London TDM

Security Management and Risk Protection Training Courses

Course Venue: Malaysia - Kuala Lumpur

Course Date: From 18 January 2026 To 22 January 2026

Course Place: Royale Chullan Hotel

Course Fees: 6,000 USD

Introduction

The "Information Security Governance and Strategy" course is designed to equip professionals with the knowledge and skills required to establish and maintain robust information security governance and strategy frameworks. Participants will explore the intersection of business objectives and security needs, ensuring effective protection of information assets while supporting organizational goals. This course covers best practices, regulatory compliance, and strategic planning necessary for leading an organization's information security efforts.

- Understand the fundamentals of information security governance and its role in organizational success.
- Develop skills to create and implement a comprehensive information security strategy.
- Learn how to align security initiatives with business objectives and regulatory requirements.
- Gain insights into risk management and incident response planning.
- Cultivate leadership and communication skills for promoting security awareness and culture.

Course Outlines

Day 1: Foundations of Information Security Governance

- Introduction to information security governance and its importance.
- Key components and principles of effective governance.
- Roles and responsibilities in security governance.
- Understanding regulatory and compliance landscapes.
- Designing a governance framework aligning with business objectives.

Day 2: Information Security Strategy Development

- Strategic planning for information security.
- Developing policies and standards to support security strategy.
- Integrating security into organizational culture and processes.
- Identifying and prioritizing security initiatives.
- Measuring and evaluating the effectiveness of security strategies.

Day 3: Risk Management and Assessment

- Overview of risk management processes and methodologies.
- Conducting a risk assessment: tools and techniques.
- Risk mitigation strategies and planning.
- Implementing continuous risk monitoring and reporting.
- Incident response and management strategies.

Day 4: Regulatory Compliance and Legal Considerations

- Understanding key regulations affecting information security.
- Compliance frameworks and how to implement them.
- Navigating legal issues in information security.
- Establishing audit and assessment protocols.
- Case studies on compliance management.

Day 5: Leadership and Communication in Information Security

- The role of leadership in promoting security culture.
- Effective communication strategies for security professionals.
- Stakeholder engagement and reporting.
- Training and awareness programs for staff and management.
- Building and leading a successful security team.