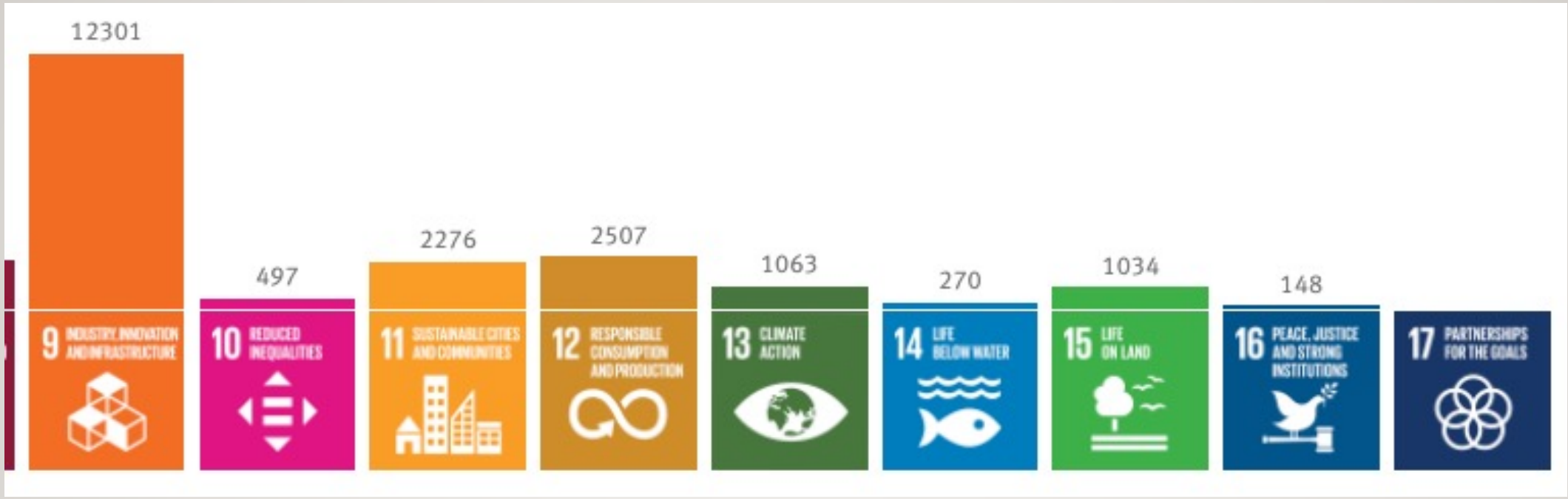

Technology Security
INNOVATION
Data-A
ISO/IEC 27001
Certification

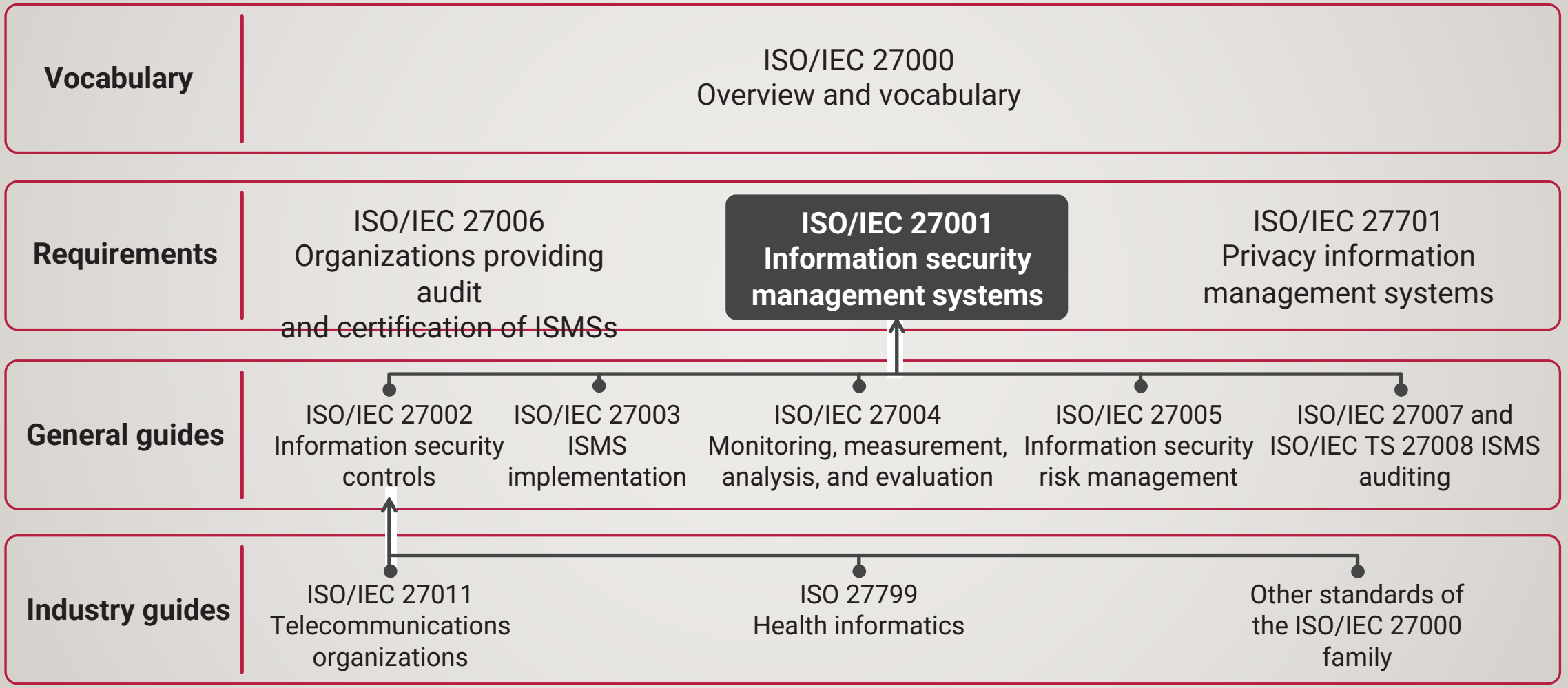
WHAT IS ISO?

- ISO is an international organization of national standards bodies from over 160 countries.
- The final results of ISO works are published as international standards.
- ISO has published over 22,000 standards since 1947.
- Some standards like 27001 are a result of a collaborative work with IEC – International Electrotechnical Commission – publishes international standards for electrical, electronic and related technology
- ISO takes broader approach and develops standards for which a market demand exists


12301
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
497
10 REDUCED INEQUALITIES
2276
11 SUSTAINABLE CITIES AND COMMUNITIES
2507
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
1063
13 CLIMATE ACTION
270
14 LIFE BELOW WATER
1034
15 LIFE ON LAND
148
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

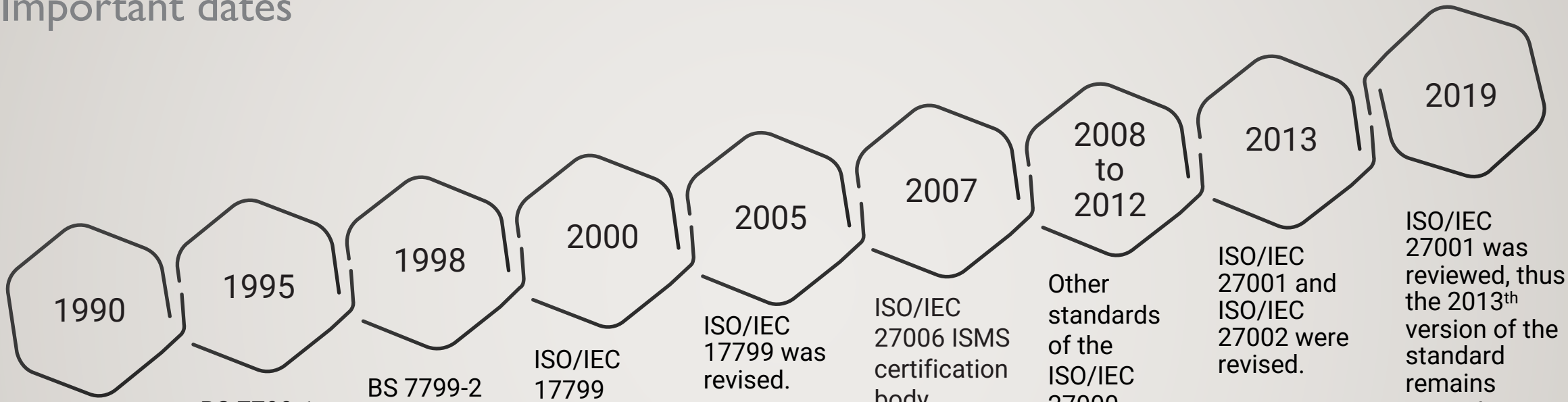

340
1 NO POVERTY
529
2 ZERO HUNGER
2733
3 GOOD HEALTH AND WELL-BEING
462
4 QUALITY EDUCATION
173
5 GENDER EQUALITY
533
6 CLEAN WATER AND SANITATION
804
7 AFFORDABLE AND CLEAN ENERGY
2371
8 DECENT WORK AND ECONOMIC GROWTH

THE ISO/IEC 27000 FAMILY OF STANDARDS



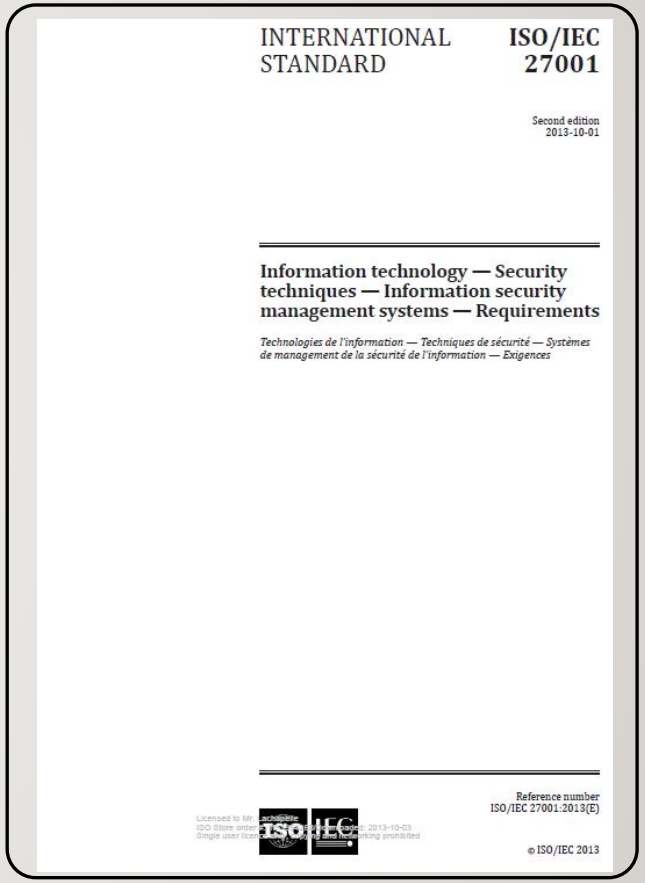
DEVELOPMENT OF THE ISO/IEC 27000 FAMILY OF STANDARDS

Important dates



ISO/IEC 27001

- The standard specifies requirements for an ISMS (clauses 4 to 10).
- Requirements (clauses) are expressed with the verb “shall.”
- Annex A contains 14 clauses, 35 control objectives, and 114 controls.
- Organizations can obtain certification against this standard.


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)

CONTEXT OF THE ORGANIZATION

ISO/IEC 27001, clause 4

4.1 Understanding the organization and its context

The organization shall establish the external and internal factors related to the ISMS that can affect the achievement of the ISMS intended outcome(s).

4.2 Understanding the needs and expectations of interested parties

The organization shall determine the interested parties and the information security requirements relevant to these interested parties.

4.3 Determining the scope of the information security management system

The organization shall establish the ISMS scope by setting its boundaries and applicability. The scope shall be available as documented information.

4.4 Information security management system

The organization shall comply with the standard's requirements to establish, implement, maintain and continually improve an information security management system.

LEADERSHIP

ISO/IEC 27001, clause 5

5.1 Leadership and commitment

- Top management shall ensure that the ISMS is compatible with the organization's strategic orientation.
- Top management shall integrate the ISMS requirements into the organization's business processes, determine the necessary resources for the ISMS, and communicate the importance of an effective information security management.

5.2 Policy

- Top management shall create an information security policy that shall be appropriately available and communicated to all interested parties.
- The policy shall be aligned with the purpose of the organization and shall include the information security objectives, a commitment to fulfill the information security requirements and a commitment for continual improvement.

5.3 Organizational roles, responsibilities and authorities

- Top management shall assign the appropriate information security roles and responsibilities in order to ensure that the information security management system conforms to the requirments of ISO/IEC 27001.

PLANNING

ISO/IEC 27001, clause 6

Actions to addresss risks and opportunities

The organization shall determine the risks and opportunities to achieve the intended outcome(s); prevent or reduce undesired effects; and achieve continual improvement. The organization shall also plan actions to address risks and opportunities, implement those actions, and evaluate their effectiveness.

Information security risk assessment

The organization shall establish and maintain risk criteria; identify, analyze, and evaluate risks; and ensure that the risk assessment process generates consistent, valid, and comparable results.

Information security risk treatment

The organization shall select the risk treatment options, determine the controls needed to implement the risk treatment options, compare the selected controls, produce the Statement of Applicability, formulate the risk treatment plan, and obtain approval for the risk treatment plan as well as for the acceptance of residual risks.

Information security objectives and planning to achieve them

The organization’s objectives shall be measurable and consistent with the information security policy. They shall also be aligned with the requirements, and risk assessment and risk treatment results. The objectives shall be appropriately communicated, and updated.

SUPPORT

ISO/IEC 27001, clause 7

7.1 Resources

The organization shall determine and provide the necessary resources for the appropriate implementation of the ISMS.

7.2 Competence

The organization shall ensure that it has the competent personnel to perform the tasks related to the ISMS.

7.3 Awareness

The organization shall ensure that its employees are aware of the information security policy, their roles in the ISMS, and the implications of failing to conform to the ISMS requirements.

7.4 Communication

The organization shall establish, implement, and maintain arrangements for communication with relevant external and internal interested parties.

7.5 Documented information

The organization's ISMS shall include documented information required by ISO/IEC 27001 and records to demonstrate the effectiveness of the ISMS.

OPERATION

ISO/IEC 27001, clause 8

8.1 Operational planning and control →

The organization shall plan, implement, and control the necessary processes to comply with the standard requirments (execution of the plans and processes that are subject of previous clauses). The organization shall also implement the plans, keep documented information as evidence of the implementation of planned processes, control and review the planned changes, and determine and control the oursourced processes.

8.2 Information security risk assessment →

The organization shall conduct information security risk assessments at planned intervals and shall keep documented information of the risk assessment results.

8.3 Information security risk treatment →

The organization shall implement the information security risk treatment plan and shall keep documented information on risk treatment results.

PERFORMANCE EVALUATION

ISO/IEC 27001, clause 9

9.1 *Monitoring, measurement, analysis and evaluation*

The organization shall evaluate the performance and effectiveness of the information security management system and keep documented information as evidence of the monitoring and measurement outputs.

9.2 *Internal audit*

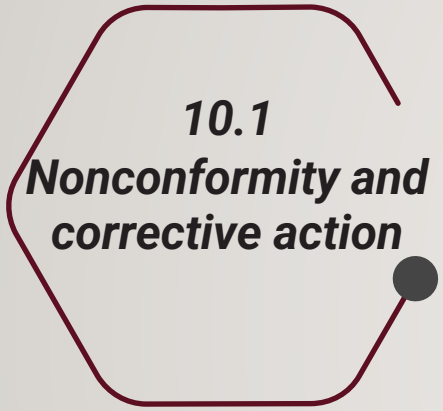
The organization shall perform internal audits at planned intervals in order to validate whether the information security management system is effectively implemented, maintained, and remains conform to the organization's own requirements as well as the standard requirements.

9.3 *Management review*

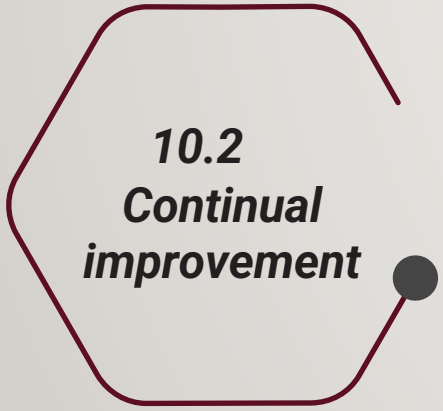
The top management shall perform reviews of the ISMS at planned intervals in order to ensure its suitability, adequacy and effectiveness. The organization shall keep documented information as evidence of the management review outputs.

IMPROVEMENT

ISO/IEC 27001, clause 10



The organization shall take the appropriate actions when a nonconformity occurs. It shall evaluate and implement those actions, review their effectiveness and, if necessary, make changes. The organization shall also keep documented information as evidence of the results of corrective actions.



The organization shall ensure the continual improvement of the suitability, adequacy, and effectiveness of the information security management system.

ANNEX A

- Annex A is part of ISO/IEC 27001 and it is comprised of 114 controls that should be considered when intending to comply with the standard.
- The list of control objectives and controls of Annex A is not exhaustive. The organization may add additional controls from other sources, when needed.
- If a certain control is not implemented, the organization should provide an acceptable justification for its exclusion.

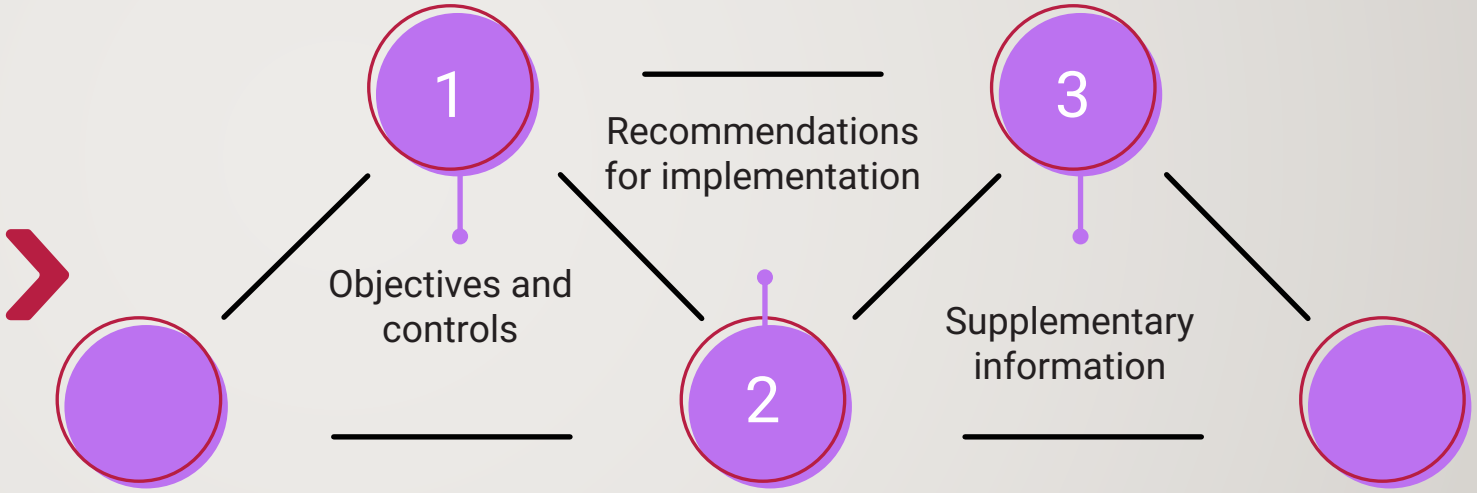
ANNEX A

Security objectives and controls

ISO/IEC 27001

Annex A
(List of security objectives and controls)

ISO/IEC 27002



Important note: Since ISO/IEC 27002 is a code of practice, there is no requirement to follow its guidance in order to obtain an ISO/IEC 27001 certification.

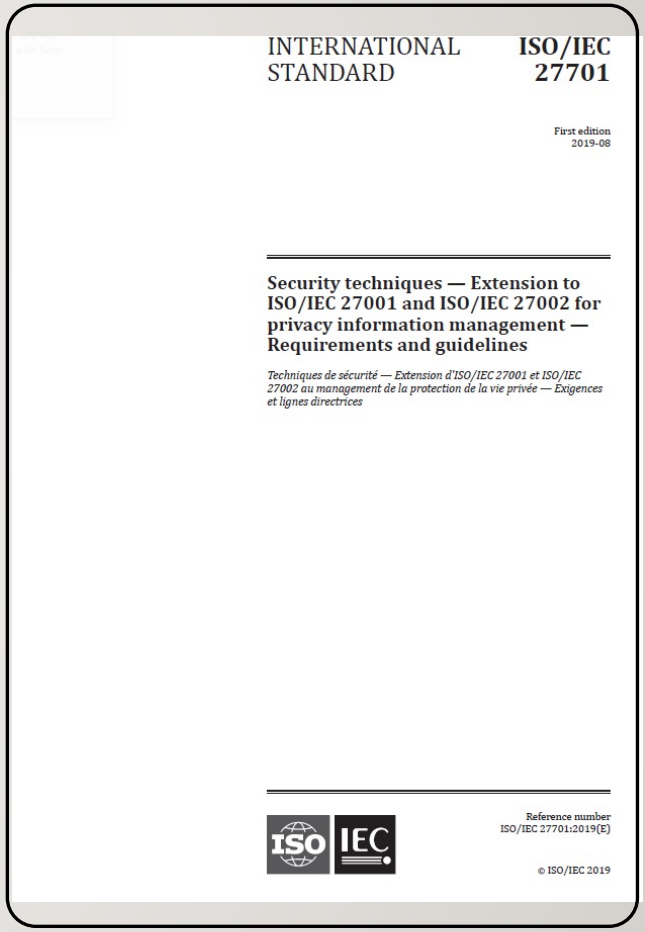
114 SECURITY CONTROLS

ISO/IEC 27001, Annex A

A.5	*Information security policies*	2 controls
A.6	*Organization of information security*	7 controls
A.7	*Human resource security*	6 controls
A.8	*Asset management*	10 controls
A.9	*Access control*	14 controls
A.10	*Cryptography*	2 controls
A.11	*Physical and environmental security*	15 controls
A.12	*Operations security*	14 controls
A.13	*Communications security*	7 controls
A.14	*System acquisition, development and maintenance*	13 controls
A.15	*Supplier relationships*	5 controls
A.16	*Information security incident management*	7 controls
A.17	*Information security aspects of business continuity management*	4 controls
A.18	*Compliance*	8 controls

ISO/IEC 27701

- The standard is an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.
- This standard specifies requirements and provides guidance for a PIMS.
- The standard's requirements (clauses) are written using the imperative verb "shall."
- Organizations can obtain certification against this standard.


INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

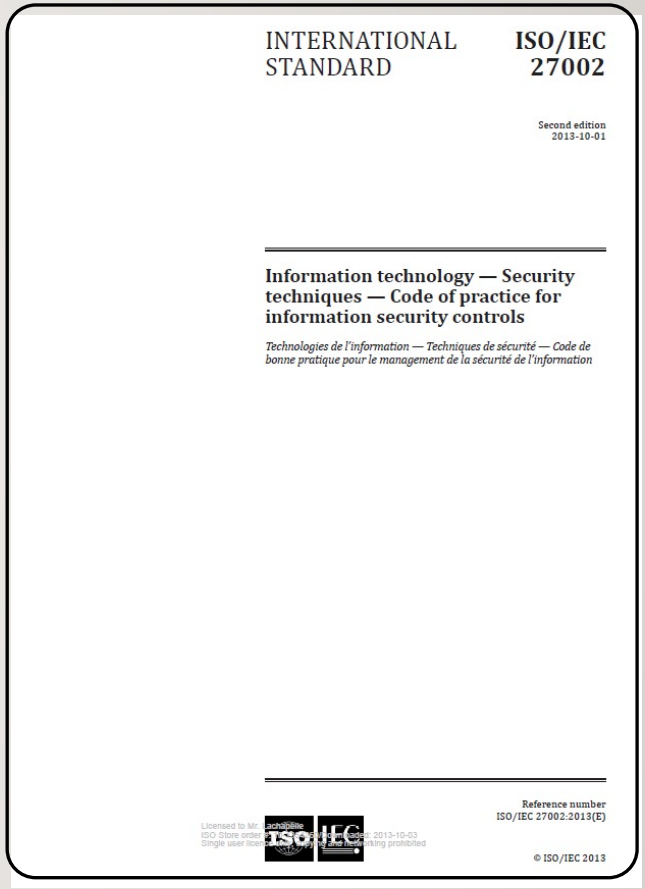
Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

ISO IEC

Reference number
ISO/IEC 27701:2019(E)

ISO/IEC 27002

- The standard provides guidance for codes of practice for information security controls (reference document).
- Clauses are expressed with the verb “should.”
- Organizations cannot obtain certification against this standard.


INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

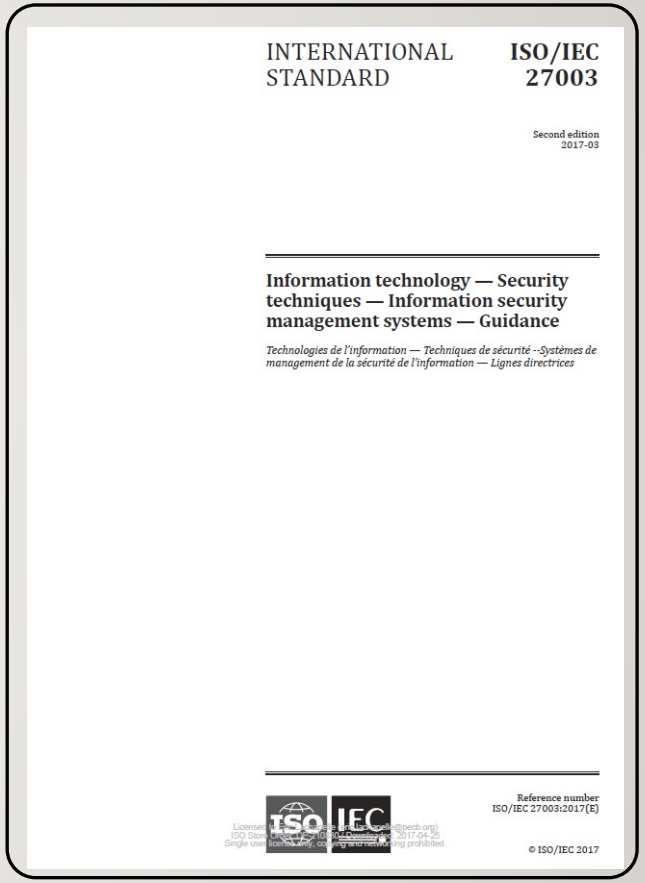
Information technology — Security techniques — Code of practice for information security controls

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 27003

- The standard provides guidance on the requirements for an information security management system.
- It serves as a reference document to be used with ISO/IEC 27001 and ISO/IEC 27002 standards.
- It is composed of 10 clauses.
- Organizations cannot obtain certification against this standard.


INTERNATIONAL STANDARD

ISO/IEC 27003

Second edition
2017-03

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

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Lignes directrices

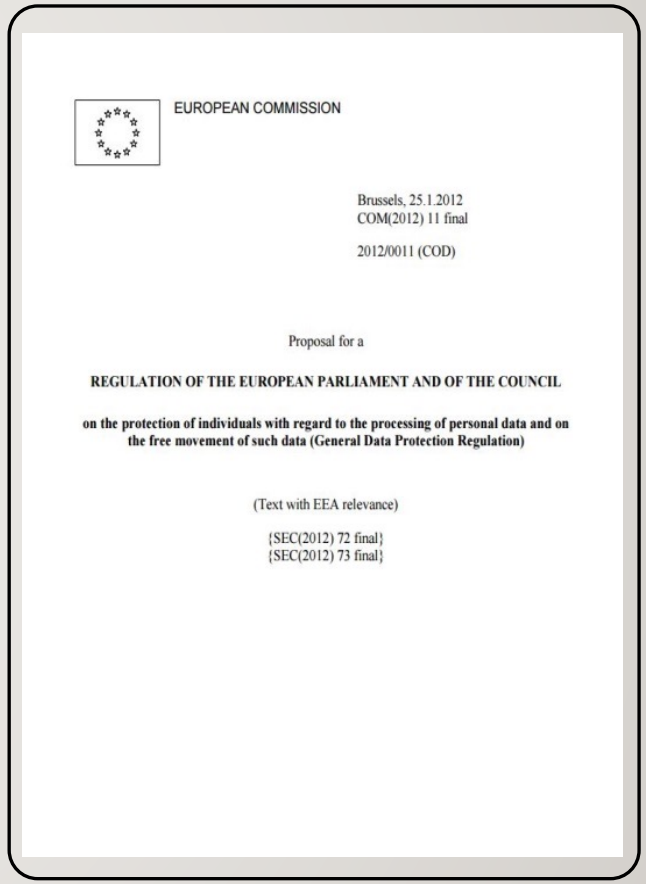
Reference number
ISO/IEC 27003:2017(E)

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards which unify the information security programs and policies with regard to credit card information.
- PCI DISS applies to any organization that accepts, transmits, or stores any cardholder data.
- PCI Security Standards Council was founded in 2006 by American Express, Discover, JCB International, MasterCard, and Visa Inc.

THE GENERAL DATA PROTECTION REGULATION

- The General Data Protection Regulation (GDPR) specifies the requirements for the protection of natural persons with regard to the processing and free movement of personal data.
- ISO/IEC 27001 framework can be used to support compliance with the GDPR (Article 32 sets out technical and organisational measures that organisations should implement to protect the personal data they store
- The GDPR is available at: http://eur-lex.europa.eu/eli/reg/2016/679/oj



EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

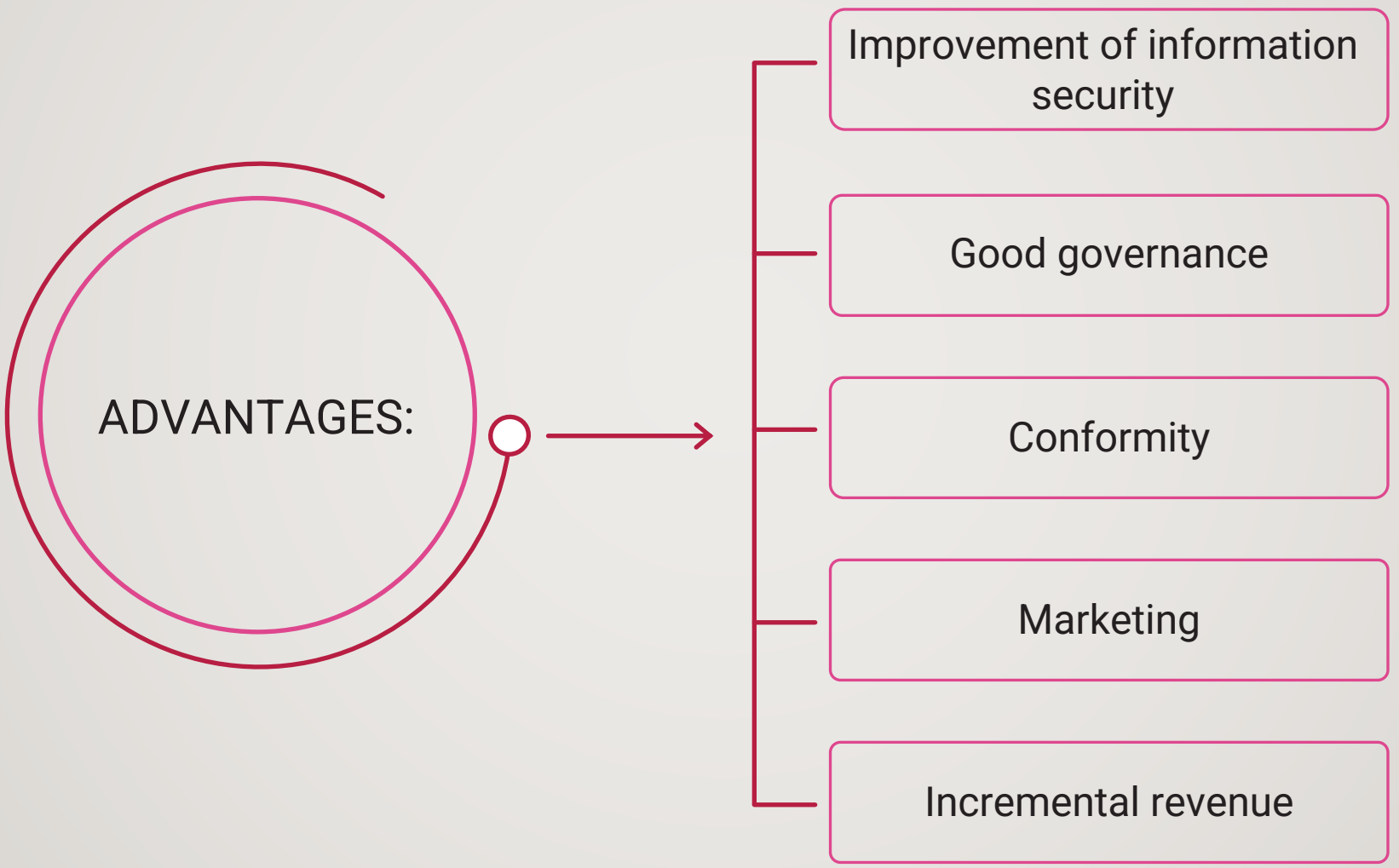
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

ADVANTAGES OF ISO/IEC 27001



Information Security Management System (ISMS)

- Definition of a management system
- Management system standards
- Integrated management systems
- Definition of an ISMS
- Process approach
- Overview — Clauses 4 to 10
- Overview — Annex A

DEFINITION OF A MANAGEMENT SYSTEM

ISO/IEC 27000, clause 3.41

- *Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives*
- 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 management systems in different fields, including quality, information security, environment, etc.
- *Note 1 to entry: A management system can address a single discipline or several disciplines.*
- *Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.*
- *Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.*

MANAGEMENT SYSTEM STANDARDS

Organizations can get certified to the following primary standards:

DEFINITION OF AN ISMS

ISO/IEC 27000, clause 4.2.1

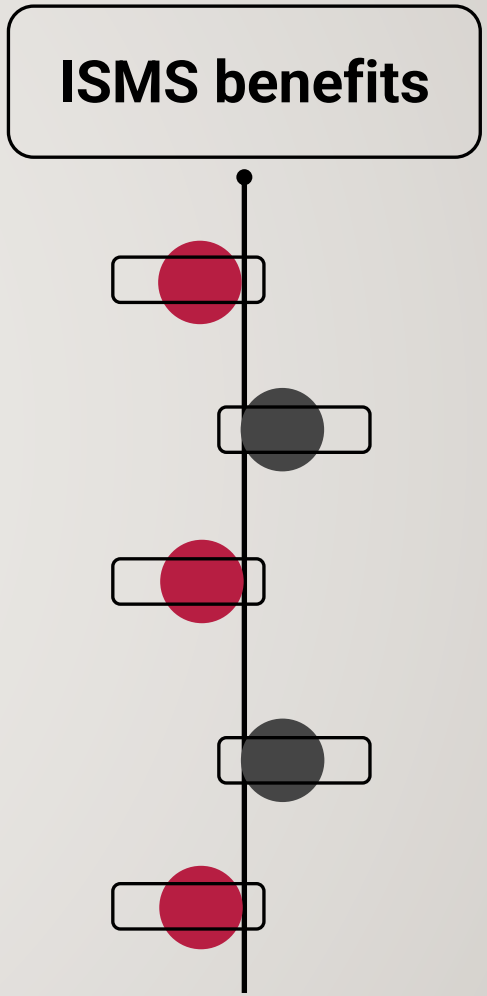
- *An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.*

- *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.*

BENEFITS OF THE ISMS

Having an effective ISMS in place helps an organization in:

- Reducing information security risks and minimizing exposure to information security breaches
- Protecting assets and sensitive information
- Creating competitive advantage
- Improving reputation and increasing customer confidence
- Protecting the confidentiality, availability, and integrity of information



CHOOSE A METHODOLOGICAL FRAMEWORK TO MANAGE THE IMPLEMENTATION OF AN ISMS

1. Define and establish	2. Implement and operate	3. Monitor and review	4. Maintain and improve
1.1 Initiation of the ISMS implementation	2.1 Documentation management	3.1 Monitoring, measurement, analysis, and evaluation	4.1 Treatment of nonconformities
1.2 Understanding the organization	2.2 Selection and design of controls	3.2 Internal audit	4.2 Continual improvement
1.3 ISMS scope	2.3 Implementation of controls	3.3 Management review	
1.4 Leadership and project approval	2.4 Communication		
1.5 Organizational structure	2.5 Competence and awareness		
1.6 Analysis of the existing system	2.6 Security operations management		
1.7 Security policy			
1.8 Risk management			
1.9 Statement of Applicability			

Continual communication and awareness

CERTIFIED ISO/IEC 27001 IMPLEMENTER

PECB Implementer Certifications Requirements

Credential	Professional experience	ISMS project experience	Other requirements
PECB Certified ISO/IEC 27001 Provisional Implementer	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Implementer	Two years: One year of work experience in Information Security Management	Project activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Lead Implementer	Five years: Two years of work experience in Information Security Management	Project activities: a total of 300 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27001 Senior Lead Implementer	Ten years: Seven years of work experience in Information Security Management	Project activities: a total of 1,000 hours	Signing the PECB Code of Ethics

CERTIFICATION EXAMPLE

PECB

Professional Evaluation and Certification Board

hereby attests that

Lena Yuryna Connolly

is awarded the title

PECB Certified ISO/IEC 27001 Lead Implementer

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: ISLI1064392-2020-06
Issue Date: 2020-06-25
This certificate is valid for three years for the purpose of PECB certification

Carolina Cabezas, Compliance Director

WHY BECOME A CERTIFIED IMPLEMENTER?

Advantages

- Qualifying yourself to manage an ISMS project
- Achieving a formal and independent recognition of your personal competences
- Potentially earning a higher salary than noncertified individuals