

A new journey to cybersecurity!

BEHAVIOUR
MASTERING
CYBERSECURITY

CyberSecurity Lead Implementer Official Course

CyberSecurity Lead Implementer Training

Bringing value to you!

ACQUIRE SUFFICIENT KNOWLEDGE AND UNDERSTANDING HOW TO IMPLEMENT A CYBERSECURITY PROGRAMME

About this course

This course enables the trainees to acquire the necessary expertise to support an organization on implementing a Cybersecurity framework/programme. The trainees will acquire sufficient knowledge to plan all required aspects for a cybersecurity framework/programme to be successfully implemented, such as which policies, processes, and procedures should be developed, how to operationalize the framework/programme after the planification, as well as, how to control, monitor and improve the cybersecurity framework/programme. Additionally, the methodology of implementation is aligned with the current most recognized frameworks for cybersecurity and it is in compliance with all include all legislative and regulative obligations.

This 5-day course prepares the participants for the Behaviour Cybersecurity Lead Implementer (CLI) certification. This certification is aligned with ISO/IEC 17024 and therefore valid at international level.

Who should participate?

- Information security professionals, consultants and/or auditors that need to acquire the fundamental knowledge about the frameworks, controls, and applicable legislation regarding cybersecurity;
- Expert advisors on cybersecurity;
- Managers in charge of implementing a cybersecurity framework/programme;
- Technical and non-technical collaborators that support the implementation, operationalization and improvement of a cybersecurity framework/programme;
- CxO and Senior Managers responsible for the IT governance of an enterprise and the management of its risks.

Master the implementation of a cybersecurity framework/programme

- Understand the fundamental concepts and how to manage a cybersecurity framework/programme
- Plan a cybersecurity framework/programme
- Implement a cybersecurity framework/programme
- Control, monitor, measure and improve a cybersecurity framework/programme
- Certify your skills and be worldwide recognized as a CyberSecurity Lead Implementer professional



+351 212 103 732
training@behaviour-group.com
www.behaviour-group.com

ACQUIRE KNOWLEDGE AND UNDERSTANDING HOW TO SUPPORT THE IMPLEMENTATION OF A CYBERSECURITY PROGRAMME

Learning Objectives

With this course is intended that the trainees gain knowledge and understanding in the following subjects and have a successful completion of the education and examination components related to this certification.

- Understand fundamental principles and concepts related to cybersecurity;
- Identify and understand current frameworks for implementation, maintenance and audit of cybersecurity frameworks/programmes;
- Understand how to implement a cybersecurity framework/programme;
- Improve the capability for monitoring, analysis, mitigation, as well as decision making regarding any issue about cybersecurity;
- Develop knowledge and skills on how to improve and modernize a cybersecurity framework/programme

Course Details

Day 1: Introduction to cybersecurity concepts; Initiating and planning a cybersecurity framework/programme

- Course introduction
- Introduction to the process approach
- Presentation of the most recognized frameworks for cybersecurity
- Fundamental principles of a cybersecurity framework/programme of an organization
- Preliminary analysis and establishment of the maturity level of an existing cybersecurity framework/programme
- Writing a business case and a project plan for the implementation of a cybersecurity framework/programme

Day 2: Planning a cybersecurity framework/programme and operationalization

- Definition of the scope of a cybersecurity framework/programme
- Definition of a cybersecurity framework/programme policies, processes, procedures, and objectives
- Selection of the approach and methodology for managing risks and opportunities
- Managing risks for the cybersecurity framework/programme
- Knowledge, training, awareness and communication management

How do we do it?

- This training is provided based on the alternation of theory and practice:

- Sessions of lectures illustrated with examples based on real cases
- Practical exercises based on a full case study including role plays and oral presentations
- Review exercises to assist the exam preparation
- Practice test similar to the certification exam

- With the number of training participants limited to benefit from practical exercises

Day 3: Implementing a cybersecurity framework/programme

- Implementation of a document management framework
- Design and implementation of controls for access management and information protection
- Implementation of an awareness and training programme
- Implementation of processes and procedures to maintain and modernize the cybersecurity framework/programme

Day 4: Controlling, monitoring, measuring and improvement of a cybersecurity framework/programme

- Controlling and monitoring the cybersecurity framework/programme
- Development of metrics, performance indicators and dashboards in accordance with ISO 27004
- Management review of the cybersecurity framework/programme
- Implementation of a continual improvement and mitigation program

Day 5: Certification Exam

ACQUIRE KNOWLEDGE AND UNDERSTANDING HOW TO SUPPORT THE IMPLEMENTATION OF A CYBERSECURITY PROGRAMME



Prerequisites

Participants should understand English as the course documentation is in this language.

General Information

- The official CyberSecurity Lead Implementer examination is included on the course price
- A student manual, in English language, containing over 400 pages of information, practical examples, quizzes and exercise will be distributed to participants
- A BEHAVIOUR, 31 CPE/CPD (Continuing Professional Education/Continual Professional Development) participation certificate will be issued to participants
- Coffee-breaks in the morning and afternoon (applies to all training sessions happening at BEHAVIOUR®) are included

Exam

- The “CyberSecurity Lead Implementer” exam covers the following competence domains:
 - Fundamental principles, concepts and definitions of cybersecurity
 - Planning a cybersecurity framework/programme
 - Implementing a cybersecurity framework/programme
 - Performance evaluation, monitoring and measurement of a cybersecurity framework/programme
 - Continual improvement of a cybersecurity framework/programme
- Opened questions exam.
- Exam duration: 3 hours (180 minutes)
- Exam mark: 70%
- Exam type: Opened Book (only the manual provided for the training sessions)

Values of BEHAVIOUR Certification

*“Credibility on the market and recognition
by peers”*

What do you achieve?

- The principal competencies and knowledge skills needed by the market
- An overall comprehension on how to implement a cybersecurity framework/programme in an organization
- Ability to support an organization in managing and controlling a cybersecurity frameworks/programme regardless of their type and scale

Benefits of the Certification Program

- Demonstrate that the certified professional holds defined competencies based on best practices
- Allows employing organizations to make an informed selection of employees or services based on competencies
- Provides incentives to the professional to constantly improve his/her skills and knowledge
- Serves as a tool for employers to ensure

ACQUIRE KNOWLEDGE AND UNDERSTANDING HOW TO SUPPORT THE IMPLEMENTATION OF A CYBERSECURITY PROGRAMME

Certification

- After successfully completing the exam, participants can apply for the credentials of Certified CyberSecurity Lead Implementer
- A certificate will be issued to participants who successfully passed the exam and comply with all the other requirements related to the selected credential
- The requirements for "Lead Implementer" certification are:

Certification	Exam	Professional experience	CSF/P Audit experience	CSF/P project experience
Associate CyberSecurity Lead Implementer	CyberSecurity Lead Implementer Exam	None	None	None
CyberSecurity Implementer	CyberSecurity Lead Implementer Exam	3 years 2 years of cybersecurity related work experience	None	Project activities totaling 250 hours
CyberSecurity Lead Implementer	CyberSecurity Lead Implementer Exam	5 years 3 years of cybersecurity work experience	None	Project activities totaling 350 hours

About BEHAVIOUR®



BEHAVIOUR® is a training company specialized in information security, best practices and management systems since 2005.

- BEHAVIOUR® is an accredited company by DGERT (Portuguese Quality Training System).
- BEHAVIOUR® is certified on ISO 9001.
- BEHAVIOUR® is a training and certification company recognized internationally by its partners and its peers in Europe, USA, Canada, Latin America and Africa.

Contact and Registration:

For more information contact us at:
+351 212 103 732

training@behaviour-group.com
www.behaviour-group.com

Or,
visit the course web page at:
www.behaviour-group.com/PT/cybersecurity-lead-implementer-training/?lang=en

Calendar 2019: Upcoming course dates...

Please check the available dates and prices at:

www.behaviour-group.com

Related courses

CyberSecurity Informed User	ISO 27001 Foundation
CyberSecurity Professional	ISO 27001 Lead Implementer
CyberSecurity Lead Auditor	ISO 27001 Lead Auditor



ACQUIRE KNOWLEDGE AND UNDERSTANDING HOW TO SUPPORT THE IMPLEMENTATION OF A CYBERSECURITY PROGRAMME

What do you need to know about BEHAVIOUR®!

- BEHAVIOUR® presents you one of the most complete and updated catalogs of courses and certifications in the most worldwide recognized **principles, best practices, methodologies, management systems and frameworks** of the market.
- Whether in **Europe, Africa, Latin America, or any other international location**, you can count on BEHAVIOUR® to form and certify your knowledge and skills, or knowledge and skills of professionals who work with your organization in the best and most recent methodologies, principles, concepts, practices, frameworks and standards available.
- Integrated into our QMS, **we work continuously to ensure the highest quality of our training and recognition of our certifications**, requiring our experienced specialists a wide range of skills and the most recognized international certifications.
- **We continually update the content of our training offer** to align it with the market needs and requirements of our clients.
- It is this continued commitment on quality that sets us apart in the market and allows us to **train and certify the best and the most recognized professionals**.
- Because our customers are the driving force of our organization and its professionals their added value, BEHAVIOUR® uses the best, the most recognized and current methodologies in the whole process of training and certification, preparing and certifying professionals of the largest and most reputable international organizations ... it is they who make the difference, and it is through them that we ensure the recognition of our brand, **BEHAVIOUR® brand**.

ISO Training and Certification

- **BEHAVIOUR®** presents one of the most completed portfolios of training and consulting services in various ISO standards and respective management systems:
 - **ISO 27001** – Information security management system
 - **ISO 20000** – Service management system
 - **ISO 22301** – Business continuity management systems
 - **ISO 27031** – Disaster recovery
 - **ISO 27005** – Information security risk management
 - **ISO 31000** – Risk management
 - **ISO 28000** – Specification for security management systems for the supply chain
 - **ISO 50001** – Energy management
 - **ISO 21500** – Project management
 - **ISO 29001** – Petroleum, petrochemical and natural gas industries
 - **ISO 13053** – Six Sigma
 - **ISO 27034** – Application security guideline
 - **ISO 38500** – IT governance