MERCURY

Data Security Management

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Data Security Management

Introduction:

The paramount significance of data security management in contemporary business operations cannot be overstated. In today's interconnected digital landscape, where information serves as the lifeblood of organizations, safeguarding sensitive data against a myriad of potential threats is imperative for sustained success and resilience. As technology advances rapidly, so do the complexities and vulnerabilities inherent in data management systems.

In recognition of these challenges, this comprehensive five-day training program has to equip participants with the knowledge, skills, and strategies to navigate the intricate domain of data security management effectively. Throughout this intensive course, participants will delve into various critical topics ranging from risk assessment and mitigation techniques to regulatory compliance frameworks and emerging trends in cybersecurity.

This program aims to empower participants to proactively identify, assess, and address potential vulnerabilities within their organizations' data infrastructure by fostering a deep understanding of the underlying principles and best practices governing data security. Through interactive lectures, practical case studies, and hands-on exercises, participants will gain invaluable insights into designing robust data protection strategies tailored to their industries' unique needs and challenges.

With an emphasis on proactive risk management and continuous improvement, this training program endeavors to cultivate a culture of vigilance and accountability, wherein data security becomes ingrained within the fabric of organizational operations. As stewards of sensitive information, participants will emerge from this course equipped with the tools and techniques necessary to safeguard their organizations' most valuable assets in an ever-evolving threat landscape.

Targeted Groups:

- IT Security Professionals.
- Data Protection Officers.
- Network Administrators.
- Compliance Officers.
- System Administrators.
- Database Administrators.
- Risk Management Professionals.
- Chief Information Security Officers CISOs.
- Information Technology Managers.
- Cybersecurity Consultants.
- Business Continuity Planners.
- Legal and Regulatory Affairs Specialists.
- Human Resources Managers.
- Internal Auditors.
- Operational Risk Managers.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

Course Objectives:

At the end of this course, the participants will be able to:

- Understand the fundamentals of data security management.
- Implement effective data protection strategies.
- Develop and enforce data security policies.
- Identify and classify sensitive data.
- Apply encryption and access control measures.
- Monitor data activities and detect potential threats.
- Respond to data security incidents promptly.
- Ensure compliance with legal and regulatory standards.
- Conduct regular security assessments and audits.
- Foster a culture of data security awareness within the organization.
- Develop incident response and disaster recovery plans.
- Manage data breaches and minimize damage.
- Utilize advanced security technologies and tools.
- Implement secure data storage and transfer methods.
- Assess and manage third-party risks.
- Understand the latest cybersecurity threats and trends.
- Train employees on data security best practices.
- Evaluate and improve existing security infrastructure.
- Establish a data governance framework.
- Promote collaboration between departments for data security.
- Maintain an up-to-date knowledge base on data security.

Targeted Competencies:

- Data Protection Techniques.
- Risk Assessment and Mitigation.
- Security Policy Development.
- Data Classification and Handling.
- Encryption Standards and Practices.
- Access Control Implementation.
- Threat Detection and Monitoring.
- Incident Response Planning.
- Regulatory Compliance Understanding.
- Security Auditing Skills.
- Cybersecurity Awareness.
- Disaster Recovery Planning.
- Secure Data Storage Solutions.
- Data Breach Management.
- Use of Security Technologies.
- Third-Party Risk Management.
- Emerge Threat Analysis.
- Employee Security Training.
- Security Infrastructure Evaluation.
- Data Governance Principles.
- Cross-Departmental Collaboration.
- Know Current Security Trends.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Course Content:

Unit 1: Fundamentals of Data Security Management:

- Intro to data security concepts.
- Importance of data protection.
- Key components of data security management.
- Overview of cybersecurity threats.
- Data lifecycle and its security implications.
- Roles and responsibilities in data security.
- Understand confidentiality, integrity, and availability.
- Basic principles of information security.

Unit 2: Risk Assessment and Management:

- Identify potential security risks.
- Conduct risk assessments.
- Evaluate risk impact and likelihood.
- Develop risk mitigation strategies.
- Implement risk management frameworks.
- Continuous risk monitoring.
- Use risk assessment tools.
- Report and document risk assessments.

Unit 3: Data Protection Mechanisms:

- Data encryption techniques.
- Access control models and methods.
- Implement multi-factor authentication.
- Secure data storage solutions.
- Data masking and obfuscation.
- Network security measures.
- Endpoint security practices.
- Protect data in transit.

Unit 4: Compliance and Regulatory Standards:

- Overview of significant data protection regulations.
- Understand GDPR requirements.
- HIPAA compliance guidelines.
- PCI DSS standards for payment data.
- ISO/IEC 27001 framework.
- Develop compliance policies.
- Conduct compliance audits.
- Report and manage compliance issues.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Unit 5: Incident Response and Recovery:

- Develop an incident response plan.
- Identify and report security incidents.
- Containment and eradication strategies.
- Recovery and restoration procedures.
- Post-incident analysis and reporting.
- Build a disaster recovery plan.
- Regularly testing response and recovery plans.
- Learn from past incidents to improve security.