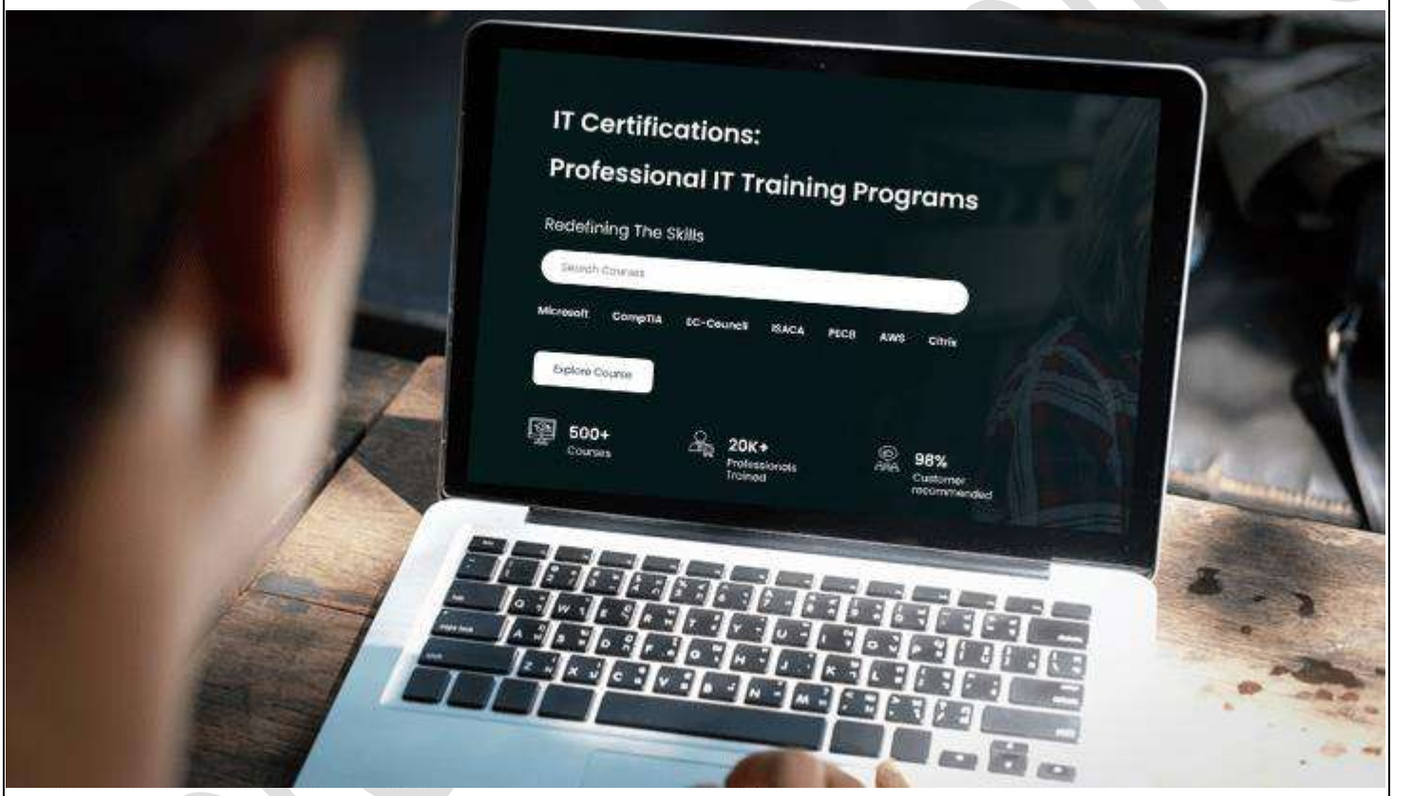
MICROTEK LEARNING | Redefining The Skills



CISM – CERTIFIED INFORMATION SECURITY MANAGER TRAINING

Duration: 3 Days

Course Description

CISM - Certified Information Security Manager Training is designed to help people develop a good understanding of the relationship between information security programs and broader organizational objectives.

It also educates and guides the candidates to attain the CISM qualification.

This certification is issued by ISACA to validate and analyze the candidate's expertise regarding the relationship between information security programs and broader business targets.

CISM certification is for experienced security management professionals who have decent work experience managing and developing information security programs.

This certification also validates that the professional has extensive knowledge of managing, developing, and implementing an information security program for a business organization.

CISM - Certified Information Security Manager Training covers all the four domains of the CISM certification exam and helps IT security professionals gain more knowledge, enhance their skills, and increase their practical experience.

Who should attend this course?

This training is intended for professionals who have expert-level experience as an information security manager.

However, the target audience for this course are IT managers, IT Auditors security policy writers, security device administrators, information security officers, security engineers, privacy officers, and IT consultants.

What you will learn

- Information Security Program Management & Development.
- Information Risk Management & Governance of Information Security.
- Information Risk Compliance & Information Security Incident Management.

Curriculum

Module 1: Information Security Governance

In this module, you will learn how to:

- Establish and maintain an information security strategy and align the strategy with corporate governance
- Identify internal and external influences to the organization
- Define roles and responsibilities
- Establish, monitor, evaluate, and report metrics

Module 2: Information Risk Management and Compliance

In this module, you will learn how to:

- Establish a process for information asset classification and ownership
- Identify legal, regulatory, organizational, and other applicable requirements
- Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted periodically

- Determine appropriate risk treatment options
- Evaluate information security controls
- Identify the gap between current and desired risk levels
- Integrate information risk management into business and IT processes
- Monitor existing risk
- Report noncompliance and other changes in information risk

Module 3: Information Security Program Development and Management

In this module, you will learn how to:

- Establish and maintain the information security program
- Identify, acquire, manage, and define requirements for internal and external resources
- Establish and maintain information security architectures
- Establish, communicate, and maintain organizational information security standards, procedures, and guidelines
- Establish and maintain a program for information security awareness and training
- Integrate information security requirements into organizational processes, as well as into contracts and activities of third parties
- Establish, monitor, and periodically report program management and operational metrics

Module 4: Information Security Incident Management

In this module, you will learn how to:

- Establish and maintain an organizational definition and severity hierarchy for information security incidents
- Establish and maintain an incident response plan
- Develop and implement processes to ensure timely identification of information security incidents
- Establish and maintain processes to investigate and document information security incidents
- Establish and maintain incident escalation and notification processes
- Organize, train, and equip teams to effectively respond to information security incidents
- Test and review the incident response plan periodically
- Establish and maintain communication plans and processes
- Conduct post-incident reviews
- Establish and maintain integration among the incident response plan, disaster recovery plan, and business continuity plan

For any query Contact Us – Microtek Learning