# Cybersecurity Fundamentals

## *Course objectives*

The Cybersecurity Fundamentals Course provides dynamic learning experience where learners can explore foundational cybersecurity knowledge and kick-start career in this crucial area.

Cybersecurity is a growing and rapidly changing field, and it is crucial that the central concepts that frame and define this increasingly pervasive field are understood by professionals who are involved and concerned with the security implications of information technology (IT).

This course is designed to provide insight into the importance of cybersecurity, and covers five key areas of cybersecurity:

- cybersecurity concepts,
- security architecture principles,
- security of networks, systems, applications and data,
- incident response, and
- the security implications of the adoption of emerging technologies.

**The course includes:**

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

## *Audience*

This course is ideal for professionals wishing to enhance comprehensive understanding of Cybersecurity's key concepts and its impacts on business.

## *Prerequisite*

There are no formal prerequisites.

## *Duration*

This is **one-day Cybersecurity Fundamentals** Course. The course starts at **09:30** and runs until **16:30** on two consecutive days.

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

## *Location*

Our **Cybersecurity Fundamentals** 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.**

# Cybersecurity Fundamentals Course Outline

## Introduction to Cybersecurity

- Cybersecurity objectives
- Cybersecurity roles
- Differences between Information Security and Cybersecurity

## Cybersecurity Principles

- Confidentiality, integrity and availability
- Authentication and nonrepudiation

## Information Security (IS) within Lifecycle Management

- Lifecycle management landscape
- Security architecture processes
- Security architecture tools
- Intermediate lifecycle management concepts

## Risks and Vulnerabilities

- Basics of risk management
- Operational threat environments
- Classes of attacks

## Incident Response

- Incident categories
- Incident response
- Incident recovery

## Future Implications and Evolving Technologies

- New and emerging IT and IS technologies
- Mobile security issues, risks and vulnerabilities
- Cloud concepts around data and collaboration