

Certified Information Security Awareness Manager (CISAM)

Duration: 16 Hours

Course Overview:

This TOC provides an organized structure for a Certified Information Security Awareness Manager (CISAM) course, including an overview of the program, its objectives, the importance of information security awareness, key concepts covered, and details about the certification. Additionally, it outlines the target audience, benefits for different roles, and any prerequisites for enrollment. **Learning Objectives:**

By the end of this module, participants will be able to:

Module 1: Fundamentals of Information Security Awareness

[Understanding Information Security](#)

[Threats and Vulnerabilities](#)

[Importance of Confidentiality, Integrity, and Availability \(CIA\)](#)

Module 2: Social Engineering Awareness

[Introduction to Social Engineering](#)

[Common Social Engineering Techniques](#)

[Preventing Social Engineering Attacks](#)

Module 3: Cybersecurity Best Practices for End-Users

[Secure Password Practices](#)

[Email Security](#)

[Safe Internet Browsing](#)

Module 4: Creating a Culture of Security Awareness

[Role of Leadership in Security Culture](#)

[Designing Effective Training Programs](#)

[Measuring and Improving Security Awareness](#)

Module 5: Incident Response and Reporting

[Recognizing Security Incidents](#)

[Reporting Security Incidents](#)

[Incident Response Procedures](#)

Module 6: Mobile Device Security Awareness

[Securing Mobile Devices](#)

[Mobile App Security](#)

[BYOD \(Bring Your Own Device\) Policies](#)

Module 7: Insider Threat Awareness

[Identifying Insider Threats](#)

[Preventing Insider Threats](#)

[Reporting Suspicious Behavior](#)

Module 8: CISAM Certification Preparation

[CISAM Exam Format and Structure](#)

[Sample Questions and Practice Tests](#)

[Continuing Education Requirements](#)