GLOBAL EXPERTS INSTITUTE FOR TRAINING.
ISO 9001-2008 TRAINING PROVISION CERTIFIED

Security Incident Management & Investigation

Schedule Dates:

Start Date	End Date	Place
20-Jul-2025	24-Jul-2025	The H Hotel Dubai

Program Introduction:

In an era of increasing cyber threats, security breaches, and workplace incidents, it is essential for organizations to effectively manage and investigate security incidents. The "Security Incident Management & Investigation" course equips professionals with the tools, strategies, and methodologies necessary to handle security incidents, mitigate risks, and conduct thorough investigations. Participants will learn how to assess, respond to, and recover from security breaches while adhering to legal, ethical, and organizational standards.

Program Objectives:

- ✓ Understand the principles and framework of security incident management.
- ✓ Learn how to classify and prioritize security incidents based on their severity and impact.
- ✓ Master the steps in responding to and managing security incidents effectively.
- ✓ Develop the skills to conduct comprehensive security investigations.
- ✓ Gain an understanding of legal and regulatory requirements in incident handling and investigations.
- ✓ Learn techniques for gathering, preserving, and analyzing evidence during investigations.
- ✓ Build communication and reporting strategies to inform stakeholders during and after an incident.
- ✓ Implement corrective and preventive actions based on incident findings to prevent future breaches.

Who should attend?

- Security managers and officers
- Incident response team members
- IT security professionals and network administrators
- Risk management and compliance professionals
- Investigators and forensic experts
- HR professionals involved in handling workplace security incidents
- Operations and facilities managers
- Any professional involved in ensuring workplace safety and security

Program Outlines

Day One

- Introduction to Security Incident Management and Investigation
- Understanding Security Incidents: Types, Causes, and Consequences
- Incident Response Framework and Methodology
- The Incident Response Lifecycle: Preparation, Detection, Containment, Eradication, Recovery
- Classifying and Prioritizing Security Incidents

Day Two

- Legal and Ethical Considerations in Security Incident Management
- Incident Detection: Tools, Techniques, and Indicators
- Building an Incident Response Team (IRT) and Roles
- Creating an Incident Response Plan (IRP)
- Incident Containment: Immediate Actions and Short-Term Responses

Day Three

- Root Cause Analysis and Impact Assessment
- Evidence Collection: Best Practices for Preserving Chain of Custody
- Incident Investigation Techniques: Interviews, Forensics, and Analysis
- Analyzing Digital Evidence: Logs, Files, and Network Traffic
- Understanding Cybersecurity Incidents: Data Breaches, Malware, Phishing

Day Four

- Physical Security Incidents: Theft, Vandalism, and Workplace Violence
- Communication Strategies during a Security Incident: Internal and External
- Post-Incident Analysis and Reporting
- Developing Corrective and Preventive Actions (CAPA)
- Managing Crisis Communications and Public Relations

Day Five

- Regulatory Compliance: GDPR, HIPAA, and Other Security Standards
- Incident Documentation and Reporting to Authorities
- Lessons Learned: Improving Security Posture Post-Incident
- Conducting a Security Incident Tabletop Exercise
- Case Studies: Real-World Examples of Security Incident Management and Investigation

Training Methodology:

- Slide presentations
- Interactive discussion
- Simulations and Gamification
- Online Video material

Cost Quotation in Kuwaiti Dinars

The total cost includes:

- Instructor(s) expenses
- Training materials
- Certification

Total Cost: 1600 KD per Participant

(One Thousand Six Hundred Kuwaiti Dinar)