**Training Program:
Cyber Security Advanced**

GGSC QMI
GERMAN GROUP QUALITY&MANAGEMENT INSTITUTE

1. Cybersecurity Advanced

Program Title:

Cybersecurity Advanced

To provide participants with in-depth knowledge of advanced cybersecurity techniques, focusing on defending against complex threats and applying best practices to secure enterprise systems.

Program Code: GGSC -QMI/ CSA/2/24
Duration: 32 hours – 8 sessions
Format: Combination of lectures, case studies, interactive discussions, and hands-on exercises

Resources: Advanced course materials, access to specialized cybersecurity tools and resources, certification exam

Program Objective: o equip participants with comprehensive expertise in advanced cybersecurity strategies, emphasizing the defense against sophisticated threats and the implementation of best practices to protect enterprise systems.

1. Cybersecurity Advanced

Program Content:

- **Module 1: Threat Modeling and Risk Analysis**

    - Developing threat models

    - Advanced risk analysis techniques

    - Prioritizing security measures based on risk assessment

- **Module 2: Advanced Network Security**

    - Securing enterprise networks

    - Implementing and managing intrusion detection and prevention systems (IDPS)

    - Network segmentation and zero-trust architecture

1. Cybersecurity Advanced

- **Module 3: Incident Response and Forensics**
  - Advanced incident response strategies
  - Digital forensics and evidence collection
  - Post-incident analysis and reporting

- **Module 4: Cloud Security**
  - Security challenges in cloud environments
  - Implementing cloud security best practices
  - Managing hybrid and multi-cloud security

1. Cybersecurity Advanced

- **Module 5: Advanced Endpoint Protection**

  - Endpoint detection and response (EDR)

  - Implementing advanced malware protection techniques

  - Securing mobile and IoT devices

- **Module 6: Secure Application Development**

  - Integrating security into the software development lifecycle (SDLC)

  - Secure coding practices and code reviews

  - Addressing vulnerabilities in web and mobile applications

1. Cybersecurity Advanced

- **Module 7: Regulatory Compliance and Governance**

  - Navigating global cybersecurity regulations

  - Developing and implementing compliance frameworks

  - Managing audits and certifications

- **Module 8: Future Trends in Cybersecurity**

  - Emerging threats and technologies

  - The role of AI and machine learning in cybersecurity

  - Preparing for the next generation of cybersecurity challenges

2. ISACA Certified Information Security Manager® (CISM®)

ISACA®

How does it benefit you?

70%
EXPERIENCED ON-THE-JOB IMPROVEMENT

42%
RECEIVED A PAY BOOST

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17024
PERSONNEL CERTIFICATION BODY

Validate your proficiencies for handling the challenges and responsibilities of a modern IT security manager with a CISM, which focuses on these domains:

Information Security Governance >

Information Security Risk Management >

Information Security Program >
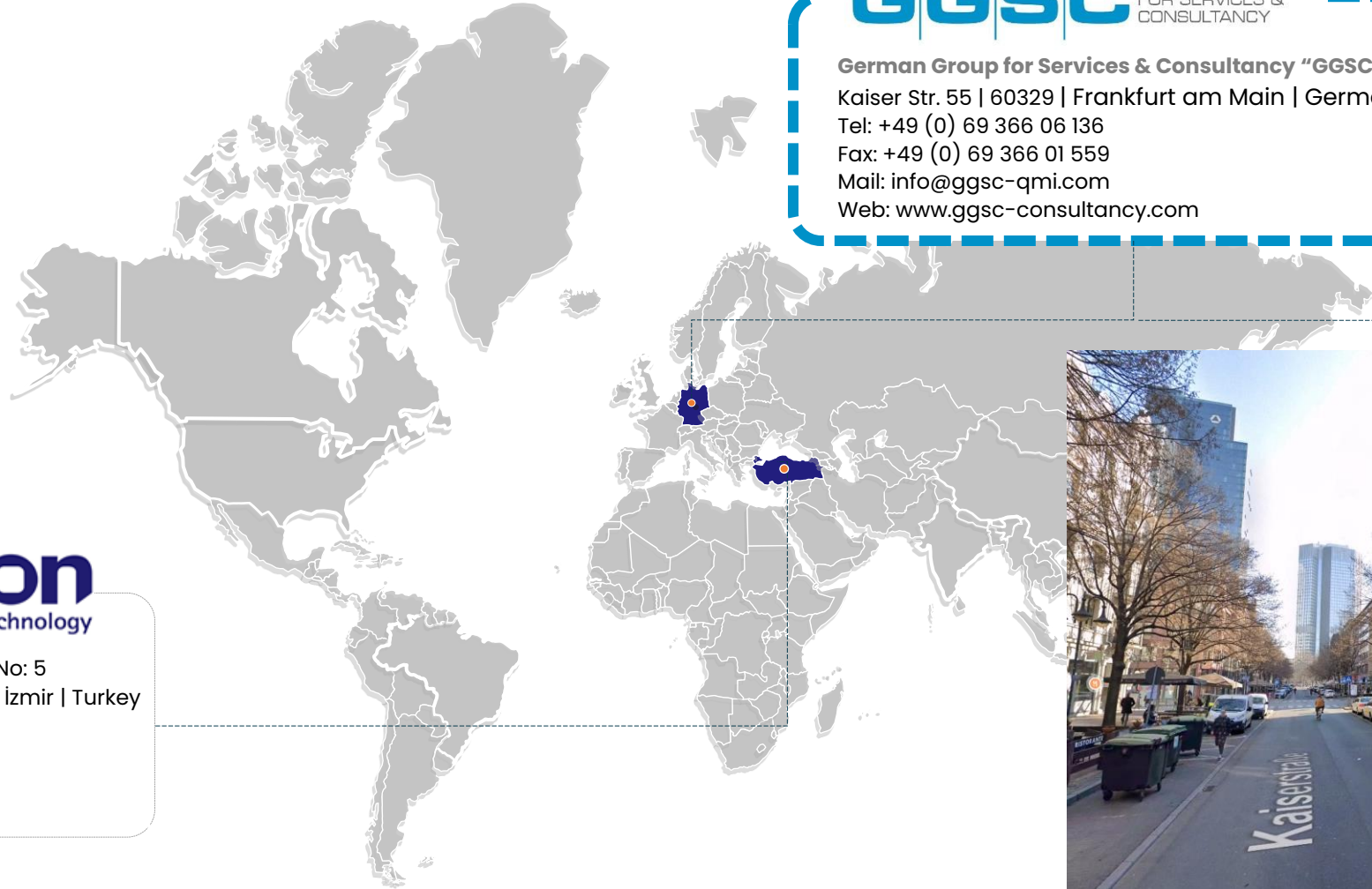
Incident Management >

VIEW ALL STUDY MATERIALS

VIEW EXAM CANDIDATE GUIDE

2. ISACA Certified Information Security Manager® (CISM®)

German Group for Services & Consultancy "GGSC-QMI"

Kaiser Str. 55 | 60329 | Frankfurt am Main | Germany
Tel: +49 (0) 69 366 06 136
Fax: +49 (0) 69 366 01 559
Mail: info@ggsc-qmi.com
Web: www.ggsc-consultancy.com

75. Yıl Mahallesi, 5310. Sokak, No: 5
Yunusemre/Manisa | Greater İzmir | Turkey
Tel: +90 850 804 05 85
cg@getucon.de