ISO27001:2022
Lec1

AGENDA

- Why ISO27001 (Benefits) ?
- Three Principles of Information Security in ISO27001
- Introduction
- Planning
- Implementation
- Monitoring and Evaluation
- Exercises & Open Discussions

Why ISO27001 (Benefits) ?

1) How to Comply with ISO27001.

("Regulations" must be applied in its entirety across the EU)

(Compliance with ISO27K provides a framework to comply with the relevant regulations)

2) Respond to evolving security threats.

(New controls like threat intelligent leads to overcome and respond to new threats every day)

3) Getting Data Protection, Privacy & IT governance.

(Protect all forms of information, whether digital, hard copy or in the Cloud)

4) Meet Contractual Obligations (SLA).

(Certification demonstrates your organization's commitment to data security and provides a valuable credential when tendering for new business.)

Why ISO27001 (Benefits) ? – Continued

5) Competitive Advantage (Selling point).

(1- By obtaining certification in ISO 27001, organizations have the opportunity to prove credibility and show customers that the organization is working according to recognized best practices.

2- An extremely valuable intangible asset.)

6) Reduce information security costs.

(Implement only the security controls you need, helping you get the most out of your budget.)

7) Improve company culture.

(An ISMS encompasses people, processes, and technology, ensuring staff understand risks and embrace security as part of their everyday working practices.)

Thress principles of Information Security in ISO27001 known as CIA triad

1) Confidentiality

Only the right people can access the information held by the organization.

2) Information integrity

Data that the organization uses to pursue its business or keeps safe for others is reliably stored and not erased or damaged.

3) Availability of data

The organization and its clients can access the information whenever it is necessary so that business purposes and customer expectations are satisfied.

Introduction

- Course Objectives
- What is ISO27001 (Definitions & Details)
- Initiating the ISMS
- Structure of ISO27001
- Understanding The Organization
- Analysis the existing management system

Planning

- Leadership and Top Management Approval
- ISMS Scope
- Information Security Policies
- Risk Management
- Organizational Structure of Information Security
- Statement of Applicability (SOA)

Implementation

- Design of Security Controls
- Implementation of Security Controls
- Document management process
- Communication Plan
- Operations Management
- Incident Management

Monitoring and Evaluation

- Monitoring, Measurement, analysis and evaluation
- Internal Audit
- Management review
- Non Conformities
- Continual Improvement
- Preparing for the certificate audit
- Competence and evaluation of implementers

Discussion and exersices

- Completing any uncovered knowledge
- Open Discussion and answering Questions
- Take some examples

Course Objectives - the Goal is to be able to Implement ISMS

- Understand the components and the operation of an Information Security Management System based on ISO/IEC 27001 and its principal processes
- Understand the goal, content and correlation between ISO/IEC 27001, ISO/IEC 27002 and other standards & regulatory frameworks
- Master the concepts, approaches, methods and techniques used for the implementation and effective management of an ISMS
- Interpret the ISO/IEC27001 requirements in the specific context of an organization
- Develop the expertise to support an organization to plan, implement, manage, monitor and maintain an ISMS as specified in ISO/IEC 27001
- Acquire the expertise to advise an organization in implementing information security management best practices
- Explain the methodology for the ISMS management project and not the management control of daily operations.

Course Objectives - ISO27001 is as a project – Continued

- Implementing ISO 27001 is a Project (takes around 6 months)
- The Project plan of the organization is completed prior to the establishment of a project dedicated to the ISMS, as well as phases of monitoring and improvement are activated only when the location of system components has been finalized. In each phase, it is usual that security controls are also implemented sequentially (e.g., antivirus policy is developed and approved before the procedures and work instructions concerning the management of this control are actually written and implemented).
- We will integrate the ISMS into existing processes
- We will Involve all the stakeholders in the organization
- Grant support from your management

Course Objectives – Process Approach (PDCA)

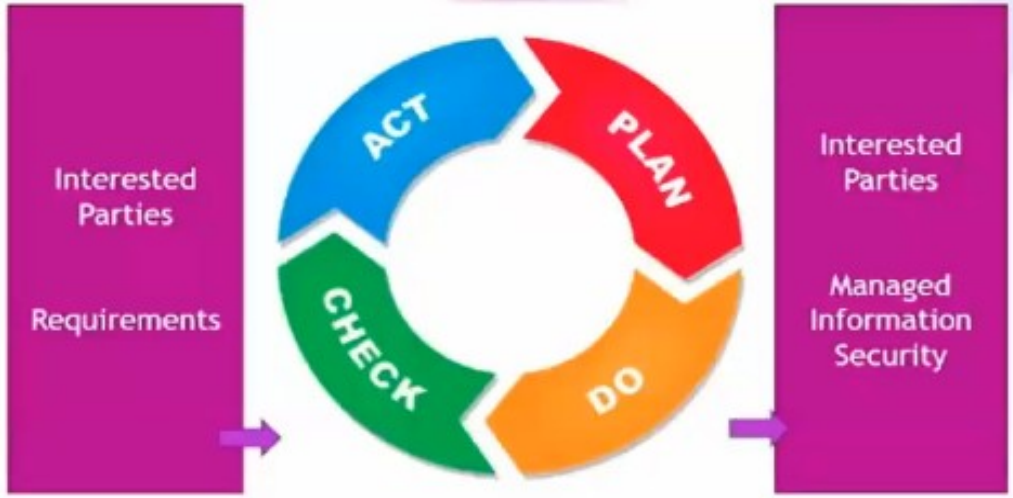
Process Approach

Plan (establish the management system): Establish the policy, the objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.

Do (implement and operate the management system): Implement and operate the policy, controls, processes and procedures of the management system.

Check (monitor and review the management system): Assess and, if applicable, measure process performances against the policy, objectives and practical experience and report the results to management for review.

Act (maintain and improve the management system): Undertake corrective and preventive actions, on the basis of the results of the internal audit and management review, or other relevant information to continually improve the system.



The figure illustrates how a management system uses as input the requirements and the expectations of the stakeholders, and how it produces, with the necessary actions and processes, the information security results that meet the requirements and expectations.

What is ISO27K - (ISO & Examples for ISO27K)

ISO and ISMS

- ISO is a network of national standardization bodies from over 150 countries.
- The final results of ISO works are published as international standards.
- Over 22,200 standards have been published since 1947
- Adoption of ISO standards is voluntary.
- Examples: ISO 9001, ISO 14001, ISO 20000, ISO 22301, ISO 27001

ISO/IEC 27000: For basic concepts and vocabulary (FREE)

ISO/IEC 27001: This information security standard defines the requirements of the Information Security Management Systems (ISMS).

ISO/IEC 27002 (previously ISO/IEC 17799): Guide of best practices for the management of information security.

ISO/IEC 27003: Guide for implementing or setting up an ISMS.

ISO/IEC 27004: Guide of metrics to facilitate ISMS management

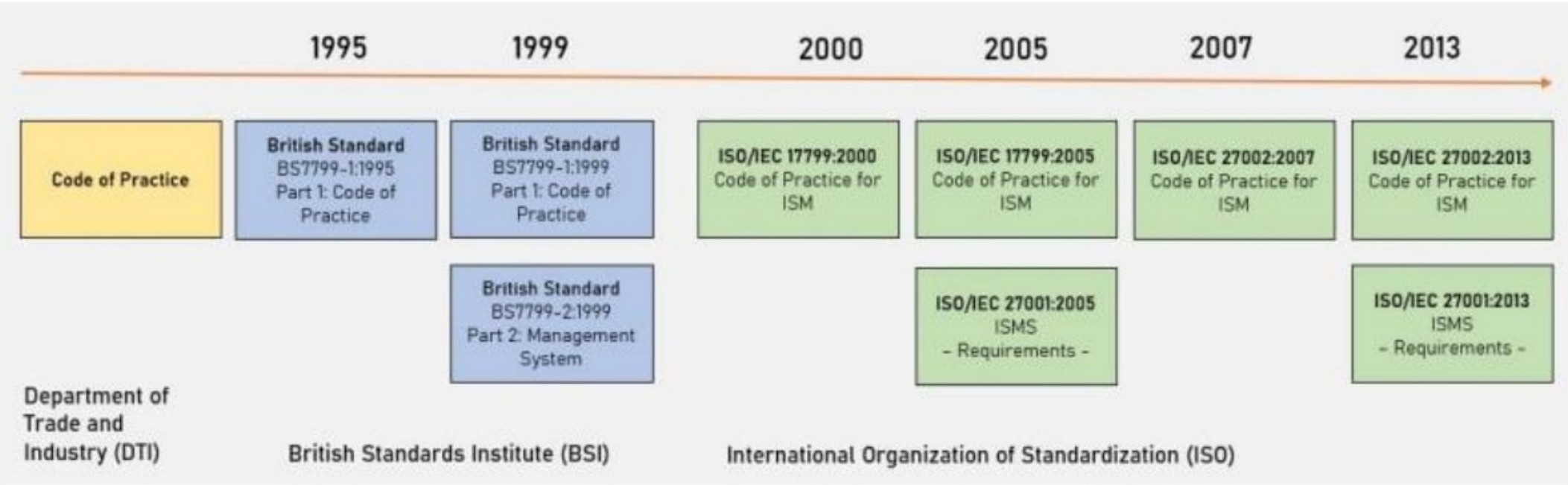
ISO/IEC 27005: Guide for information security risk management

What is ISO27K - ISO27001 in details - Continued

ISO/IEC 27001

- A set of normative requirements for the establishment, implementation, operation, monitoring and review of an Information Security Management System (ISMS)
- A set of requirements for selecting information security controls tailored to the needs of each organization based on industry best practices
- A management system that is integrated in the overall risk framework associated with the activity of the organization
- Suit all types of organizations (commercial enterprises, government agencies, nonprofit organizations ...), of all sizes in all industries.
- Specifies the requirements for an ISMS (Clause 4 to 10)
- Annex A: 14 clauses containing 35 control objectives and ~~114~~ 93 controls

History of 27001

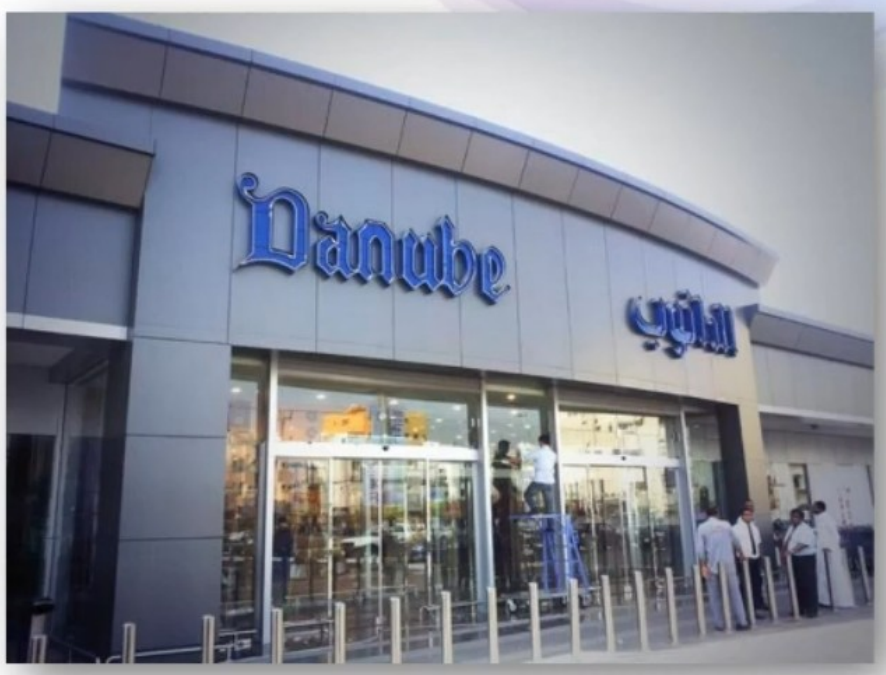


Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

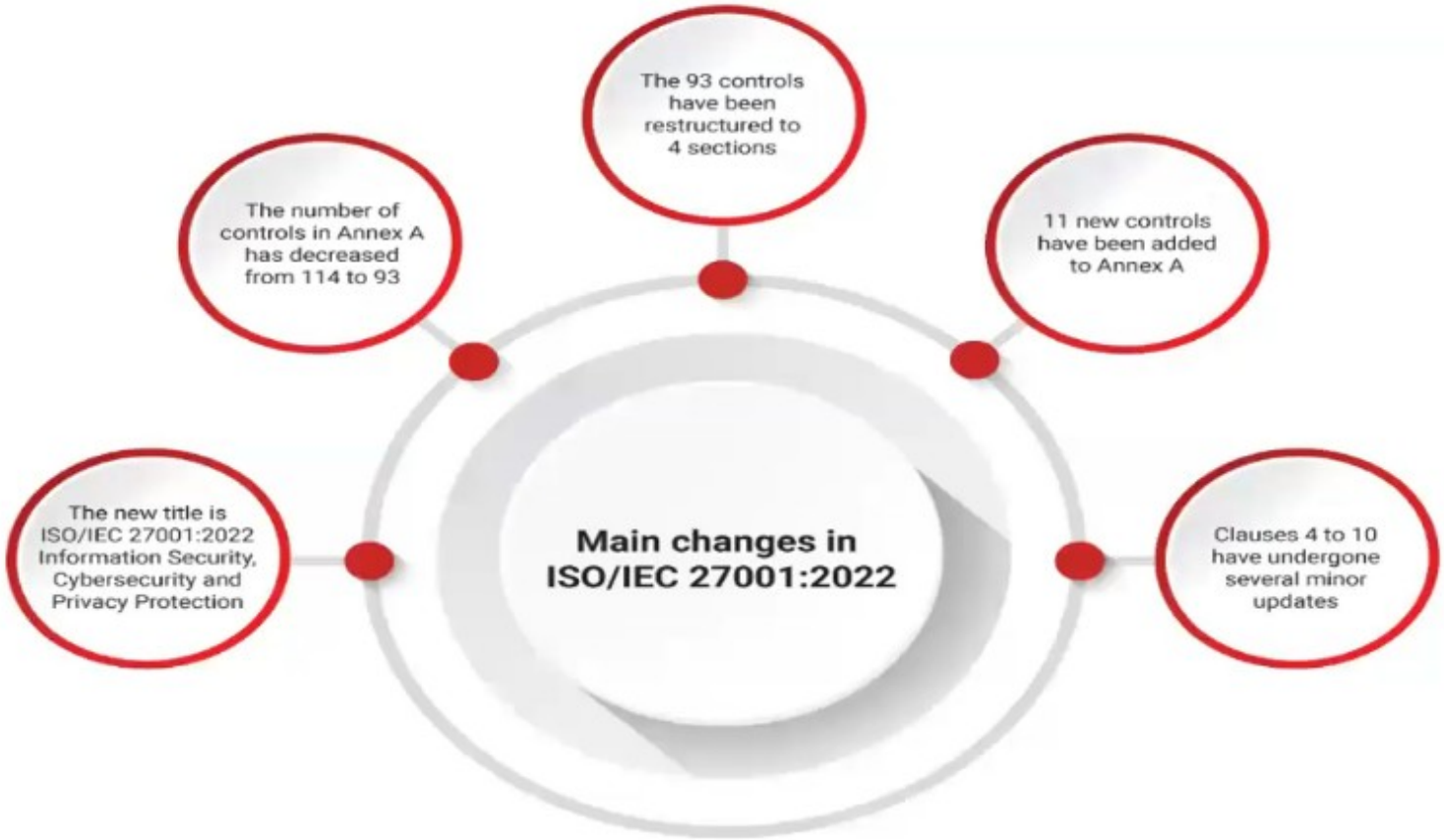
4.3 Determining the scope of the information security management system

Q: Can we implement ISO 27001 without any information systems, networks or any infrastructure ?

Yes, because our concern is the information not the systems



What is ISO27K - The new Changes ISO27001:2022 – Continued



What is ISO27K - Reduction from 114 into 93 controls – Continued

The 93 controls have been restructured to four control groups or sections:-

- A.5 Organizational controls - contains 37 controls.
- A.6 People controls - contains 8 controls.
- A.7 Physical controls - contains 14 controls.
- A.8 Technological controls - contains 34 controls.

What is ISO27K - The new 11 controls – Continued

ISO/IEC 27001:2022 has also added the below-mentioned 11 new controls to its Annex A:-

1) Threat intelligence
2) Information security for the use of cloud services
3) ICT readiness for business continuity
4) Physical security monitoring
5) Configuration management
6) Information deletion
7) Data masking
8) Data leakage prevention (DLP)
9) Monitoring activities
10) Web filtering
11) Secure coding

Initiating the ISMS - Management System

Definition of Management System and Process

- A management system is a system that allows organizations to establish policies and objectives and to subsequently implement them. The management system of an organization may include different management systems, such as a quality management system, information security, environmental, etc.

- Organizations use management systems to develop their policies and put them into effect through objectives using:
  - An organizational structure;
  - Systematic processes and associated resources;
  - An effective assessment methodology;
  - A review process to ensure that the problems are adequately corrected and that opportunities for improvement are recognized and implemented when justified.

- Processes can be defined as being a logical group of interrelated tasks, performed to reach a defined objective.
- A process is a sequence of structured and measured activities designed to create a product or a service for a specific market or a particular client.

Initiating the ISMS - Information Security & ISMS Definitions

Definition of Information Security and Information Security Management System (ISMS) - ISO/IEC 27000

- Information security: Preservation of confidentiality, integrity and availability of information (ISO/IEC 27000, 3.28).
- An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.
- An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

THANKS!