PECB CERTIFIED ISO/IEC 27032
LEAD CYBERSECURITY MANAGER

MASTERING THE FUNDAMENTAL PRINCIPLES, CONCEPTS, APPROACHES, STANDARDS, METHODS, AND TECHNIQUES TO SET UP AND EFFECTIVELY MANAGE A CYBERSECURITY PROGRAM WITHIN AN ORGANIZATION BASED ON ISO/IEC 27032.

SUMMARY

This five day intensive course enables the participants to develop the knowledge and competence needed to support an organization in implementing and managing a Cybersecurity program based on ISO/IEC 27032. This training will enable participants to have an overview of Cybersecurity, to understand the relationship between Cybersecurity and other types of security, and stakeholders' role in Cybersecurity. This course can be used as guidance for addressing common Cybersecurity issues, and presents a framework that enables stakeholders to collaborate on resolving Cybersecurity issues.

WHO SHOULD ATTEND?

- Cybersecurity professionals
- Information security experts
- Project managers wanting to manage the Cybersecurity program
- Technical experts wanting to prepare themselves for Cybersecurity functions
- Persons responsible to develop the Cybersecurity program

COURSE AGENDA

DURATION: 5 DAYS

DAY 1

Introduction to Cybersecurity and related concepts as required by ISO/IEC 27032

- Course objective and structure
- Standard and regulatory framework
- Fundamental concepts and definitions of Cybersecurity
- Planning a Cybersecurity Program

DAY 2

Initiating a Cybersecurity Program

- Organizational structure
- Defining roles and responsibilities of stakeholders in Cybersecurity
- Establish policies and principles for governing Cybersecurity
- Risk management
- Risk assessment
- Risk analyses and evaluation

DAY 3

Implementing a Cybersecurity Program

- Implementation of a document management framework
- Information sharing and coordination
- Development of a training & awareness program
- Implementation of Cybersecurity controls
- Business Continuity
- Incident management

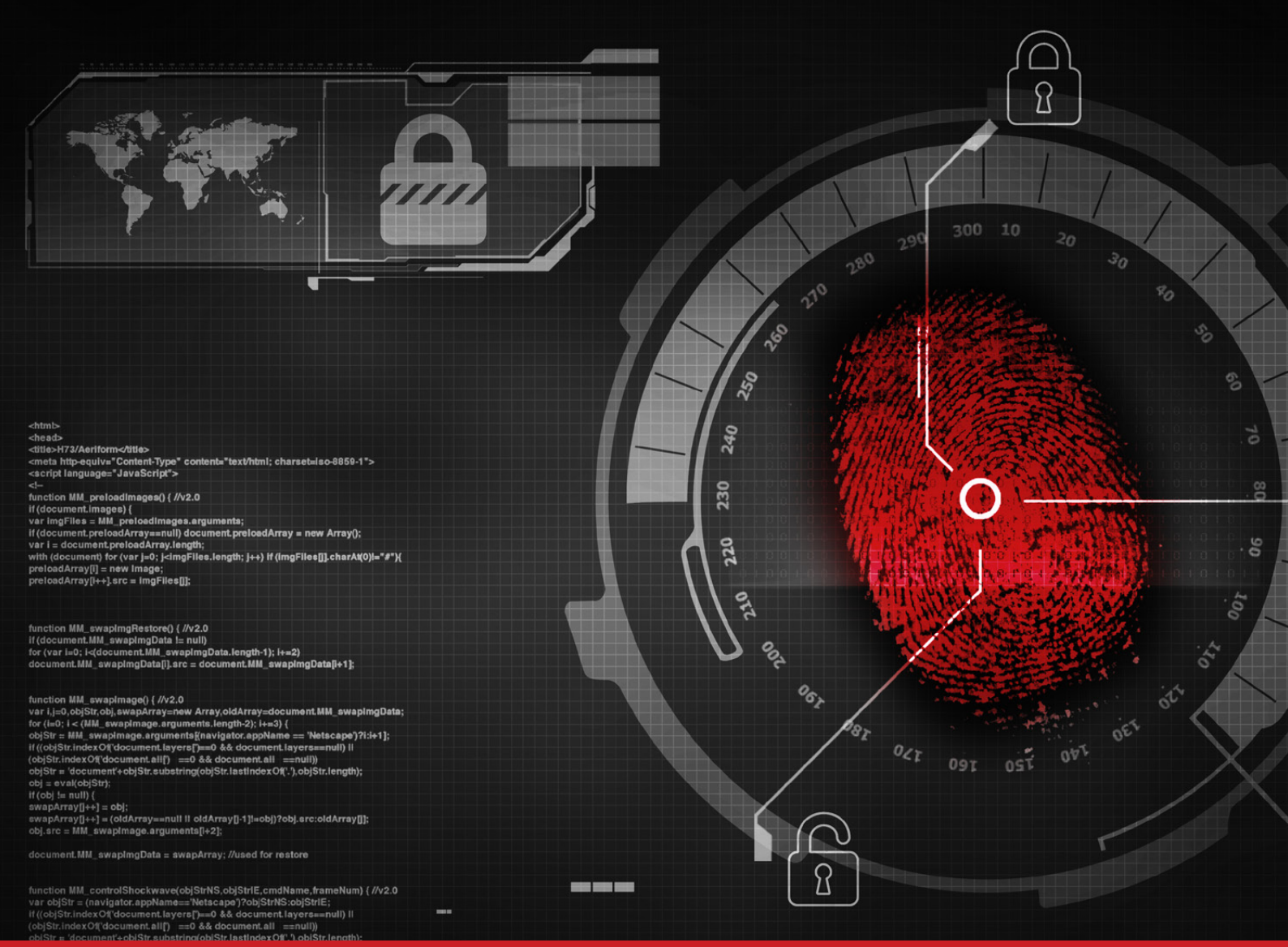
DAY 4

Cybersecurity assessment and performance

- Performance Measurement
- Self-Assessment
- Cybersecurity readiness
- Continual Improvement
- PECB Certification Scheme
- Closing the Training

DAY 5

Certification Exam



LEARNING OBJECTIVES

- To understand and acquire comprehensive knowledge on the components and operations of a Cybersecurity program in conformance withISO/IEC 27032
- To explain the goal, content and correlation between ISO/IEC 27032 and other standards, and operating frameworks
- To master concepts, approaches, standards, methods and techniques to set up, implement, and effectively manage a Cybersecurity program within an organization
- To be able to interpret the requirements of ISO/IEC 27032 in the specific context of an organization
- To acquire the necessary expertise to plan, implement, manage, control and maintain a Cybersecurity program as specified in ISO/IEC 27032
- To develop the expertise to advise an organization about best practices for managing Cybersecurity
- To strengthen personal skills that are necessary for the establishment and maintenance of a Cybersecurity program

EXAM

The "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" exam completely meets the requirements of the PECB Examination and Certification Program (ECP). The exam covers the following competence domains:

- Domain 1: Fundamental concepts and definitions of Cybersecurity
- Domain 2: Guidance for initiating, implementing and managing a Cybersecurity Program
- Domain 3: Guidance for roles and responsibilities of stakeholders in Cybersecurity
- Domain 4: Cybersecurity Risk Management and Cybersecurity Controls
- Domain 5: Monitor all activities related to Cybersecurity Program

- The "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" exam is available in English only
- Duration: 3 hours
- For more information about the exam, refer to PECB section on ISO/IEC 27032 Lead Cybersecurity Manager Exam

CERTIFICATION

- After successfully completing the "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" exam, participants can apply for one of the credentials listed below, depending on their criteria.
- A certificate will be issued to participants who successfully pass the exam and comply with all the other requirements related to the selected credential

Credential	Exam	Professional Experience	Cybersecurity Management experience	Other Requirements
PECB Certified ISO/IEC 27032 Provisional Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Exam	None	None	Signing the PECB code of ethics
PECB Certified ISO/IEC 27032 Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Exam	**Two years** One year of Cybersecurity Management related	Cybersecurity Management activities totaling 200 hours	Signing the PECB code of ethics
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Exam	**Five years** Two years of Cybersecurity Management related	Cybersecurity Management activities totaling 300 hours	Signing the PECB code of ethics

GENERAL INFORMATION

- Exam and certification fees are included in the training price
- A student manual containing over 400 pages of information and practical examples will be distributed to participants
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued to participants
- In case of failure of an exam, participants are allowed to retake the exam for free under certain conditions