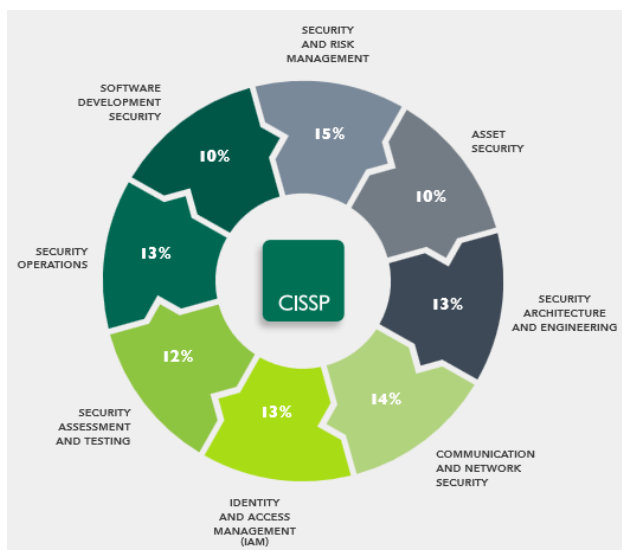




CISSP

Certified Information Systems Security Professional



مقدمه

مخاطبان دوره

- Chief Information Officer
- Chief Information Security Officer
- Director of Security
- IT Director/Manager
- Network Architect
- Security Analyst
- Security Architect
- Security Auditor
- Security Consultant
- Security Manager
- Security Systems Engineer

مدت زمان دوره

4 روز (32 ساعت)

این دوره یکی از معتبرترین دوره ها در زمینه امنیت اطلاعات IT می باشد در این دوره به شرکت کنندگان دانش معمول امنیت آموزش داده می شود . در این دوره شرکت کنندگان با مباحثی چون تدوین خط مشی امنیتی، فرآیندهای توسعه ایمن نرم افزار، آسیب پذیریهای شبکه، انواع حملات و اقدامات متقابل در قبال آنها، مفاهیم رمزنگاری و موارد استفاده از آنها، طرح ریزی ترمیم سوانح، تحلیل مخاطرات، قوانین و مقررات امنیتی، مبانی حقوقی، فرآیندهای بازرسی جرائم رایانه ای، امنیت فیزیکی و بسیاری مطالب دیگر آشنا می شوند. در این دوره مفاهیم گسترده ای برای آموزش شرکت کنندگان گرد هم آوری شده و چگونگی کارکرد همه این مفاهیم با یکدیگر به منظور ایجاد لایه های دفاعی مستحکم آموزش داده می شود

CISSP
Certified

Information Systems Security Professional

تیم مدیریتی IT House از سال ۱۳۸۷ به صورت جدی به منظور ارائه خدمات مشاوره ای و آموزشی در حوزه ی چارچوب های مدیریتی فناوری اطلاعات پا به عرصه ی ظهور گذاشت. این گروه در ابتدا تحت نام های تجاری دیگری همچون NIS ICT شروع به فعالیت نموده که در سال ۱۳۹۸ به منظور ارائه خدمات جدید و متفاوت برند IT House را ایجاد نموده اند. IT House با اتکا به توانمندی نیروهای متخصص داخلی و همچنین حمایت شبکه ای گسترده از شرکای بین المللی، همچون گذشته آمادگی دارد سبد کاملی از خدمات مورد نیاز سازمان ها را در حوزه های استانداردها و چارچوب های مدیریت فناوری اطلاعات و امنیت اطلاعات، ارائه نماید. حوزه های اصلی فعالیت این شرکت چارچوب ها و استانداردها و به روش های مدیریتی فناوری اطلاعات از جمله و نه محدود به موارد مندرج در دیاگرام های ذیل است که در هر یک از چارچوب های درج شده خدمات مرتبط با:

- آموزش
 - مشاوره
 - نرم افزار
 - ممیزی و صدور گواهینامه
 - ارزیابی
- بسته به نوع محصول، ارائه می شود.

سرفصل های دوره

Lesson 01 - Course Introduction

- Course Introduction

Lesson 02 - Security and Risk Management

- Security and Risk Management
- Information Security Management
- Security Controls
- Information Security Management and Governance
- Goals, Mission, and Objectives
- Due Care
- Security Policy
- Compliance
- Computer Crimes
- Legal Systems
- Intellectual Property (IP) Law
- Privacy
- General Data Protection Regulation
- Security
- Risk Analysis
- Types of Risk Analysis
- Security Control Assessment
- Threat Modeling
- Supply-Chain Risk Management
- Third-Party Management
- Business Continuity Planning
- Business Continuity Planning Phases
- Managing Personnel Security
- Security Awareness Training
- Program Effectiveness Evaluation
- Key Takeaways
- Knowledge Check

Lesson 03 - Asset Security

- Asset Security
- Information Classification
- Data Classification
- Data Life Cycle
- Data Management
- Different Roles
- Data Remanence
- Privacy
- States of Data
- Data Loss Prevention
- Key Takeaways
- Knowledge Check

Lesson 04 - Security Engineering

- Introduction
- Security Engineering
- Security Architecture
- Security Models
- Evaluation Criteria
- System Security
- CPU
- Memory
- Security Mode
- Cloud Computing
- IoT
- Industrial Control System (ICS)
- Cryptography
- Encryption Methods
- DES
- Asymmetric Cryptography
- Public Key Infrastructure
- Cryptanalysis
- Key Management
- Critical Path Analysis
- Site Location
- Fire
- HVAC
- Key Takeaways
- Knowledge Check

Lesson 05 - Communications and Network Security

- Introduction
- Network Architecture and Design
- IP Addressing
- Network Protocols
- Transmission Media
- Firewall
- Intrusion Detection System and Intrusion Prevention System
- Network Access Control (NAC)
- Content Delivery Network (CDN)
- Networks
- Software-Defined Networking (SDN)
- Remote Access
- Internet Security Protocol (IPsec)
- Voice over Internet Protocol (VoIP)
- Phreaking
- Secure Access Protocols
- Wireless Technologies
- Network Attacks
- Key Takeaways

- Electronic Discovery
- Incident Management
- Security Operations Management
- Identity and Access Management
- Assets
- Malware
- Management
- Recovery and Backup
- Disaster Recovery
- Perimeter Security
- Key Takeaways
- Knowledge Check

Lesson 09 - Software Development Security

- Software Development Security
- Importance of Software Development Security
- Programming Concepts
- Systems Development Life Cycle
- Application Program Interface
- Software Security and Assurance
- Database and Data Warehouse Environments
- Knowledge Management
- Web Application Environment
- Security Threats and Attacks
- Key Takeaways
- Knowledge Check

درباره مدرک

به شرکت کنندگان در این دوره ی آموزشی گواهی حضور از سوی شرکت IT HOUSE اعطا خواهد شد.

محتوای آموزشی

محتوای مورد استفاده در این دوره ی آموزشی آخرین ویرایش از الگوها و استانداردهای ارائه شده توسط انجمن جهانی ISC2 آمریکا می باشد که دارای درجه کیفی مطلوب از این انجمن جهانی می باشد.

- Knowledge Check

Lesson 06 - Identity and Access Management

- Identity and Access Management
- Identity Management
- Biometrics
- Passwords
- Tokens
- Memory Cards and Smart Cards
- Access and Authorization Concepts
- Identity Management Implementation
- Kerberos
- Access Control Types
- Access Control Models
- Access Control Tools and Techniques
- Accountability
- Access Control Monitoring
- Identity Proofing
- Markup Languages
- Identity as a Service (IDaaS)
- Key Takeaways
- Knowledge Check

Lesson 07 - Security Assessment and Testing

- Security Assessment and Testing
- Security Assessment
- Vulnerability Assessment
- Penetration Testing
- Audits
- Log Management
- Synthetic Transaction and Real Transaction
- Testing
- Software Testing
- Interface Key Performance Indicators (KPI)
- Key Takeaways Knowledge Check

Lesson 08 - Security Operations

- Security Operations
- Investigation
- Forensic Investigation
- Evidence