

Szkolenie: PECB
Risk assessment with OCTAVE

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	3000 PLN NETTO*	3 dni
Stacjonarne	Tablet CTAB	3400 PLN NETTO*	3 dni
Metoda dlearning	Tradycyjne	3000 PLN NETTO*	3 dni
Metoda dlearning	Tablet CTAB	3000 PLN NETTO*	3 dni

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00

Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

Cel szkolenia:

In this three-day intensive course participants develop the competence to master the basic risk management elements related to all assets of relevance for information security using OCTAVE method (including OCTAVE-S and OCTAVE Allegro). The OCTAVE method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was developed by CERT (Computer Emergency Response Team). Based on practical exercises and case studies, participants acquire the necessary knowledge and skills needed to perform an optimal information security risk assessment and manage risks in time by being familiar with their life cycle. This training fits perfectly in the framework of an ISO/IEC 27001:2005 standard implementation process.

Who should attend?

- Risk managers
- Persons responsible for information security or conformity within an organization
- Member of the information security team
- IT consultants
- Staff participating in the activities of risk assessment with the OCTAVE method

Learning objectives

- To understand the concepts, approaches, methods and techniques allowing an effective management of risk according to the OCTAVE method
- To develop the necessary skills to conduct a risk assessment with the OCTAVE method
- To master the steps to conduct a risk assessment with the OCTAVE method (including OCTAVE-

S and OCTAVE Allegro)

- To interpret the requirements of ISO 27001 on information security risk management
- To understand the relationship between the information security risk management, the security controls and the compliance with the requirements of different stakeholders of an organization
- To acquire the competence to implement, maintain and manage an ongoing information security risk management program
- To acquire the competence to effectively advise organizations on the best practices in information security risk management

Plan szkolenia:

- Day 1: Start of a risk assessment with OCTAVE
 - Concepts and definitions related to risk management
 - Standards, frameworks and methodologies in risk management
 - Presentation of OCTAVE
 - Phase 1 - Process 1 to 3 (Understanding the Organization)
 - Phase 1 - Process 4 (Create profile threats)
 - Phase 2 - Process 5 (identification of key components)
- Day 2: Assessment of vulnerabilities and risk, according to OCTAVE
 - Phase 2 - Process 5 (Continued)
 - Phase 2 - Process 6 (Evaluation of selected components)
 - Phase 3 - Process 7 (Conduct the risk assessment)
 - Phase 3 - Process 8 (Development of Protection Strategy)
- Day 3: The OCTAVE Method Implementation approach and conclusion
 - Phase 3 - Process 8 (Development of a Protection Strategy - cont.)
 - The OCTAVE Method Implementation Guide
 - OCTAVE - S and OTAVE Allegro
 - Summary

Wymagania:

A basic knowledge of risk management is recommended.

Poziom trudności



Certyfikaty:

The participants will obtain certificates signed by PEBC (course completion).

Prowadzący:

Authorized PEBC Trainer.

Informacje dodatkowe:

- This training is based on both theory and practice:
 - Sessions of lectures illustrated with examples based on real cases
 - Practical exercises based on case studies including role playing and oral presentations
 - Review exercises to assist the exam preparation
 - Practice test similar to the certification exam
- To benefit from the practical exercises, the number of training participants is limited
- A copy of the official documentation on OCTAVE (including OCTAVE-S and OCTAVE Allegro) published by CERT is given to participants together with a student manual containing over 250 pages of information and practical examples
- A participation certificate of 21 CPD (Continuing Professional Development) credits is awarded to participants