Certified Information Security Manager (CISM) Exam Preparation

Modality: Virtual Classroom

Duration: 4 Days

About this course:

This training course of information security is a course that is specially produced for information security experts who are preparing to give the exam of CISM. It is getting harder to make sure about big business information along these lines, this training of information security course of ISACA encourages you to give nitty gritty inclusion on the four CISM areas. These areas incorporate security incident management; risk management and compliance; security governance, and security program management and development.

The normal compensation for a Certified Information Security Manager is $116,155 every year.

Course Objective:

- Make a general data security structure and keep up its activities and work.
- Establish, evaluate, monitor, and report metrics
- Plan the measures to take for procedure execution alongside making an information security system.
- Respond to and recover from harming happenings for information security.
- Examination preparation and completion of CISM (Certified Information Security Manager)
- Obtain management commitment
- Control and Handle a wide range of threats to information security.
- Develop a business case
- Identify external and internal influences on the organization
- Ensure that vulnerability assessment, risk assessments, and risk analyses are conducted periodically
- Set up a procedure for information asset ownership and classification
- Explain roles and responsibilities
- Identify organizational, regulatory, legal, and other applicable requirements
- Determine appropriate options for risk treatment
- Incorporate information risk management into IT and business processes
- Assess the controls of information security
- Explain noncompliance and other changes in information risk
- Recognize the gap between desired and current risk levels
- Monitor existing risk
- Maintain and establish the program of information security
- Confirm alignment between the program of information security and other functions of the business.
- Identify, manage, acquire, and explain needs for external and internal resources
- Setup and maintain the architectures of information security
- Communicate, establish, and maintain organizational information security procedures, standards, and guidelines

- Setup and maintain a program for information security training and awareness
- Review and test the plan of incident response periodically
- Maintain and Establish notification processes and incident escalation
- Train, organize, and equip groups to effectively react to the incidents of information security.
- Conduct post-incident reviews
- Maintain and establish communication processes and plans.

Audience:

The course planned for:

- Individuals related to IT work like IT managers, consultants or auditors.
- Experts with the responsibilities of information security like policy writers, security device administrators, information security managers, officers, and security engineers.
- Network administrators

Prerequisites:

The information security practice of around Five years is a must for all device administrators and security engineers, professionals, consultants, IT auditors, privacy officers, managers, information security officers, and security policy writers.

Suggested prerequisites courses:

CEH -- Certified Ethical Hacking

CISSP -- Certified Information Systems Security Professional

Course Outline: