MERCURY

Data Quality Management & Digital Security Evaluation

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Data Quality Management & Digital Security Evaluation

Introduction

This Data Quality Management & Digital Security Evaluation course provides a comprehensive framework for ensuring reliable data and resilient digital environments in modern organizations. It focuses on integrating data quality governance with advanced cybersecurity evaluation practices to support informed decision-making. Participants explore how to assess, test, recommend, coordinate, monitor, and maintain digital security policies, procedures, and systems effectively. The course also develops the ability to verify enterprise systems and applications and to align network design with security best practices. It emphasises deploying secure networks, servers, and endpoint protection solutions across complex infrastructures. Professionals will strengthen data integrity, reduce cyber risk, and support secure digital transformation initiatives.

Targeted Groups

This Data Quality Management & Digital Security Evaluation training targets professionals seeking knowledge and skills:

- Data quality managers and data governance specialists.
- Cybersecurity and information security professionals.
- IT auditors and risk management officers.
- Network and system administrators.
- Digital transformation and compliance managers.
- Professionals responsible for enterprise data protection.
- Technology consultants and IT project leaders.
- Professionals supporting secure infrastructure operations.

Course Objectives

Participants will achieve the following objectives by completing the Data Quality Management & Digital Security Evaluation course:

- Understand principles of enterprise data quality management.
- Define data governance and data integrity standards.
- Evaluate digital security policies and control frameworks.
- Test security procedures using structured assessment methods.
- Recommend improvements to cybersecurity architecture.
- Coordinate security operations across IT environments.
- Monitor compliance with data protection requirements.
- Maintain secure systems and hardened infrastructures.
- Verify applications and enterprise system configurations.
- Design secure network architectures for organizations.
- Deploy servers with integrated security controls.
- Implement endpoint protection and monitoring solutions.
- Strengthen risk-based security decision-making.
- Support continuous improvement in data and security management.

Targeted Competencies

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Participants will gain the following competencies during the Data Quality Management & Digital Security Evaluation program:

- Managing enterprise data quality frameworks.
- Applying data validation and cleansing techniques.
- Conducting digital security risk assessments.
- Evaluating cybersecurity policies and procedures.
- Monitoring security controls and compliance status.
- Verifying systems and application security posture.
- Designing secure network infrastructures.
- Deploying hardened servers and endpoint security.
- Coordinating cross-functional security activities.
- Supporting continuous security improvement initiatives.

Studying Scenarios

In this Data Quality Management & Digital Security Evaluation training, participants develop skills through the following scenarios:

- Assessing data quality gaps in enterprise databases.
- Reviewing digital security policy effectiveness.
- Testing incident response readiness in organizations.
- Verifying application security configurations.
- Designing a secure corporate network model.
- Deploying endpoint protection across distributed systems.
- Monitoring compliance with data protection standards.
- Recommending improvements to security architecture.

Course Content

Unit 1: Foundations of Data Quality Management and Governance

- Introduction to data quality management principles and business value.
- Understanding dimensions of data quality in enterprise environments.
- Establishing data governance frameworks and accountability models.
- Defining data standards, ownership, and stewardship roles.
- Implementing data profiling and data quality assessment methods.
- Applying data cleansing, normalization, and validation techniques.
- Monitoring data accuracy, completeness, and consistency metrics.
- Aligning data quality initiatives with digital transformation goals.

Unit 2: Digital Security Policies and Risk Evaluation

- Overview of modern cybersecurity frameworks and control models.
- Structuring effective digital security policies and procedures.
- Performing cyber risk assessment and threat modeling.
- Evaluating security controls across IT environments.
- Testing policy compliance using audit and review techniques.
- Coordinating security governance with enterprise risk management.
- Monitoring regulatory compliance and data protection requirements.
- Recommending improvements based on security maturity assessments.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Unit 3: Systems and Applications Verification Techniques

- Fundamentals of secure system architecture and hardening.
- Verifying operating systems against security baselines.
- Assessing application security and configuration management.
- Performing vulnerability assessment and security testing.
- Reviewing identity and access management controls.
- Validating logging, monitoring, and alerting mechanisms.
- Documenting verification results and remediation priorities.
- Supporting secure software and system lifecycle practices.

Unit 4: Secure Network Design and Infrastructure Protection

- Principles of secure network architecture design.
- Segmenting networks to reduce cyber risk exposure.
- Designing secure routing, switching, and firewall strategies.
- Implementing network access control and zero-trust concepts.
- Protecting data in transit using encryption protocols.
- Evaluating network monitoring and intrusion detection systems.
- Planning resilient and scalable secure network environments.
- Aligning network design with enterprise security strategy.

Unit 5: Deployment of Servers and Endpoint Security Systems

- Preparing secure server deployment environments.
- Hardening Windows and Linux servers using best practices.
- Implementing endpoint security and EDR solutions.
- Managing patching and vulnerability remediation processes.
- Monitoring endpoint threats and suspicious activities.
- Coordinating incident response with security operations teams.
- Maintaining continuous security monitoring dashboards.
- Supporting lifecycle management of security controls.

Final Insights & Key Takeaways

Effective data quality management combined with strong digital security evaluation enables organizations to build trusted, resilient, and compliant digital ecosystems. Professionals who master these integrated practices can significantly reduce risk while enhancing data reliability and operational security.