Certified DORA Lead Manager Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The PECB Certified DORA Lead Manager training course equips you with the necessary skills to lead and oversee the implementation of digital operational resilience strategies within financial entities to help them ensure compliance with European Union's Digital Operational Resilience Act (DORA).

As DORA will come into force on January 17, 2025, there's never been a more crucial time to grasp its implications and requirements thoroughly. Attending the PECB Certified DORA Lead Manager training course offers a unique opportunity to engage with industry experts and peers, fostering valuable discussions and insights into best practices for digital operational resilience.

Prerequisites

The main requirement for participating in this training course is having a fundamental understanding of information security and cyber security concepts, and familiarity with risk management principles.

Target Audience:

- Financial institutions executives and decision-makers
- Governance, risk, and compliance managers
- IT & security professionals
- Legal and regulatory affairs personnel
- Consultants and advisors specialising in financial regulation and cyber security

What You Will Learn

After successfully completing the training course, you will be able to:

1. Understand the regulatory landscape and compliance requirements outlined in DORA, focusing on key pillars such as ICT risk management, ICT-related incident management and reporting, digital operational resilience testing, and ICT third-party risk management
2. Implement effective strategies and measures to enhance digital operational resilience and mitigate ICT risks within financial institutions, aligning with DORA requirements and industry best practices
3. Identify, analyze, evaluate, and treat ICT risks relevant to the financial entities
4. Develop and maintain robust ICT risk management frameworks, incident response plans, business continuity and disaster recovery plans
5. Foster collaboration and communication with key stakeholders to ensure successful implementation and ongoing compliance with DORA
6. Utilise industry-standard tools and methodologies for monitoring, assessing, and managing ICT risks and vulnerabilities, enhancing the overall security posture of financial institutions