



Strategic Leadership in Cybersecurity Risk and Compliance

www.masterpeaktraining.com

phone: +905302682631

Email: info@masterpeaktraining.com



Strategic Leadership in Cybersecurity Risk and Compliance

5 days training course

For detailed information on training course dates, please click the link:

[Strategic Leadership in Cybersecurity, Risk, and Compliance](#)

Introduction

This 5-day training is designed for senior professionals responsible for managing cybersecurity risks and ensuring regulatory compliance. The course provides practical strategies for aligning cybersecurity with business goals, handling cyber threats, and building strong compliance programs. Participants will learn how to lead cybersecurity initiatives, strengthen organizational resilience, and navigate complex regulations effectively.

Who Should Attend?

This program is ideal for:

- **Senior Cybersecurity Professionals** overseeing security frameworks.
- **CISOs, CTOs & IT Directors** responsible for cyber risk strategies.
- **Risk & Compliance Officers** managing regulatory adherence.
- **Executives & Decision-Makers** ensuring business resilience.

Course Objectives

By the end of the course, participants will:

- Develop leadership skills for managing cybersecurity risks.
- Align cybersecurity strategies with business priorities.
- Understand and implement key compliance regulations.
- Learn risk assessment and mitigation techniques.
- Build a security-aware culture within their organizations.
- Monitor, measure, and report on cybersecurity performance.

Course Outline:

Day 1: Leadership in Cybersecurity Strategy

- The role of cybersecurity in business success.
- Aligning cybersecurity initiatives with organizational goals.
- Building a security-conscious corporate culture.
- Leadership best practices in cybersecurity management.

Day 2: Cyber Risk Management & Threats

- Identifying and assessing cybersecurity risks.
- Managing threats such as ransomware and data breaches.
- Implementing risk mitigation and resilience strategies.
- Hands-on workshop: Building a cybersecurity risk plan.

Day 3: Compliance & Regulatory Standards

- Understanding global cybersecurity regulations (GDPR, HIPAA, etc.).
- Legal requirements for data protection and security.
- Developing a compliance framework for organizations.
- Practical session: Creating a cybersecurity compliance plan.

Day 4: Incident Response & Crisis Management

- Preparing an effective incident response plan.
- Managing communication during cybersecurity crises.
- Working with stakeholders and regulators in case of a breach.
- Simulation exercise: Responding to a cyberattack.

Day 5: Cybersecurity Monitoring & Reporting

- Establishing key performance indicators for cybersecurity.
- Using analytics to track risks and compliance.
- Reporting security risks to leadership and stakeholders.
- Final project: Developing a long-term cybersecurity strategy.



DOCUMENTATION

The **MTC team** has meticulously prepared **high-quality training materials** for distribution to all delegates.

CERTIFICATES

An **accredited Certificate of Completion** will be awarded to participants who successfully attend and complete the program.

SCHEDULE

Course sessions are scheduled as follows:

- **Morning Session:** 09:00 AM – 1:00 PM
- **Afternoon Session:** 01:00 PM – 05:00 PM

REGISTRATION & PAYMENT

To register, please complete the **registration form** available on the course page and submit it with your **preferred payment method**. Alternatively, you can contact us via **email or WhatsApp** for assistance.

TRAVEL & TRANSPORT

We ensure a **seamless travel experience** by providing **airport-hotel-airport** transfers for all participants.