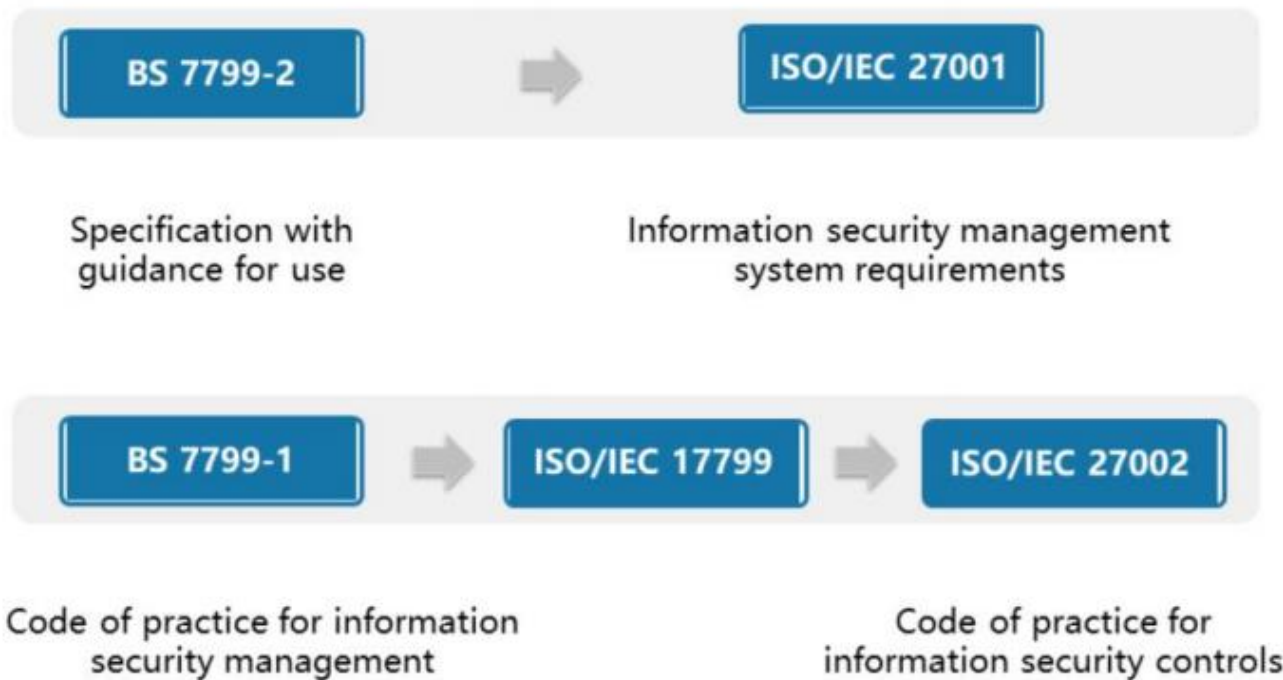
ISO 27000 ISMS Family of Standards

I	II	III	IV
Requirements and supporting guidelines	Audit and certification guidelines	Industry information security management requirements	Health information security management standards
ISO/IEC 27000	ISO/IEC 27006	Finance	ISO 27799
ISO/IEC 27001		Telecommunication	Projects that are in the research phase. For example, medicine supply chain and storage security.
ISO/IEC 27002	ISO/IEC 27007	Other specific security domains	
ISO/IEC 27003	ISO/IEC 27008		
ISO/IEC 27004			
ISO/IEC 27005			



ISO 27001 Evolution

- ISO/IEC 27001 and ISO/IEC 27002, released in 2013, are the currently used standards.



ISMS and ISO/IEC 27000

- ISO/IEC 27001 is an international standard that describes the requirements for an ISMS.



- ISO/IEC 27002 proposes 35 control objectives and 113 controls across 14 categories. These control objectives and controls are the best practices of information security management.



- Any company can implement an ISMS, but how? What requirements must be met? ISO 27000 provides detailed requirements which organizations can use to establish ISMSs.
- ISO 27001 is to manage information security risks based on risk assessments and to comprehensively, systematically, and continuously improve information security management using the Plan, Do, Check, Action (PDCA) cycle. It can be used to establish and implement ISMSs and ensure information security of organizations.
- ISO 27001, an overall information security management framework based on the PDCA cycle, focuses on the establishment of a continuous-cyclic long-term management mechanism. Only certification to ISO/IEC 27001 is possible. Other ISO/IEC standards are the specific clauses and operation guides for the certification. For example, ISO 27002 defines a specific information security management process under the guidance of ISO 27001.



Elements for Building an ISMS

- 14 control areas in ISO 27002:

1. Information Security Policies	2. Organization of Information Security	3. Human Resource Security
4. Asset Management	5. Access Control	6. Cryptography
7. Physical and Environmental Security	8. Operation Security	9. Communication Security
10. System Acquisition, Development and Maintenance	11. Supplier Relationships	12. Information Security Incident Management
13. Information Security Aspects of Business Continuity Management		14. Compliance

Elements for Building an ISMS

- The key check points in the ISO 27001 certification process are as follows:
 - Document review:
 - ☐ Risk assessment reports
 - ☐ Security principles
 - ☐ Statement of Applicability (SoA)
 - ☐ Other ISMS documents
 - Formal review:
 - ☐ Check records, including account and permission assignment, training, business continuity drill, access control, and media usage records.
 - ☐ Check the information asset identification and processing, and risk assessment and handling forms.
 - ☐ Perform terminal security check, including the screen saver, screen lock, and antivirus software installation and upgrade status.
 - ☐ Carry out the physical environment survey, including the field observation and inquiry of equipment rooms and office environments.



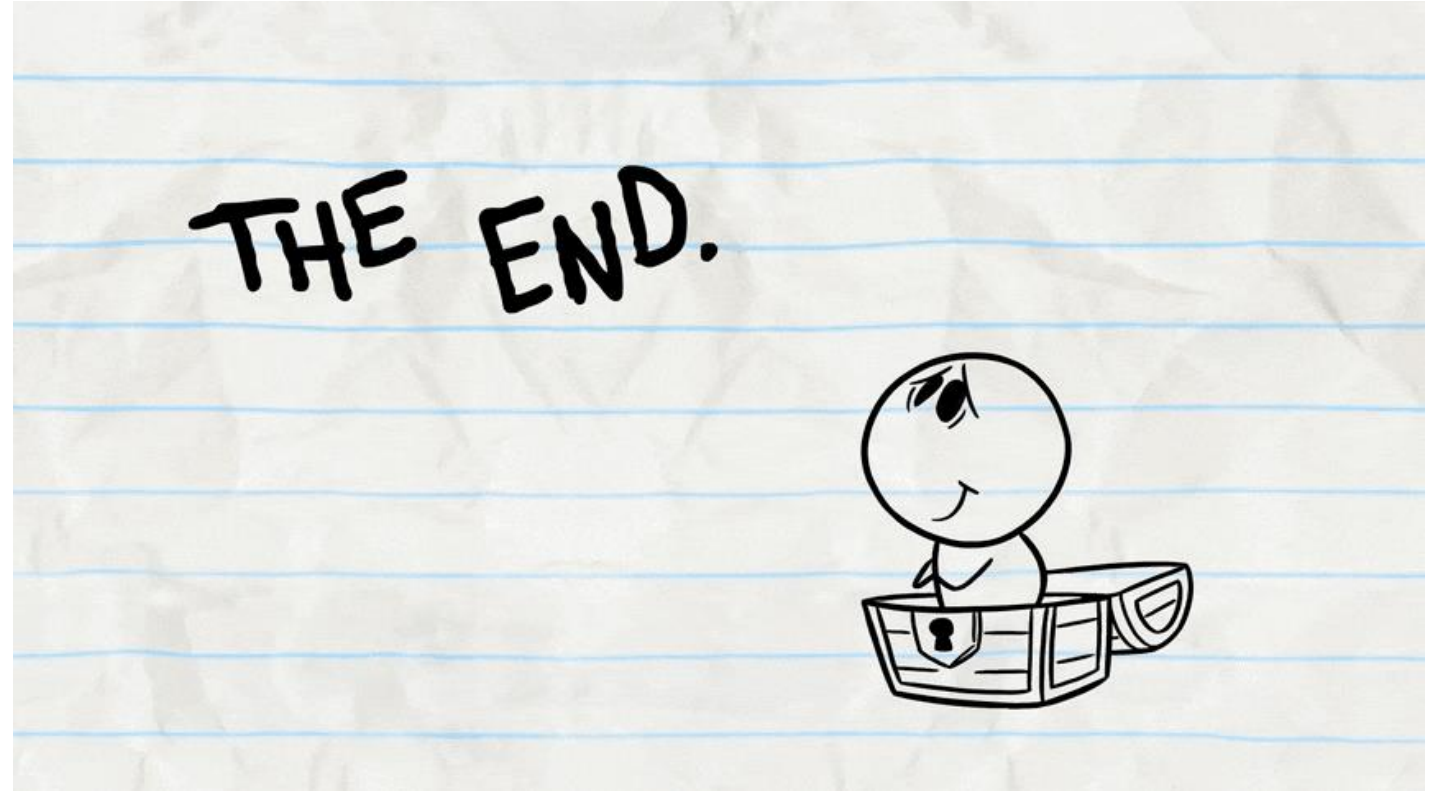
ISO 27001 Project Implementation Methodology and Steps



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY