Management and Information Technology Solutions

Decker Consulting GmbH

Training Catalog

Decker Consulting GmbH

Birkenstrasse 49

CH-6343 Rotkreuz

Revision 9.1

05.12.2018

public

PECB

Authorized Training

Partner

Table of contents

1 General information

1.1 Trainers

PD Dr. Karsten M. Decker, CEO Decker Consulting GmbH, is a Certified ISO/IEC 27001 Lead Auditor and a PECB Certified Trainer. He holds a B.Sc. in Chemistry, a M.Sc. and a Ph.D. in Theoretical Physics as well as a Habilitation (Dr. habil.) in Applied Computer Science. Karsten Decker has more than 30 years of experience as a manager in the fields of information security and IT service management, in consulting, as reviewer and auditor, as university teacher and in professional training. As a member of the standard committee INB NK 149 UK 7 of the Swiss Association for Standardization (SNV), he actively contributes to the development of the standards of the ISO 27000 family in ISO JTC 1/SC 27. Karsten Decker is coauthor of the standards ISO/IEC 27001:2013, ISO/IEC 27002:2013 and ISO/IEC 27003:2017. Currently, he is also involved as coauthor in the revision of the standard ISO/IEC 27005. As a member of the DACH council for the German translation of ISO/IEC 27000:2016, ISO/IEC 27001:2013 and ISO/IEC 27002:2013 as well as Annex SL of the ISO/IEC Directives he has also co-written the official German editions.

1.2 Course manuals

Our training courses utilizes the training material developed, maintained and certified by the Professional Evaluation and Certification Board Inc. (PECB), incorporated in Canada and the USA. This material is the best available in the market worldwide.

For every single training day, the course manual consists of more than 100 pages of information, practical examples, exercises and numerous references to and excerpts from all relevant standards. The course manuals are completed by a comprehensive case study where this is important to achieve an optimal success of training. These manuals are also well suited as reference books.

1.3 Course languages

The training courses are offered in English or German.

1.4 Training course and trainer certification

The training courses and the trainers are certified by PECB and are exclusively conducted by trainers that have passed through the PECB Trainer Certification Program. All trainers have long-term, proven and documented training experience.

1.5 Continuing Professional Development (CPD) participation certificate

For each full training day, a 7 CPD participation certificate is issued to all participants.

1.6 Certification exam and exam language

The certification exam and the related material is certified by PECB and fully meet the requirements of the PECB Examination Certification Programme (ECP). PECB has been accredited by the International Accreditation Service (IAS) as personnel certification body according to the international standard ISO/IEC 17024:2012 (Conformity assessment – General requirements for bodies operating certification of persons).

Participation in the final written certification exam is not compulsory. Participants who pass the exam can register with PECB free of charge and, after signing the PECB code of ethics and depending on their level of experience, will be awarded a professional certification title. For more specific information on the title, please refer to the respective course description.

Independently of the training language, each participant can take the certification exam in English or German.

The duration of the certification exam depends on the course. Participants that take an exam in a language which is not their mother tongue obtain extra time to complete the exam.

If a participant fails to pass the certification exam, he can re-register to an exam from PECB at no additional cost. Moreover, it is possible to re-register at marginal costs to a second sitting of the same course (complete or in part).

1.7 Course duration, organization and times

- Depending on the course, the course duration is two to five days
- The five day courses can be trained in up to two blocks over a maximum period of three weeks
- To ensure an extensive training experience, the number of participants is limited
- Course times on training days are 08:00 – 18:00
- Starting times can be adjusted according to participants' needs

1.8 Course fees

The course fee depends on the duration of the course. Please refer to the respective course description.

1.9 Examination fees

The fee for the optional certification exam is CHF 500.00 + 7.7% VAT for all courses. Registration with PECB and the certification fee are included in the exam fee.

1.10 Internal courses

All training courses are also offered as internal courses. The emphasis of the various topics can be adjusted to the organization's specific needs. Fees upon request.

1.11 References

Up to now, the certified training and examination material from PECB was used to train more than 20,000 professionals in over 100 countries worldwide. Participants include representatives from companies such as Accenture, Atos, CSC, HP, IBM, IMF, KPMG, Lockheed Martin, Merck, Microsoft, Novartis, Orange, Swiss Life AG and United Nations and from industries such as certification bodies, defense, governmental organizations, insurance, life science, management and IT consulting, network coordination centers, private banks, software development and telecommunication providers.

The feedback from all participants is excellent. Participants especially emphasize:

- Courses based on real practice, not just theory
- Very well educated trainers with large competence and experience
- Very good discussions of course contents and participants requests
- Very high quality, detailed and extensive course manuals that are also well-suited as reference books

Names of individuals trained are available on request.

2 PECB Certified ISO/IEC 27001 Lead Auditor (5 days)

2.1 Summary

In this five-day intensive course participants develop the competence needed to audit an Information Security Management System (ISMS) and to manage a team of auditors by applying widely recognized audit principles, procedures and techniques.

During this training, participants acquire the necessary knowledge and skills to proficiently plan, perform and follow-up audits compliant with the certification process of ISO/IEC 27001:2013. Based on lectures, practical exercises alone or in a group, role plays, a case study and written home work, participants develop the abilities (mastering audit techniques) and skills (managing audit teams and an audit programme, communicating with customers, conflict resolution, etc.) necessary to the efficient conduct of an audit.

The training is aligned with ISO 19011:2018 (Guidelines for auditing management systems), the Generally Accepted Auditing Standards (GAAS), the professional practices of the Institute of Internal Auditors (IIA) as well as with the practices of the International Federation of Accountants (IFAC).

2.2 Who should attend?

- Information security officers
- Compliance officers
- Data privacy officers
- Internal auditors
- Auditors wanting to perform and lead ISMS certification audits
- Project managers and consultants wanting to master the ISMS audit process
- CxO and senior managers responsible for the governance of an enterprise and the management of its inherent risks
- Members of information security teams

2.3 Learning objectives

- Acquire the competence to perform an ISO/IEC 27001:2013 internal audit following ISO 19011:2018 guidelines
- Acquire the competence to perform an ISO/IEC 27001:2013 certification audit following ISO 19011:2018 guidelines and the requirements of ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015
- Acquire the competence necessary to manage an ISMS audit team
- Understand the operation of the ISMS in accordance with ISO/IEC 27001:2013
- Understand the relationship between an ISMS, including risk management and controls, and compliance with the requirements of different interested parties of the organization
- Improve the skills to analyze the internal and external context of an organization, to determine the risk assessment requirements and to make audit decisions in the context of an ISMS

2.4 Training program

2.4.1 Day 1: Introduction to information security and ISO/IEC 27001

- Standards and legal and regulatory frameworks
- Certification process

– Fundamental principles of information security
– ISO/IEC 27001:2013 information security management system

2.4.2 Day 2: Principles of auditing, preparing and launching an audit

– Fundamental concepts and principles of auditing
– Audit approach based on evidence and on risk
– Initiating the audit
– Stage 1 audit
– Preparing the stage 2 audit (on-site audit)

2.4.3 Day 3: On-site audit activities

– Stage 2 audit (overview)
– Communication during the audit
– Audit procedures
– Creating audit test plans
– Drafting audit findings and nonconformity reports

2.4.4 Day 4: Closing the audit and audit follow-up

– Documentation of the audit and quality review
– Closing the audit
– Evaluating action plans by the auditor
– Beyond the initial audit
– Managing an internal audit programme
– Competence and evaluation of auditors

2.4.5 Day 5: PECB exam

– PECB Certified ISO/IEC 27001 Lead Auditor exam (optional, three hours)

2.5 Prerequisites

PECB Certified ISO/IEC 27001 Foundation or a basic knowledge of ISO/IEC 27001:2013 is recommended.

2.6 Continuing Professional Development (CPD) participation certificate

A 31 CPD participation certificate is issued to all participants.

2.7 Certification exam

The optional PECB Certified ISO/IEC 27001 Lead Auditor exam takes place at the beginning of the last day and has a duration of three hours. The exam fully meets the requirements of the PECB Examination Certification Programme (ECP) and covers the following competence domains:

– Fundamental principles of information security
– Information security management systems
– Fundamental concepts and principles of auditing
– Preparing an ISO/IEC 27001:2013 audit

- Conducting an ISO/IEC 27001:2013 audit
- Concluding an ISO/IEC 27001:2013 audit
- Managing an ISO/IEC 27001:2013 audit programme

Successful participants can register with PECB free of charge and, after signing the PECB code of ethics and depending on their level of experience, will be awarded the title *PECB Certified ISO/IEC 27001 Provisional Auditor*, *PECB Certified ISO/IEC 27001 Auditor* or *PECB Certified ISO/IEC 27001 Lead Auditor*.

2.8 Course organization and times

- The course can be trained in up to two blocks over a maximum period of three weeks
- To ensure an extensive training experience, the number of participants is limited to 4 – 8
- Course times on training days are 08:00 – 18:00
- Starting times can be adjusted according to participants' needs

2.9 Course fee

The course fee is CHF 4,000.00 + 7.7% VAT. This fee comprises the course manual, a 31 CPD participation certificate and the expenses for coffee and lunch breaks.

2.10 Examination fee

The fee for the optional certification exam is CHF 500.00 + 7.7% VAT. Registration with PECB and the certification fee are included in the exam fee.

3 PECB Certified ISO/IEC 27001 Lead Implementer (5 days)

3.1 Summary

In this five-day intensive course participants develop the competence to support an organization in implementing and managing an Information Security Management System (ISMS) as specified in ISO/IEC 27001:2013. Participants will also learn to master good practice for implementing information security controls from the 14 security control clauses of ISO/IEC 27002:2013.

During this training, participants acquire the necessary knowledge and skills to plan, implement, manage, monitor and maintain an ISMS as specified in ISO/IEC 27001:2013. Based on lectures, practical exercises alone or in a group, a case study and written homework, participants also learn how the implementation of an ISMS is supported by the three standards ISO/IEC 27003:2017 (Information security management system implementation guidance), ISO/IEC 27004:2016 (Information security management – Measurement) and ISO/IEC 27005:2018 (Information security risk management).

3.2 Who should attend?

- Information security officers
- Compliance officers
- Data privacy officers
- Project managers and consultants
- CxO and senior managers
- Members of information security teams

3.3 Learning objectives

- Understand the components and the operation of an ISMS based on ISO/IEC 27001:2013 and its principal processes
- Understand the relationship between an ISMS, including risk management and controls, and compliance with the requirements of different interested parties of the organization
- Develop the skills to analyze the internal and external context of an organization and to perform the risk assessment
- Acquire the skills necessary to interprete the requirements of ISO/IEC 27001:2013 in the specific context of an organization
- Master the concepts, approaches, standards, methods and techniques to support an organization in planning, implementing, managing, monitoring and maintaining an effective ISMS
- Acquire the competence necessary to manage an ISMS implementer team

3.4 Training program

3.4.1 Day 1: Introduction to information security and ISO/IEC 27001

- ISO standards
- Fundamental principles of information security
- ISO/IEC 27001:2013 information security management system

3.4.2 Day 2: Initiating the implementation, context and leadership

- Context of the organization, I

- Gap analysis
- ISMS project
- Context of the organization, II
- Leadership

3.4.3 Day 3: Planning, support and operation

- Planning
- Support
- Operation

3.4.4 Day 4: Performance evaluation and improvement

- Performance evaluation and improvement
- Preparing and conducting the certification audit
- Competence and evaluation of implementers

3.4.5 Day 5: PECB exam

- PECB Certified ISO/IEC 27001 Lead Implementer exam (optional, three hours)

3.5 Prerequisites

PECB Certified ISO/IEC 27001 Foundation or a basic knowledge of ISO/IEC 27001:2013 is recommended.

3.6 Continuing Professional Development (CPD) participation certificate

A 31 CPD participation certificate is issued to all participants.

3.7 Certification exam

The optional PECB Certified ISO/IEC 27001 Lead Implementer exam takes place at the beginning of the last day and has a duration of three hours. The exam fully meets the requirements of the PECB Examination Certification Programme (ECP) and covers the following competence domains:

- Fundamental principles of information security
- Information security management systems
- Planning an ISMS based on ISO/IEC 27001:2013
- Implementing an ISMS based on ISO/IEC 27001:2013
- Monitoring, measuring and evaluating an ISMS based on ISO/IEC 27001:2013
- Continual improvement of an ISMS based on ISO/IEC 27001:2013
- Preparing the certification audit of an ISMS

Successful participants can register with PECB free of charge and, after signing the PECB code of ethics and depending on their level of experience, will be awarded the title *PECB Certified ISO/IEC 27001 Provisional Implementer*, *PECB Certified ISO/IEC 27001 Implementer* or *PECB Certified ISO/IEC 27001 Lead Implementer*.

3.8 Course organization and times

- The course can be trained in up to two blocks over a maximum period of three weeks
- To ensure an extensive training experience, the number of participants is limited to 4 – 8

- Course times on training days are 08:00 – 18:00
- Starting times can be adjusted according to participants' needs

3.9 Course fee

The course fee is CHF 4,000.00 + 7.7% VAT. This fee comprises the course manual, a 31 CPD participation certificate and the expenses for coffee and lunch breaks.

3.10 Examination fee

The fee for the optional certification exam is CHF 500.00 + 7.7% VAT. Registration with PECB and the certification fee are included in the exam fee.

4 PECB Certified ISO/IEC 27005 Foundation (2 days)

4.1 Summary

In this two-day intensive course participants develop the competence to master the basic risk management elements related to all assets of relevance for information security using the ISO/IEC 27005:2018 standard as a reference framework.

Based on practical exercises and a case study, participants acquire the necessary knowledge and skills 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 27001:2013 implementation process.

4.2 Who should attend?

- Risk managers
- Persons responsible for information security in an organization
- Members of information security teams
- Consultants in information security
- CxO and senior managers responsible for the governance of an enterprise and the management of its inherent risks

4.3 Learning objectives

- Understand the concepts, approaches, methods and techniques allowing an effective management of risk according to ISO/IEC 27005:2018
- Interpret the requirements of ISO/IEC 27001:2013 on information security risk management
- Understand the relationship between the information security risk management, the security controls and the compliance with the requirements of different interested parties of an organization
- Acquire the competence to implement, maintain and manage an ongoing information security risk management program according to ISO/IEC 27005:2018
- Acquire the competence to effectively advise organizations on good practice in information security risk management

4.4 Training program

4.4.1 Day 1: Introduction, risk management program, risk identification and analysis

- Concepts and definitions related to risk management
- Standards, frameworks and methodologies in risk management
- Implementation of an information security risk management program
- Risk identification
- Risk analysis

4.4.2 Day 2: Risk evaluation, treatment, acceptance, communication and surveillance

- Risk evaluation
- Risk treatment
- Acceptance of information security risks and management of residual risks
- Information security risk communication

– Information security risk monitoring and review
– PECB Certified ISO/IEC 27005 Foundation exam (optional, two hours)

4.5 Prerequisites

None.

4.6 Continuing Professional Development (CPD) participation certificate

A 14 CPD participation certificate is issued to all participants.

4.7 Certification exam

The optional PECB Certified ISO/IEC 27005 Foundation exam takes place at the end of the second training day and has a duration of two hours. The exam fully meets the requirements of the PECB Examination Certification Programme (ECP) and covers the following competence domains:

– Fundamental concepts, approaches, methods and techniques of risk management
– Implementation of a risk management program
– Information security risk assessment based on ISO/IEC 27005:2018

Successful participants can register with PECB free of charge and, after signing the PECB code of ethics and depending on their level of experience, will be awarded the title *PECB Certified ISO/IEC 27005 Foundation*.

4.8 Course organization and times

– To ensure an extensive training experience, the number of participants is limited to 4 – 8
– Course times are 08:00 – 18:00
– Starting times can be adjusted according to participants' needs

4.9 Course fee

The course fee is CHF 2,000.00 + 7.7% VAT. This fee comprises the course manual, a 14 CPD participation certificate and the expenses for coffee and lunch breaks.

4.10 Examination fee

The fee for the optional certification exam is CHF 500.00 + 7.7% VAT. Registration with PECB and the certification fee are included in the exam fee.

5 PECB Certified ISO/IEC 27005 Risk Manager (3 days)

5.1 Summary

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 the ISO/IEC 27005:2018 standard as a reference framework.

Based on practical exercises and a case study, participants acquire the necessary knowledge and skills to perform an optimal information security risk assessment and manage risks in time by being familiar with their life cycle. Participants are also introduced to the different methods of risk assessment used on the market, for instance, OCTAVE, MEHARI, EBIOS and Harmonized TRA. This training fits perfectly in the framework of an ISO/IEC 27001:2013 implementation process.

5.2 Who should attend?

- Risk managers
- Persons responsible for information security in an organization
- Members of information security teams
- Consultants in information security
- CxO and senior managers responsible for the governance of an enterprise and the management of its inherent risks

5.3 Learning objectives

- Understand the concepts, approaches, methods and techniques allowing an effective management of risk according to ISO/IEC 27005:2018
- Interpret the requirements of ISO/IEC 27001:2013 on information security risk management
- Understand the relationship between the information security risk management, the security controls and the compliance with the requirements of different interested parties of an organization
- Acquire the competence to implement, maintain and manage an ongoing information security risk management program according to ISO/IEC 27005:2018
- Acquire the competence to effectively advise organizations on good practice in information security risk management

5.4 Training program

5.4.1 Day 1: Introduction, risk management program, risk identification and analysis

- Concepts and definitions related to risk management
- Standards, frameworks and methodologies in risk management
- Implementation of an information security risk management program
- Risk identification
- Risk analysis

5.4.2 Day 2: Risk evaluation, treatment, acceptance, communication and surveillance

- Risk evaluation
- Risk treatment

– Acceptance of information security risks and management of residual risks
– Information security risk communication
– Information security risk monitoring and review

5.4.3 Day 3: Introduction to risk assessment methods; certification exam

– Introduction to OCTAVE
– Introduction to MEHARI
– Introduction to EBIOS
– Introduction to Harmonized TRA
– PECB Certified ISO/IEC 27005 Risk Manager exam (optional, two hours)

5.5 Prerequisites

None.

5.6 Continuing Professional Development (CPD) participation certificate

A 21 CPD participation certificate is issued to all participants.

5.7 Certification exam

The optional PECB Certified ISO/IEC 27005 Risk Manager exam takes place at the end of the third training day and has a duration of two hours. The exam fully meets the requirements of the PECB Examination Certification Programme (ECP) and covers the following competence domains:

– Fundamental concepts, approaches, methods and techniques of risk management
– Implementation of a risk management program
– Information security risk assessment based on ISO/IEC 27005:2018

Successful participants can register with PECB free of charge and, after signing the PECB code of ethics and depending on their level of experience, will be awarded the title *PECB Certified ISO/IEC 27005 Provisional Risk Manager, PECB Certified ISO/IEC 27005 Risk Manager or PECB Certified ISO/IEC 27005 Lead Risk Manager*.

5.8 Course organization and times

– To ensure an extensive training experience, the number of participants is limited to 4 – 8
– Course times are 08:00 – 18:00
– Starting times can be adjusted according to participants' needs

5.9 Course fee

The course fee is CHF 2,800.00 + 7.7% VAT. This fee comprises the course manual, a 21 CPD participation certificate and the expenses for coffee and lunch breaks.

5.10 Examination fee

The fee for the optional certification exam is CHF 500.00 + 7.7% VAT. Registration with PECB and the certification fee are included in the exam fee.

