# PECB Certified ISO/IEC 27032
Lead Cybersecurity Manager

### Master the implementation and management of a Cybersecurity Program based on ISO/IEC 27032

## Why should you take this training course?

In the era of digital transformation, with almost everything being done digitally from education, to business, to communication, cybersecurity has never been more important! One should not forget that as technology advances, so do malicious threats and attacks. As a result, there is an ever growing need for cybersecurity professionals, competent to protect people's data.

ISO/IEC 27032 Lead Cybersecurity Manager training course enables you to acquire the expertise and competence needed to support an organization in implementing and managing a cybersecurity program based on ISO/IEC 27032 and NIST Cybersecurity Framework. During this training course, you will gain a comprehensive knowledge of cybersecurity, the relationship between cybersecurity and other types of IT security, and the different stakeholders' role in cybersecurity.

## Why is this course more desirable than the others?

This course is an amalgamation of ISO/IEC 27032 and the NIST Cybersecurity Framework. The course not only elaborates the theoretical information provided in the aforementioned documents, but gives you practical advice based on real-life experience.

The development of this course is the result of strenuous work by PECB's network of experts and course developers.

@esdqrsdqhmf `kksgdmdbdrr`qx bnmbdosrne bxadqrdbtqhsx+xnt b`m rhsenqsgddw`l `mc `ookx enq` -ODBA Bdqshehdc HRN.HDB 27032 Lead Cybersecurity Manager" credential. By holding this credential, you will be able to demonstrate that you have the practical knowledge and professional capabilities to support and lead a team in managing cybersecurity. By obtaining your bdqshehb`shnm+xnt rgnvb`rd ` bdqs`hmrjhkkkdudkvghbg vhkkchrok`x `ccdc u`ktd mnsnmkxsn xntq oqnedrrhnm`kb`qddqats sn xntq organization as well. This can help you stand out from the crowd and increase your earning potential.

## What will the certification allow you to do?

Bdqshehb`shnmhrsgdenql`k qdbnfmhshnmnc oqnenejmnvkdcfd vghbg b`qqhdr`m hlonqs`msvdhfgs vgdm xnt `qd dmsdqhmsgdk`anq market, or when you want to advance in your career. Due to the technological advancements and the complexity of cyberattacks, the demand for information security professionals continues to grow.

ODBAhrrtdr bdqshehb`shnmrsg`sg` ud hmsdqm`shnm`kqdbnfmhshnmsg`sr kd`chmfsn lnq d dlokn xldms noonqstmhshdrenqxnt nql`jhmf you even more competitive in an already fast-developing job market.

## Who should attend this training course?

- Cybersecurity professionals
- Information Security experts
- Professionals seeking to manage a cybersecurity program
- Individuals responsible to develop a cybersecurity program
- IT specialists
- Information Technology expert advisors
- IT professionals looking to enhance their technical skills and knowledge

## Course agenda

Duration: 5 days

### Day 1 | Introduction to Cybersecurity and related concepts as recommended by ISO/IEC 27032

- Course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts in cybersecurity
- Cybersecurity program
- Initiating a cybersecurity program
- Analyzing the organization
- Leadership

### Day 2 | Cybersecurity policies, risk management and attack mechanisms

- Cybersecurity policies
- Cybersecurity risk management
- Attack mechanisms

### Day 3 | Cybersecurity controls, information sharing and coordination

- Cybersecurity controls
- Information sharing and coordination
- Training and awareness program

### Day 4 | Incident management, monitoring and continuous improvement

- Business continuity
- Cybersecurity incident management
- Cybersecurity incident response and recovery
- Testing in Cybersecurity
- Performance measurement
- Continuous improvement
- Closing the training

### Day 5 | Certification Exam

## Learning objectives

- Acquire a comprehensive understanding of the elements and operations of a Cybersecurity Program in conformance with ISO/IEC 27032 and NIST Cybersecurity Framework
- Acknowledge the correlation between ISO/IEC 27032, NIST Cybersecurity Framework, and other standards and operating frameworks
- Master the concepts, approaches, standards, methods, and techniques used to effectively set up, implement, and manage a cybersecurity program within an organization
- Kd`qm gnv sn hmsdqoqds sgd fthcdkhmdr ne HRN.HDB 16/21 hm sgd rodbĥb bnmsdws ne `m nqf`mhy`shnm
- L`rsdq sgd mdbdrr`qx dwodqshrd sn ok`m+ hlokdldms+ l`m`fd+ bnmsqnk+ `mc l`hms`hm ` bxadqrdbtqhsx oqnfq`l `r rodbĥdc hm ISO/IEC 27032 and NIST Cybersecurity Framework
- Acquire the necessary expertise to advise an organization on the best practices for managing cybersecurity

## Examination

**Duration: 3 hours**

Sgd !ODBA Bdqshĥdc HRN.HDB 16/21 Kd`c Bxadqrdbtqhsx L`m`fdq! dw`l lddsr sgd qdpthqdldmsr ne sgd ODBA Dw`lhm`shnm `mc Bdqshĥb`shnm Oqnfq`l 'DBO(- Sgd dw`l bnudqr sgd enkknvhmf bnlodsdmbx cnl`hmr9

**Domain 1** | **Fundamental principles and concepts of cybersecurity**

**Domain 2** | **Roles and responsibilities of stakeholders**

**Domain 3** | **Cybersecurity Risk Management**

**Domain 4** | **Attack mechanisms and cybersecurity controls**

**Domain 5** | **Information sharing and coordination**

**Domain 6** | **Integrating cybersecurity program in Business Continuity Management (BCM)**

**Domain 7** | **Cybersecurity incident management and performance measurement**

Enq rodbĥb hmenql`shnm `ants dw`l sxod+ k`mft`fdr `u`hk`akd+ `mc nsgdq cds`hkr+ okd`rd uhrhs sgd List of PECB Exams and the Examination Rules and Policies.

## Certification

After successfully completing the exam, you can apply for the credentials shown on the table below. You will receive a bdqshehb`sd nmbd xnt bnlokx vhsg `kk sgd qdpthqdldmsr qdk`sdc sn sgd rdkdbsdc bqdcdmsh`k+ Enq lnqd hmenql`shnm `ants HRN.HDB 16/21 bdqshehb`shnmr `mc sgd ODBA bdqshehb`shnm oqnbdrr+ okd`rd qdedq sn sgd Bdqshehb`shnm Qtkdr `mc Onkhbhdr

| Credential | Exam | Professional experience | CSMS project experience | Other requirements |
|---|---|---|---|---|
| **PECB Certified ISO/IEC 27032 Provisional Cybersecurity Manager** | ODBA Bdqshehdc ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent | None | None | Signing the PECB Code of Ethics |
| **PECB Certified ISO/IEC 27032 Cybersecurity Manager** | ODBA Bdqshehdc ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent | **Two years:** One year of work experience in cybersecurity | Bxadqrdbtqhsx `bshuhshdr9 a total of 200 hours | Signing the PECB Code of Ethics |
| **PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager** | ODBA Bdqshehdc ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent | **Five years:** Two years of work experience in cybersecurity | Bxadqrdbtqhsx `bshuhshdr9 a total of 300 hours | Signing the PECB Code of Ethics |
| **PECB Certified ISO/IEC 27032 Senior Lead Cybersecurity Manager** | ODBA Bdqshehdc ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent | **Ten years:** Seven years of work experience in cybersecurity | Bxadqrdbtqhsx `bshuhshdr9 a total of 1,000 hours | Signing the PECB Code of Ethics |

***Note:*** *PECB certified individuals who possess Lead Implementer and Lead Auditor credentials are qualified for the respective PECB Master credential, given that they have taken four additional Foundation exams related to this scheme. More detailed information about the Foundation exams and the Master credential requirements can be found here.*

## General information

- Bdqshehb`shnm `mc dw`lhm`shnm edDr `qd hmbktcdc hm sgd oqhbd ne sgd sq`hmhmf bntqrd
- Training material containing over 400 pages of information and practical examples will be distributed
- @m `ssdrs`shnm ne bntqrd bnlokdshnm vnqsg 20 BOC 'Bnmshmthmf Oqnedrrhnm`k Cdudknoldms( bqdchsr vhkk ad hrrtdc sn `kk candidates who have attended the training course
- In case you do not pass the exam, you can retake it within 12 months following the initial attempt for free