1. Course Details:

Course Code : ISAC-001
Course Title : CSX Fundamentals
Course Duration : 5 Days

2. Course Overview:

- The CSX fundamentals Certification is the globally recognized and much desired credential for the experienced and aspiring cyber security professionals as well as for any IT professional whose role gets affected by the increasing complicacies and possibilities of cyber threat.

- Cybersecurity Nexus CSX Cybersecurity Fundamentals Certificate from ISACA's Cybersecurity Nexus™ (CSX) is designed the help the professionals demonstrate their understanding of cybersecurity principles. ISACA certification adds globally required values to your profile helping you advance your career at better pace as well as to perform better in current role.

3. Learning Outcomes:

- Understanding basic principles, concepts and processes of cybersecurity
- Learning cybersecurity fundamental framework
- Understanding the role of a cybersecurity professional for safeguarding the business information
- Getting basic qualification to get advanced level CSX certifications

4. Course Contents:

Domain 1:

- Concepts of Cyber Security
- Cyber security principles to manage risks related to the use, storage, processing and transmission of data or information
- Risk Management Processes- steps & methods for risk assessment
- Security Management
- Cyber Security Roles

- Threat Actors
- Common Adversary Tactics and Advanced Procedures (TTPs)
- Cyber Security Controls
- Relevant Laws, Governance Requirements, Policies and Procedures

Domain 2:

- Principles of Cyber Security Architecture
- Network Design Processes including understanding of security objectives, trade-offs and operational objectives.
- Network Identity and Access Management
- Security System Design Tools, Techniques and Methods.
- Security Principles & Methods for Information Technology
- Network Security Architecture Concepts including components, principles, topology & protocols
- Malware Analysis Methodology and Concepts
- Intrusion detection techniques and methodologies to detecting host and network-based intrusions by applying various intrusion detection techniques
- Encryption Algorithms
- Cryptography
- Defense in Depth Principles
- Network Security Architecture Defense
- Encryption Methodologies
- Traffic flows process across the network (transmission & encapsulation)
- Dynamic Host Configuration Protocol, Directory Services & Network Protocols

Domain 3:

- Security Management of Networks, Systems, Applications and Data
- Vulnerability Assessment Tools and Capabilities
- Basics of System Administration and Network Operating System Hardening Techniques
- Penetration Testing
- Risk Associated with Virtualization
- Network Systems Management Modules, Methods, Tools and Principles
- Remote Access Technology & Unix Command Line
- System & Application Security Threats
- Life Cycle Management Principles including software usability and security
- Local Specific System Requirements regarding Safety, Performance and Reliability.
- Social Dynamics of Computer Attackers
- Secure Configuration Techniques
- Capabilities & Applications of Network Equipment

- Communication Principles, Concepts and Methods that Support Network Infrastructure
- Common Networking Protocols & Services
- Different Types of Network Communication
- Virtualization Technologies
- Virtual Machine Maintenance and Development
- Application Security & Risk Threat Assessment

Domain 4:

- Incident Response
- Incident Categories and Response
- Incident Response & Handling Methodologies
- Business Continuity/Disaster Recovery
- Processes for Seizing & Preserving Digital Evidence
- Security Event Correlating Tools
- Digital Forensics Data Types
- Processing Digital Forensics Data - Concepts & Practices
- Anti-Forensics Tactics, Techniques and Procedures (TTPS)
- Forensic Tool Configuration & Support Applications
- Methods of Network Traffic Analysis
- Identifying which System Files Contain Relevant Information

Domain 5:

- Security Implications & Adoption of Evolving Technology
- Emerging Technology & Associated Security Risks, Vulnerabilities & Issues
- Cloud Concepts for Data & Collaboration
- Risk Associated to Mobile Computing
- Risk factors for Moving Applications and Cloud Infrastructure
- Supply Chain Risk Management Processes & Practices
- Risk Management for Outsourcing

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?

- System administrators planning
- Graduate students interested to development career in the field of cybersecurity
- Individuals with 2-3 years of experience in cyber security domain