APEX
QUALITY ASSURANCE

4-Day

VDA ISA TISAX and ISO/IEC 27001:2013

Internal Auditor Training

Information Security Management Systems

Register by phone

919-635-5581

Register online

www.apexqualityassurance.com

Exemplar Global

VDA ISA TISAX and ISO/IEC 27001 (4-Day)

At A Glance

Lead Auditor Training for Information Security Management Systems

This four-day course was developed to cover all requirements of the ISO/IEC 27001:2013 standard, as well as provide awareness and understanding of the requirements of the TISAX information security assessment maturity model (ISA released by the VDA) and illustrate important linkages to the controls and requirements from ISO/IEC 27001:2013.

The course includes definitions from ISO/IEC 27000:2018 (Information Security Management Systems – Overview and Vocabulary), Guidance from ISO/IEC 27003:2017 (Information Security Management System Implementation and Guidance) and auditing requirements from both ISO 19011:2018 (Guidelines for Auditing Management Systems) and ISO/IEC 27007:2017 (Guidelines for Information Security Management Systems Auditing). Group exercises and case studies will be used to develop the required skills.

Other topics covered include the auditing process and methodologies, e. g., planning and conducting an audit, writing nonconformity statements, preparing an audit summary and report, and verifying corrective actions following the requirements of ISO 19011 and ISO 27007. Auditing case studies to develop skills for identifying nonconformities will be used.

This course is being partnered with Omnex who is an Exemplar Global Certified TPECS provider for the Exemplar Global AU Competency Unit. This three-day course has been developed to satisfy the Exemplar Global AU Examination Profile and, as such, all attendees who successfully pass the exams during this course will achieve a Certificate of Attainment for the Exemplar Global-AU competency unit.

Who Should Attend

Internal Auditor Training for Information Security Management Systems

This seminar is primarily designed for internal auditor candidates, but can also be valuable for Information Security Assurance Managers, ISO/IEC 27001:2013 Implementation and/or Transition Team Members, Management Representatives, and all others who would like to develop competency in ISO/IEC 27001:2013 and the auditing process for first party auditing.

An understanding of the ISO/IEC 27001:2013 requirements and/or work experience in applying ISO/IEC 27001:2013 is recommended. An understanding of Risk Management for Information Security Management – there is a whitepaper available on the VDA TISAX information portal – is also important.

VDA ISA TISAX and ISO/IEC 27001 (4-Day)

Seminar Goals

Lead Auditor Training for Information Security Management Systems

- Understand the application of Information Security Assessment principles, and maturity of controls
- Understand the application of Information Security Management principles in the context of ISO/IEC 27001:2013.
- Relate the Information Security Management system to the organizational products, services, activities and operational processes.
- Relate organization's context and interested party needs and expectations to the planning and implementation of an organization's Information Security Management system.
- Understand the application of the principles, procedures and techniques of auditing.
- Understand the conduct of an effective audit in the context of the auditee's organizational situation.
- Understand the application of the regulations, and other considerations that are relevant to the management system, and the conduct of the audit.
- Practice personal attributes necessary for the effective and efficient conduct of a management system audit.

VDA ISA TISAX and ISO/IEC 27001 (4-Day)

Seminar Outline

Internal Auditor Training for Information Security Management Systems

Day One:

- Introduction and Welcome
- What is TISAX and Why Do We Need an Information Security Management System?
- Expectations of Interested Parties
- Introduction to the VDA Information Security Assessment workbook
- TISAX Requirements – Shoulds, Musts and Shalls
- Attainment of Maturity Levels
- A Look at Related ISO/IEC 27001:2013 ISMS Clauses and Requirements
- Additional (Good to Know) Information for Implementation

Day Two:

- The ISO Standards Explained
- Introduction to ISO/IEC 27001:2013 and Key Terms from the ISO 27000:2014 – Overview and Vocabulary
- ISO/IEC 27001:2013 Requirements Including Applicable Guidance from ISO 27003:2017 o Group Exercise:
  - Context of the Organization
  - Group Exercise: Interested Parties
  - Group Exercise: Audit Scenarios
  - Group Exercise : IT Security Controls
- Understanding ISMS Final Exam

Day Three:

- Process Approach to Auditing, Turtle Diagrams and Audit Trails
- Audit Guidance, Definitions and Principles
- The Audit Program
- Audit Planning and Preparation including ISO 27007 Guidelines for Information Security Management Systems Auditing
  - Breakout Exercise 1: Writing an Objective and Scope Statement
  - Breakout Exercise 2: Documentation Review
  - Breakout Exercise 3: Creating an Audit Plan

Day Four:

- Performing the Audit
  - Breakout Exercise 4: Performing an Audit
- Writing Nonconformity Statements
  - Breakout Exercise 5: Writing Nonconformity Statements
- Closing Meeting
- Completing the Audit Report
- Corrective Action and Close-Out
- Management Systems Auditing Final Exam

Attendees successfully completing the examinations provided in conjunction with this course receive a Certificate of Completion from Omnex, a partner of Apex Quality Assurance.