Hands-On

CISM - Certified Information Security Manager Prep

Course Description

While information has become more easily accessible and readily available, the associated risks and security threats have not only increased in number, but also complexity. As a result, the importance of ensuring that an enterprise's information is protected has also increased. It is now more important than ever for executives to ensure that their IT security managers have the expertise needed to reduce risk and protect the enterprise.

Designed specifically for information security professionals who are preparing to sit for the CISM exam, the course focuses on the four content areas of the Certified Information Security Manager (CISM) job practice

-Information security governance

-Risk management and compliance

-Information security program development and management

-Information security incident management.

CISM Impacts Your Career and Your Organization

The demand for skilled information security management professionals is on the rise, and the CISM certification is the globally accepted standard of achievement in this area.

CISMs understand the business. They know how to manage and adapt technology to their enterprise and industry.

The CISM certification program was developed by ISACA for experienced information security management professionals who have experience developing and managing information security programs and who understand the programs relationship to the overall business goals. The CISM exam consists of 200 multiple-choice questions that cover the four CISM domains. The American National Standards Institute (ANSI) has accredited the CISM certification program under ISO/IEC 170242003, General Requirements for Bodies Operating Certification Systems of Persons.

Students Will Learn

- **Information Security Governance**
- **Information Risk Management and Compliance**
- **Information Security Program Development and Management**
- **Information Security Incident Management**
- **Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives**

- **Distinguishes you as having not only information security expertise, but also knowledge and experience in the development and management of an information security program**
- **Puts you in an elite peer network**
- **And more...**

Target Audience

Experienced information security managers and those who have information security management responsibilities, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Prerequisites

This course prepares students to pass the ISACA CISM certification exam.

In order to be awarded the CISM designation, students must meet the following requirements

Successfully pass the CISM exam.
Adhere to ISACA's Code of Professional Ethics.
Agree to comply with the Continuing Education Policy.
Work experience in the field of information security.
Submit an Application for CISM Certification.

Course Outline

Information Security Governance

Students will understand the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy, and be able to formulate a plan of action to implement this strategy.

- Establish and maintain an information security strategy and align the strategy with corporate governance
- Establish and maintain an information security governance framework
- Establish and maintain information security policies
- Develop a business case
- Identify internal and external influences to the organization
- Obtain management commitment
- Define roles and responsibilities
- Establish, monitor, evaluate and report metrics

Information Risk Management and Compliance
Students will be able to manage information security risks.

- 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

Information Security Program Development and Management
Students will be able to develop and manage an information security plan.

- Establish and maintain the information security program
- Ensure alignment between the information security program and other business functions
- 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, guidelines
- Establish and maintain a program for information security awareness and training
- Integrate information security requirements into organizational processes
- Integrate information security requirements into contracts and activities of third parties
- Establish, monitor and periodically report program management and operational metrics

Information Security Incident Management
Students will effectively manage information security within an enterprise and develop policies and procedures to respond to and recover from disruptive and destructive information security events.

- Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents
- Establish and maintain an incident response plan
- Develop and implement processes to ensure the 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

Delivery Method

Instructor-Led with Labs and exercises throughout.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring

their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

5 Days