Information Security Risk Management (2 days)

Course Description

With the increasing number of internal and external information security threats, organizations recognize the importance of adopting a formal risk management program. Without a mechanism to identify, analyze and manage information security risks, it's difficult for organizations to prioritize their security remediation efforts and resource allocation and associated costs. This leaves organizations more susceptible to security breaches, which can lead to financial and reputational damage.

Building on the concepts and framework specified in ISO/IEC 27001, ISO/IEC 27005:2018 provides guidelines for adopting an information security risk management approach that is appropriate to all organizations.

Course objectives

This course aims to provide you with clear and practical guidance on the framework and steps involved to identify, analyse and manage information security risks. It will help you to review your existing risk treatments and controls and ensure they are appropriate to manage and reduce the identified risks. This will give you the confidence to get the most effective allocation of resources in place to address information security issues for your organization.

Candidates should expect to gain competencies in the following areas after successful completion of the training course:

- Explain concepts specific to information risk management, including terms and definitions
- Recognize and evaluate typical information security risks faced by organizations
- Explain how ISO/IEC 27005:2018 integrates and interfaces with other standards, such as ISO/IEC 27001:2013
- Determine the value of the information assets under your control
- Prioritize and choose appropriate risk treatments

The course includes:

- Course reference manual containing copy of course slides, support documents, quizzes and answers
- Course Certificate

Audience

The course is designed for and ne who wants to learn about Identifying and analyzing information security risks, How risks can be evaluated, What treatments, controls and measures can be implemented in order to mitigate risks, Ongoing governance and risk monitoring processes and

The course is applicable to individuals from any size or type of organization who are currently involved in (or will be in the future) planning, implementing, maintaining, supervising or assessing information security, as part of an ISO/IEC 27001 ISMS or a standalone system.

Prerequisite

Attendees should have a basic knowledge of business processes and technology concepts. No specialized technical knowledge is assumed.

Duration

This is **a Two-day Information Security Risk Management course**. The course starts at **09:30** and runs until **16:30**.

Alternate timings can be arranged upon request. The course can be held on a **date that suits you.**

Location

Our **Information Security Risk Management course** will be **delivered Online Remotely using online training platforms**. It can also be run at **our training venue** near **Liverpool Street (London)** or any preferred location in the **UK or Europe.**

Information Security Risk Management Course Outline

Introduction

Information security and risk management

ISO/IEC 27005:2018 Structure and approach

Typical implementation approach (methodology and integration with ISO/IEC 27002)

IT Risk Identification

Identify potential threats and vulnerabilities to the organization's people, processes and technology to enable IT risk analysis.

Develop IT risk scenarios

Establish an IT risk register

IT Risk Assessment

Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.

Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.

Communicate the results of risk assessments to senior management and appropriate stakeholders.

Risk Response and Mitigation

Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.

Development of risk action plans.

Design and implementation of mitigating controls.

Risk and Control Monitoring and Reporting

Define and establish key risk indicators (KRIs)

Monitor and analyze key risk indicators (KRIs)

Report on changes or trends related to the IT risk profile