Auditing GDPR maturity and compliance

GDPR essentials and guidance on tools and techniques to assess an organisation's maturity on Data Protection and GDPR compliance

Overview

This one-day training class helps auditors and audit managers to understand, and be able to develop a risk-based audit approach to assess compliance with the GDPR and data protection procedures. The GDPR introduced new and additional responsibilities for organisations processing personal data and assigned more rights to the individuals whose personal data is processed. This requires the implementation of additional processes and robust procedures and is not at all limited to IT security.

First, basic GDPR principles will be discussed and clarified through the use of practical cases so that participants understand the essential control objectives and required controls. The training will include an overall Data Protection maturity assessment model to assist with a broad and efficient screening of the overall maturity and to quickly identify blind spots and poor controls.

Next, participants will be coached on the development of compliance audit programs for specific high-risk GDPR provisions such as data subject rights, 3rd party processors of personal data, handling of data breaches and records of processing activities. This will happen through a series of exercises, feedback sessions and class discussions.

Objectives

- Obtain profound knowledge on data protection key risk areas and processes in order to understand key areas to focus on during audits.
- Learn how to use good practice checklists such as the "EU GDPR checklist for data controllers" to help you secure your organization, protect your customers' data, and avoid costly fines for non-compliance.
- Receive guidance on audit tools and techniques which will enhance the efficiency and effectiveness of auditing GDPR compliance.

Topics covered

- Accountability and governance around the DPO function, privacy policies and training
- Processing principles such as data minimization, legitimate purposes, lawful processing, appropriate technical or organizational measures to ensure security of personal data.
- Risk assessments and Data Protection Impact Assessment
- Completeness and accuracy of records of processing activities
- Provision and execution of data subject rights
- Obtaining consent and communication of privacy notices

- Handling of, and reporting on, data breaches
- Data Processing Agreements with 3rd party processors of personal data

Including

The class will include practical examples, full group discussions and individual exercises. The training class itself and all materials will be provided in English. As a preparation; please read the joint FERMA and ECIIA publication "GDPR and Corporate Governance: the Role of Internal Audit and Risk Management One Year After Implementation", issued November 2019.

Who should attend?

Internal auditors, audit managers and directors with basic knowledge on the GDPR and with a keen interest to gain an in-depth understanding of the GDPR implications on an organisation's data protection procedures and how Internal Audit can provide independent assurance over the key risks relating to the GDPR.

About the facilitator

Koen Albers

Experienced Professional in Data Privacy, Auditing and Fraud Risk Management

Koen Albers's experience includes over 20 years in internal audit, IT governance, data protection and fraud risk management. After 10 years as an ICT project manager in banking and insurance (Belgium and Norway), his career as an auditor started with an international ICT service provider, EDS, where he quickly became manager and director responsible for the audit function in EMEA and Asia-Pacific, managing a team of 20+ auditors. In 2009, he switched to the public sector where he has developed or reorganised the internal audit function in De Watergroep, MIVB-STIB and Port of Antwerp. Since 2018, Mr. Albers has been consulting and advising organisations in the domains of governance, data privacy and protection, fraud risk management and internal audit. For the last 10 years, he's also providing training on internal audit, data protection and fraud risk management. Mr. Albers is a member of the VDAB and the OISZ audit committee and is a board member of Cera and ACFE Belgium. He has a Master's degree "Commercial and Managerial Engineer" (KU Leuven), and is a Certified Information Systems Auditor (CISA),

Fraud Examiner (CFE), Information Security Manager (CISM) and a Licensed Private Detective.