INFORMATION SECURITY 27001 LEAD IMPLEMENTER

ESTAESTABLISH, IMPLEMENT, MAINTAIN AND IMPROVE AN INFORMATION SECURITY MANAGEMENT SYSTEM

PRACTICAL COURSE WITH STEP-BY-STEP IMPLEMENTATION METHODOLOGY OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

The course challenges the students on the implementation of an Information Security Management System (ISMS) based on the requirements and best practices defined by the ISO/IEC 27000 family of standards and supported by a customized methodology, proposed by BEHAVIOUR, that was created by experts on information security and ISO and other related well known best practices on the information security and IT fields.

- Information Security and/or IT Consultants, Auditors, Managers or Risk Professionals participating in an ISMS implementation based on ISO/IEC 27001
- CISO, CIO, CSO, or any Executive or Senior Manager responsible for ensuring the alignment and delivery of value using an ISMS based on ISO/IEC 27001 to maintain Information Security in their organization
- Experts responsible for the Information Security/IT Governance in the organization
- Project managers leading or preparing to lead an ISO/IEC 27001 implementation program
- Any professional, either, IT, information security, business, or any other, involved in the establishment, implementation, operations, and/or continual improvement of an Information Security Management System (ISMS) based on ISO/IEC 27001
- Anyone who wants to acquire the knowledge needed to implement an ISO/IEC 27001 ISMS

TRAINING METHODOLOGY

This course is based on theorical, and practical sessions supported by a real-world adapted case-study.

The course includes hands-on practical and theorical exercises to:

- better prepare the students for the real-world challenges, and
- to prepare and increase the likelihood of success on the certification exam, and
- train and prepare professionals for participating in an ISMS implementation program or ISMS audit based on ISO/IEC 27001.

WHAT WILL YOU LEARN?

- Understand the fundamental information security concepts and the main requirements and controls of ISO/IEC 27001
- Get to know and understand the correlation of the ISO/IEC 27000 family standards, including ISO/IEC 27001, ISO/IEC 27002, and related ISO and other best practices, legislation and regulation
- Establish, implement, maintain, and continually improve an Information Security Management System (ISMS), in accordance with the requirements of the ISO/IEC 27001 International Standard
- Understand and know how to implement and operate an ISMS in the context of an organization, including the required processes, techniques, and tools
- Assess and treat risks and opportunities to successfully achieve the information security objectives in response to the organization objectives
- Identify, draft, and implement the required information security controls based on ISO/IEC 27002 best practices, including the approach for managing information security incidents and ensuring information security during business continuity
- Identify and draft the ISMS required documented information, including templates for policies, processes, and procedures, among others required
- Understand and implement the performance evaluation requirements, including the approaches for monitoring and measure the ISMS, the internal audit program, and the management review
- Identify and respond to the ISMS continual improvement requirements based on the continual changes in the context of an organization
- Advise an organization on the latest information security best practices in support to the information security and business objectives
- Lead the organization to the achievement of the ISO/IEC 27001 certification
- Acquire the required knowledge to succeed in the “BEHAVIOUR Certified Information Security 27001 Lead Implementer” exam and achieve a personnel certification

PROGRAM

1. **Introduction to Information Security, the ISO/IEC 27001 standard, and related best practices**
   - Course introduction
   - Information security standards and compliance requirements
   - Information security fundamentals
   - Presentation and overview of the ISMS requirements
   - Preparing for ISMS implementation – approach and methodology
   - Understanding of the organization drivers and establishing the information security context
   - Drafting the ISMS scope
   - Assessing the current and target state for the ISMS Gap Analysis

2. **Establish (Plan) an ISMS based on ISO/IEC 27001**
   - Leadership and commitment to the ISMS Information Security Program establishment
   - Drafting the Information Security Policy
   - Establish the ISMS organizational structures (roles, responsibilities, and authorities)
   - Assessment of ISMS risks and opportunities
   - Information Security Risk Assessment
   - Drafting the Statement of Applicability (SoA)
   - Risk treatment process
   - Establishing and planning the Information security objectives

3. **Implement and Operate (Do) an ISMS based on ISO/IEC 27001**
   - Determine and provide the ISMS required resources
   - Competence, training, and awareness
   - Information security internal and external communication
   - Drafting the documented information management process
   - Required ISMS documented information and templates for the ISMS implementation and operation (Policies, Processes, Procedures, among others)
   - Best practices for drafting and implementing information security controls based on ISO/IEC 27002
   - Transitioning the ISMS to operations

4. **Monitor and Review (Check) and, Maintain and Improve (Act) an ISMS based on ISO/IEC 27001; Advance for the ISO/IEC 27001 Certification Audit**
   - Monitoring, measurement, analysis, and evaluation
   - Internal audit program
   - Management review
   - Managing findings, including nonconformities, and apply corrective actions
   - Continual improvement process
   - Advance for the ISO/IEC 27001 certification audit
   - Personnel certification and closing the training

5. C**ertified Information Security 27001 Lead Implementer Exam**

EXAM

O *Certified Information Security 27001 Lead Implementer* abrange os seguintes domínios de competência:

Domain 1
Information security fundamentals and ISO/IEC 27001 requirements

Domain 2
Establish (Plan) an ISMS based on ISO/IEC 27001

Domain 3
Implement and Operate (Do) an ISMS based on ISO/IEC 27001

Domain 4
Monitor and Review (Check) an ISMS based on ISO/IEC 27001

Domain 5
Maintain and Improve (Act) an ISMS based on ISO/IEC 27001

Domain 6
Advance for the ISO/IEC 27001 Certification Audit

CERTIFICATION

After successfully completing the certification exam, and signing the agreement/code of ethics, you may apply for one of the credentials, depending on your professional experience.

Certified Information Security 27001 Associate Implementer
no previous experience required

Certified Information Security 27001 Implementer
2 years of experience in information security

Certified Information Security 27001 Lead Implementer
5 years of experience in information

The certification diploma will be issued to candidates who successfully complete the exam and who meet all requirements related to the chosen certification.

REGISTER AND PARTICIPATE

See online the next public dates

https://behaviour-group.com/PT/information-security-27001-lead-implementer-course/?lang=en