1. Course Details:

Course Code : ISCS-001
Course Title : CISSP® - Certified Information Systems Security Professional
Course Duration : 5 Days

2. Course Overview:

- Attend this official (ISC)2® CISSP certification course and get prepared to pass the exam and become a CISSP. You will gain the foundational knowledge to fully prepare for the exam, including a comprehensive understanding of the CISSP® CBK® 8 domains.

3. Learning Outcomes:

- Understand and apply fundamental concepts and methods related to the fields of information technology and security
- Align overall organizational operational goals with security function sand implementations
- Understand how to protect assets of the organization as they go through their lifecycle
- Understand the concepts, principles, structures and standards used to design, implement, monitor and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of confidentiality, integrity and availability
- Implement system security through the application of security design principles and application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures
- Understand the importance of cryptography and the security services it can provide into day's digital and information age
- Understand the impact of physical security elements on information system security and apply secure design principles to evaluate or recommend appropriate physical security protections
- Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function
- Identify standard terms for applying physical and logical access controls to environments related to their security practice

- Appraise various access control models to meet business security requirements
- Name primary methods for designing and validating test and audit strategies that support business requirements
- Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it; identify which security control(s) are appropriate for the development environment; and assess the effectiveness of software security.

4. Course Contents:

- Access Control - a collection of mechanisms that work together to create a security architecture to protect the assets of the information system
- Application Development Security
- Business Continuity and Disaster Recovery Planning – for the preservation and recovery of business operations in the event of outages
- Cryptography - the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- Information Security Governance and Risk Management
- Legal, Regulations, Investigations and Compliance
- Computer crime laws and regulations
- The measures and technologies used to investigate computer crime incidents
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security
- Network structures
- Transmission methods
- Transport formats
- Security measures used to provide availability, integrity, and confidentiality

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?

- SecurityConsultant
- SecurityManager
- ITDirector/Manager
- SecurityAuditor
- SecurityArchitect
- SecurityAnalyst
- Security SystemsEngineer
- Chief Information SecurityOfficer
- SecurityDirector
- NetworkArchitect