Certified in Risk and Information Systems Control Boot Camp (CRISC)

Course Summary

Description

This CRISC training and certification boot camp provides the necessary skills for IT and business professionals seeking a reinforced management position. This immersion course brings the essential material to these professionals in the 5 job practice domains. These areas and statements were developed by the CRISC Task Force and represent a job practice analysis of the work performed in risk identification, assessment, evaluation, response, and monitoring and in the design, implementation, monitoring, and maintenance of information system controls. The domains are as follows:

- Domain 1: Risk Identification, Assessment, and Evaluation
- Domain 2: Risk Response
- Domain 3: Risk Monitoring
- Domain 4: Information Systems Control Design and Implementation
- Domain 5: IS Control Monitoring and Maintenance

We add in this program additional training of taking the theory of this certification and map it to a real-world examples.

CRISC is the only certification that prepares and enables IT professionals for the unique challenges of IT and enterprise risk management, and positions them to become strategic partners to the enterprise. Our CISM certification training program will teach you the necessary requirements to pass the CRISC exam via in-depth lectures, discussions, demos and much more.

The required courseware is:

- CRISC Review Manual by ISACA
- CRISC Review Questions, Answers & Explanations Manual by ISACA

The CRISC exam consists of 200 items taken over a 4-hour period. Candidate scores are reported as a scaled score. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. ISACA uses and reports scores on a common scale from 200 to 800.

A candidate must receive a score of 450 or higher to pass the exam. A score of 450 represents a minimum consistent standard of knowledge as established by ISACA's CRISC Certification Committee.

A candidate receiving a passing score may then apply for certification the following requirements are met including:

- Adhering to the ISACA Code of Professional Ethics
- Agreeing to comply with the CRISC Continuing Education Policy
- Risk management and information systems control experience

Certified in Risk and Information Systems Control Boot Camp (CRISC)

Course Summary (cont'd)

Topics

- Risk Identification, Assessment, and Evaluation
- Risk Response and Risk Monitoring
- Information Systems Control Design and Implementation
- Control Monitoring and Maintenance
- Review and Practice Test

Audience

This course is ideal for those looking for:

- A prestigious, lifelong symbol of knowledge and expertise as a risk professional.
- Increased value to your organization as it seeks to manage IT risk.
- A competitive advantage over peers when seeking job growth.
- Access to ISACA's global community of knowledge and the most up-to-date thinking on IT risk management.
- Achievement of a high professional standard through ISACA's requirements for continuing education and ethical conduct.

This course is designed for the following job roles:

- IT professionals
- Risk professionals
- Control professionals
- Business analysts
- Project managers
- Compliance professionals

Prerequisites

To register for the exam, individuals must provide evidence of appropriate work experience in risk management and information system control as defined by the CRISC job practice.

Duration

Four days

Certified in Risk and Information Systems Control Boot Camp (CRISC)

Course Outline

I. Risk Identification, Assessment, and Evaluation
- A. Intro to Risk Management
- B. System Development Life Cycles
- C. Understanding the enterprise
- D. Legal, regulatory, and contractual requirements
- E. Working with stakeholders
- F. Asset management
- G. Information threats
- H. Vulnerability analysis
- I. Understanding impacts
- J. Validating risk appetite and tolerance

II. Risk Response and Risk Monitoring
- A. Develop and implement risk responses
- B. Evaluating risk response options
- C. Validation of efficiency, effectiveness, and economy
- D. Developing of the risk profile
- E. Developing of business cases
- F. Collect and validate data that measure key risk indicators (KRIs)
- G. Facilitating independent risk assessments and process reviews
- H. Identifying and reporting

III. Information Systems Control Design and Implementation
- A. Understanding of the business process objectives
- B. Design information systems controls
- C. Facilitate the identification of resource
- D. Ensuring implementation within time, budget and scope
- E. Provide progress reports
- F. Implementing information systems controls
- G. Identification of metrics and key performance indicators (KPIs)
- H. Assess and recommend tools

IV. Control Monitoring and Maintenance
- A. Plan, supervise, and conduct testing
- B. Review information systems policies, standards, and procedures
- C. Using CMMI to evaluate the current state of information systems processes
- D. Correcting information systems control deficiencies and maturity gaps
- E. Provide information systems control status

V. Review and Practice Test
- A. Understanding multiple-choice exams strategies
- B. Time management for exam
- C. Practice test and reviewing answer