1. Course Details:

Course Code : ISAC-006
Course Title : Certified Information Security Manager (CISM)
Course Duration : 5 Days

2. Course Overview:

- The Certified Information Security Manager (CISM) certification is a unique management-focused certification that has been earned by more than 20,000 professionals since its introduction in 2004. Unlike other security certifications, CISM is for the individual who manages, designs, oversees and assesses an enterprise's information security. The demand for skilled information security management professionals is on the rise. Earning a CISM designation will give you a competitive advantage. Many enterprises and government agencies increasingly recognize, require and expect there IS and IT professionals to hold this certification.

3. Learning Outcomes:

- Maintain an individual's competency by requiring the update of existing knowledge and skills in the areas of information systems auditing, management, accounting and business areas related to specific industries (e.g., finance, insurance, business law, etc.)
- Provide a means to differentiate between qualified CISMs and those who have not met the requirements for continuation of their certification
- Provide a mechanism for monitoring information systems audit, control and security professionals maintenance of their competency
- Aid top management in developing sound information systems audit, control and security functions by providing criteria for personnel selection and development
- Provide an environment in which security professionals can acquire, thoroughly and properly,the skills and knowledge expected of a world class information security manager
- To maximize your prospects at the CISM exam if you choose to sit it

4. Course Contents:

Domain 1 – Information Security Governance

- Knowledge Statements
- Introduction to Information Security Governance
- Effective Information Security Governance
- Governance and Third-Party Relationships
- Information Security Metrics
- Information Security Governance Metrics
- Information Security Strategy
- Information Security Strategy Development
- Strategy Resources and Constraints
- Other Frameworks
- Compliances
- Action Plans to Implement Strategy
- Governance of Enterprise IT

Domain 2 – Information Risk Management and Compliance

- Information Risk Management
- Task and Knowledge Statements
- Risk Management Overview
- Risk Assessment
- Information Asset Classification
- Assessment Management
- Information Resource Valuation
- Recovery Time Objectives
- Security Control Baselines
- Risk Monitoring
- Training and Awareness
- Information Risk Management Documentation

Domain 3 – Information Security Program Development and Management

- Task and Knowledge Statements
- Information Security Program Management Overview
- Information Security Program Objectives
- Information Security Program Concepts
- Information Security Program Technology Resources
- Information Security Program Development
- Information Security Program Framework
- Information Security Program Roadmap
- Enterprise Information Security Architecture (EISA)

- Security Program Management and Administration
- Security Program Services and Operational Activities
- Security Program Metrics and Monitoring
- Measuring Operational Performance
- Common Information Security Program Challenges

Domain 4 – Information Security Incident Management

- Task and Knowledge Statements
- Incident Management Overview
- Incident Management Procedures
- Incident Management Resources
- Incident Management Objectives
- Incident Management Metrics and Indicators
- Defining Incident Management Procedures
- Business Continuity and Disaster Recovery Procedures
- Post Incident Activities and Investigation
- ISACA Code of Professional Ethics
- Laws and Regulations
- Policy Versus Law Within an Organization
- Ethics and the Internet IAB
- Certified Information Security Manager
- Certification requirements
- CISM in the Workplace
- The CISM Priorities
- Understand How Questions Are Structured
- Preparing for the Examination
- Recommended Reading for the CISM Exam

5. Our Methodology:

- Make coaching and monitoring innovative and using modern
- Media training also using on the go training by using interactive means and focusing on
- The exercises, practical applications and real situations study.
- Live delivery method, instructor-led training.
- Experienced consultant, trainers, and professional.
- Qualified trainer with high-level experience

6. Attendance Reports:

- Send daily attendance reports to trainingdep
- Send full attendance report to training dep. by the end of thecourse
- Attend 100 % from the course days also providedaily
- Issue attendance certificate for participant who attend minimum 80% from the course duration

7. Pre/Post Reports:

- Pre- assessment before starting training.
- Post assessment after finish training
- Full report for the deferent between Pre-& Post assessment

8. Who Should Attend?

- Senior Executives, IT managers
- Information Security Professionals
- IT Software System
- Application Developers and IT Auditors