PECB RISK ASSESSMENT WITH THE OCTAVE METHOD

DEVELOPING THE NECESSARY SKILLS TO PERFORM A RISK ASSESSMENT BASED ON THE OCTAVE METHOD

SUMMARY

It should be noted that this training can be delivered as a specific course or in combination with ISO 27005 or ISO 31000. 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. 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 standard implementation process.

WHO SHOULD ATTEND?

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

COURSE AGENDA

DURATION: 3 DAYS

DAY 1

Start of a risk assessment with OCTAVE

- Standards, frameworks and methodologies in risk management
- 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
- Tailoring the evaluation to your organization
- OCTAVE -S

EXAM AND CERTIFICATION

- Not applicable

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
- 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

GENERAL INFORMATION

- A copy of the official documentation on OCTAVE published by CERT is given to participants together with a participant manual containing over 250 pages of information and practical examples
- A participation certificate of 21 CPD (Continuing Professional Development) credits is awarded to the participants