MERCURY

Implementing and Auditing CIS Controls

1 – 5 August 2027
Cairo (Egypt)



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

MERCURY

Implementing and Auditing CIS Controls

Ref: 121333_1028184 **Date:** 1 – 5 August 2027 **Location:** Cairo (Egypt) **Fees:** 4000 Euro

Introduction

The Implementing and Auditing CIS Controls course provides professionals with a structured approach to securing IT environments using CIS Center for Internet Security best practices. Participants will learn to implement critical security controls, assess system vulnerabilities, and audit network compliance. The course emphasizes practical techniques for threat detection, risk mitigation, and continuous monitoring. It covers auditing strategies to ensure organizational adherence to security frameworks. Participants will gain skills to align security measures with industry standards and regulatory requirements. This course equips professionals to strengthen cybersecurity posture efficiently and effectively.

Targeted Groups

The Implementing and Auditing CIS Controls course targets professionals seeking specialized knowledge and skills:

- IT security managers.
- Cybersecurity analysts.
- Network administrators.
- Risk and compliance officers.
- Auditors focusing on IT systems.
- Incident response teams.
- Professionals aiming for CIS-focused certifications.

Course Objectives

Participants will achieve the following objectives by completing the Implementing and Auditing CIS Controls course:

- Understand the CIS Control framework and its applications.
- Implement critical security controls across IT environments.
- Identify and assess system vulnerabilities.
- Conduct effective audits and ensure compliance.
- Apply risk mitigation strategies.
- Monitor and report on cybersecurity effectiveness.
- Align organizational security with regulatory standards.
- Enhance incident response capabilities.
- Develop actionable security improvement plans.

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

MERCURY

Targeted Competencies

Participants will gain the following competencies during the program:

- Practical knowledge of CIS control implementation.
- Ability to conduct system audits and risk assessments.
- Expertise in threat detection and vulnerability analysis.
- Understanding of compliance and governance requirements.
- Skills in reporting security gaps and corrective actions.
- Competence in improving security operations.
- Application of audit results to organizational policies.
- Proficiency in continuous security monitoring and evaluation.

Studying Scenarios

In this training, participants will develop their skills through the analysis of the following scenarios:

- Auditing a corporate network for compliance with CIS Controls.
- Assessing risks in cloud and on-premises environments.
- Identifying gaps in access controls and authentication.
- Applying incident response protocols after detecting breaches.
- Developing security improvement plans based on audit findings.
- Evaluating the effectiveness of implemented security measures.

Course Content

Unit 1: Introduction to CIS Controls

- Overview of CIS Controls and best practices.
- Understanding control categories and priorities.
- Mapping CIS Controls to organizational security needs.
- Key principles of cybersecurity risk management.
- Regulatory compliance and standards alignment.
- Introduction to auditing CIS Controls.
- Security metrics and performance indicators.

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

Unit 2: Implementing Technical Controls

- Configuring secure network devices.
- Implementing endpoint protection and monitoring.
- Managing user access and authentication.
- Securing cloud resources and services.
- Patch management and system updates.
- Detecting and responding to malware threats.
- Data protection strategies and encryption.

Unit 3: Conducting Security Audits

- Planning and preparing for security audits.
- Reviewing system configurations and policies.
- Evaluating access controls and user permissions.
- Assessing logging and monitoring effectiveness.
- Identifying non-compliance and vulnerabilities.
- Generating audit reports and recommendations.
- Audit follow-up and corrective action verification.

Unit 4: Risk Assessment and Mitigation

- Identifying organizational security risks.
- Prioritizing vulnerabilities based on impact.
- Implementing risk mitigation strategies.
- Integrating risk assessment into IT processes.
- Continuous monitoring of risks and controls.
- Developing incident response plans.
- Case studies on effective risk management.

Unit 5: Advanced Auditing and Continuous Improvement

- Advanced auditing techniques and methodologies.
- Leveraging automation in audits and assessments.
- Benchmarking against industry best practices.
- Measuring the effectiveness of implemented controls.
- Enhancing compliance and governance programs.
- Continuous improvement of security posture.
- Preparing for certification and external audits.

Final Insights & Key Takeaways

Participants will leave equipped to implement, audit, and optimize CIS Controls effectively. The course enhances cybersecurity readiness and compliance in organizational IT environments.