Cybersecurity & IT Governance

www.masterpeaktraining.com
phone: +905302682631
Email:info@masterpeaktraining.com

Cybersecurity & IT Governance

5 days training course

For detailed information on training course dates, please click the link: Cybersecurity & IT Governance.

Target Audience:

This course is designed for senior executives, IT managers, cybersecurity professionals, risk managers, compliance officers, and anyone responsible for protecting information systems and ensuring robust IT governance. It is also ideal for those seeking to strengthen their organization’s cybersecurity strategy, governance framework, and compliance with industry regulations.

Introduction:

Cybersecurity & IT Governance focuses on the critical intersection of securing information technology systems and ensuring proper governance. As cyber threats evolve, organizations must integrate robust cybersecurity measures with effective governance frameworks to protect assets, comply with regulations, and mitigate risks. This course provides a deep dive into the principles of cybersecurity, risk management, IT governance models, and frameworks such as COBIT and ISO/IEC 27001. Participants will learn how to assess vulnerabilities, implement security strategies, and ensure that cybersecurity practices align with overall business goals, regulatory requirements, and industry standards.

Training Objectives:

- Understand the core principles of cybersecurity and IT governance.
- Learn how to design and implement a cybersecurity strategy aligned with business objectives.
- Gain knowledge of industry-leading IT governance frameworks and standards (COBIT, ISO/IEC 27001).
- Identify and assess cybersecurity risks and vulnerabilities.
- Explore methods for securing information systems, including data protection, threat mitigation, and incident response.
- Learn how to ensure compliance with legal, regulatory, and ethical standards in cybersecurity.
-
- Develop the skills to manage and monitor cybersecurity policies, frameworks, and controls within an organization.
- Understand how to measure and report cybersecurity performance to key stakeholders.

Course Outline:

Day 1: Introduction to Cybersecurity and IT Governance

- Understanding cybersecurity and its importance in the digital age
- Overview of IT governance and its role in organizational success
- Key concepts in risk management, compliance, and governance
- Introduction to industry frameworks: COBIT, ISO/IEC 27001, NIST
- The role of leadership in cybersecurity and IT governance
- Practical exercise: Assessing your organization's current cybersecurity posture

Day 2: Cybersecurity Threats and Risk Management

- Types of cybersecurity threats: Malware, ransomware, phishing, DDoS, etc.
- Risk management techniques for cybersecurity
- Identifying vulnerabilities and threat modeling
- Strategies for assessing and mitigating risks
- Best practices for network security, endpoint protection, and data protection
- Practical exercise: Conducting a risk assessment of IT assets
- Case study: Analyzing a recent cybersecurity breach and lessons learned

Day 3: IT Governance Frameworks and Compliance

- Deep dive into IT governance frameworks: COBIT, ISO/IEC 27001, NIST
- Understanding governance structures: Roles, responsibilities, and reporting
- Compliance and regulatory requirements: GDPR, HIPAA, CCPA, SOX
- Implementing IT governance policies and controls
- Auditing and monitoring for compliance
- Practical exercise: Designing an IT governance model for your organization

- Case study: Implementing ISO/IEC 27001 in a global enterprise

Day 4: Implementing and Managing Cybersecurity Controls

- Key cybersecurity controls: Firewalls, encryption, multi-factor authentication, etc.
- Data protection strategies: Encryption, backup, and disaster recovery
- Network security: Firewalls, IDS/IPS, VPNs
- Incident response and disaster recovery planning
- The importance of cybersecurity culture and training within organizations
- Practical exercise: Developing a cybersecurity incident response plan

- Case study: A day in the life of a cybersecurity operations center (SOC)

Day 5: Measuring Cybersecurity Performance and Reporting

- Key Performance Indicators (KPIs) for cybersecurity success
- Continuous monitoring and reporting tools
- Communicating cybersecurity risks to executives and stakeholders
- Conducting audits and assessments to ensure effectiveness of cybersecurity strategies
- Responding to security incidents and post-incident reviews
- Creating a cybersecurity roadmap and improvement plan
- Final assessment: Building an IT governance and cybersecurity strategy for your organization

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.