Cognixia®

Certified Information Systems Security Professional (CISSP)

www.cognixia.com

About Cognixia

Cognixia- A Digital Workforce Solutions Company is dedicated to delivering exceptional trainings and certifications in digital technologies. Founded in 2014, we provide interactive, customized training courses to individuals and organizations alike, and have served more than 130,000 professionals across 45 countries worldwide.

Our team of more than 7000 industry experts facilitate more than 450 comprehensive digital technologies courses, along with state-of-the-art infrastructure, to deliver the best learning experience for everyone. Our comprehensive series of instructor-led online trainings, classroom trainings and on-demand self-paced online trainings cover a wide array of specialty areas, including all of the following:

- IoT
- Big Data
- Cloud Computing
- Cyber Security
- Machine Learning
- AI & Deep Learning
- Blockchain Technologies
- DevOps

Cognixia is ranked amongst the top ve Ā emerging technologies training companies by various prestigious bodies. We're also RedHat Enterprise Partner, Microsoft Silver Learning Partner and an authorized training partner for ITIL, Automation Anywhere and ISC2.

OUR AWARDS & AFFILIATIONS

Best Workplace Amongst Emerging Enterprises Awarded By
Great Indian Workplace Awards – 2018
Mumbai, India

Best Training Provider of the Year
Awarded By
The Golden Globe Tiger Awards – 2018
Kuala Lampur, Malaysia

TOP 5 Big Data TRAINING INSTITUTES 2017 siliconindia

WORLD HRD CONGRESS
Cognixia is awarded as Training Company of the Year, 2018

Top 10 IoT Training Companies for the **Second consecutive year.**
2017 IoT India MAGAZINE

TOP 10 PROMISING IoT TRAINING INSTITUTES IN INDIA 2017 HIGHER EDUCATION Review

World HRD Congress has awarded for Excellence in Training (Asia)

TOP 5 CLOUD TRAINING INSTITUTIONS INDIA 2016 HIGHER EDUCATION Review

Asian Training & Leadership Award, Dubai

siliconindia BEST TRAINING PROVIDER BIG DATA HADOOP DEVELOPER OF THE YEAR 2016

Top 10 IoT Training Institutes – 2016
Analytics India MAGAZINE

Best of Pages 2019
Top 10 Linkedin Best of Pages, 2019

ISO 9001 2015 CERTIFIED
ISO 9001:2015 Certified Quality Management System

ISO ISO/IEC 27001 : 2013
ISO/IEC 27001:2013 Certified Information Security Management System

AUTHORIZED TRAINING PARTNERS FOR

(ISC)² OFFICIAL TRAINING PARTNER

AUTOMATION ANYWHERE

ITIL®

Silver Microsoft Partner

PMI®

CISSP Market Outlook

- The CISSP certification is the most globally recognized certification in the information security market and is considered as the most valuable security certification, according to LinkedIn.
- According to the (ISC)2 Cybersecurity Workforce Study, the demand for CISSP-certified personnel is significantly higher than the number of credential holders, with an estimated global cyber workforce shortage of over 2.9 million individuals.
- On an average, (ISC)2 members report earning 35% more than non-members.

Cognixia's CISSP Training & Certification Course

The CISSP training and certification by Cognixia would help you get an increased level of credibility and trustworthiness. It will help you sharpen your ability to manage and communicate better with different stakeholders.

Cognixia's live hands-on online CISSP training is delivered by experts and covers all the eight domains of the CISSP exam outline. This CISSP training will help you prepare thoroughly for the official CISSP examination and achieve your CISSP certification.

Who should take this course?

The CISSP certification is ideal for experienced security practitioners, managers, and executives interested in proving their knowledge across a wide array of security practices and principles.

Prerequisites

To be eligible for the CISSP certification, candidates must have a minimum of five years of cumulative paid work experience in two or more of the eight domains of the CISSP CBK. Having a four-year college degree or a regional equivalent or additional credential from the (ISC)2 approved list would count as one year of the required experience.

If a candidate does not have the required experience to become a CISSP, they can become an Associate of (ISC)2 by successfully passing the CISSP examination. They will then have six years to earn the five years of the required experience.

Program Structure

- 40 hours of live online instructor-led training
- Industry experienced instructor
- 24x7 dedicated PoC support
- Multiple hands-on labs for different modules

Detailed Curriculum: Modules

Module 1: Security and Risk Management

- Understand, adhere to, and promote professional ethics
  - (ISC)2 Code of Professional Ethics
  - Organizational code of ethics
- Understand and apply security concepts
  - Confidentiality, integrity, availability, authenticity, and non-repudiation
- Evaluate and apply security governance principles
  - Alignment of the security function to business strategy, goals, mission, and objectives
  - Organizational processes (e.g., acquisitions, divestitures, governance committees)
  - Organizational roles and responsibilities
  - Security control frameworks
  - Due care/due diligence
- Determine compliance and other requirements
  - Contractual, legal, industry standards, and regulatory requirements
  - Privacy requirements
- Understand legal and regulatory issues that pertain to information security in a holistic context
  - Cybercrimes and data breaches
  - Import/export controls
  - Licensing and Intellectual Property (IP) requirements
  - Transborder data flow
  - Privacy
- Understand requirements for investigation types – administrative, criminal, civil, regulatory, industry standards
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
  - Business Impact Analysis (BIA)
  - Develop & document the scope and the plan
- Contribute to and enforce personnel security policies and procedures
  - Candidate screening and hiring
  - Compliance policy requirements
  - Employment agreement and policies
  - Privacy policy requirements
  - Onboarding, transfers, and termination processes
  - Vendor, consultant, and contractor agreements and controls
- Understand and apply risk management concepts
  - Identify threats and vulnerabilities
  - Risk assessment/analysis
  - Risk response
  - Countermeasure selection and implementation
  - Applicable types of controls – preventive, detective, corrective, etc.
  - Control assessments – security & privacy
  - Monitoring and measurement
  - Reporting
  - Continuous improvement (e.g., Risk maturity modeling)
  - Risk frameworks
- Understand and apply threat modeling concepts and methodologies
- Apply Supply Chain Risk Management (SCRM) concepts
  - Risks associated with hardware, software, and services
  - Minimum security requirements
  - Third-party assessments and monitoring
  - Service level requirements
- Establish and maintain a security awareness, education, and training program
  - Methods and techniques to present awareness & training (e.g., social engineering, phishing, security champions, gamification)
  - Periodic content reviews
  - Program effectiveness evaluation

Detailed Curriculum: Modules

Module 2: Asset Security

- Identify and classify information and assets
  - Data classification
  - Asset classification
- Establish information and asset handling requirements
- Provision resources securely
  - Information and asset ownership
  - Asset inventory (e.g., tangible, intangible)
  - Asset management
- Manage data lifecycle
  - Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
  - Data collection
  - Data location
  - Data maintenance
  - Data retention
  - Data remanence
  - Data destruction
- Ensure appropriate asset retention (e.g., End-of-Life (EOL) End-of-Support (EOS))
- Determine data security controls and compliance requirements
  - Data states (e.g., in use, in transit, at rest)
  - Scoping and tailoring
  - Standards selection
  - Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

Module 3: Security Architecture and Engineering

- Research, implement and manage engineering processes using secure design principles
  - Threat modeling
  - Least privilege
  - Defense in depth
  - Secure defaults
  - Fail securely
  - Separation of Duties (SoD)
  - Keep it Simple
  - Zero trust
  - Privacy by design
  - Trust but verify
  - Shared responsibility
- Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
- Select controls based on systems security requirements
- Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
  - Client-based systems
  - Sever-based systems
  - Database systems
  - Cryptographic systems
  - Industrial Control Systems (ICS)
  - Cloud-based systems (e.g., SaaS, IaaS, PaaS)
  - Distributed systems
  - Internet of Things (IoT)
  - Microservices
  - Containerization
  - Serverless
  - Embedded Systems
  - High-Performance Computing (HPC) systems
  - Edge Computing systems
  - Virtualized systems

Detailed Curriculum: Modules

Module 3: Security Architecture and Engineering

- Select and determine cryptographic solutions
  - Cryptographic lifecycle (e.g., keys, algorithm selection)
  - Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
  - Public Key Infrastructure (PKI)
  - Key management practices
  - Digital signatures and digital certificates
  - Non-repudiation
  - Integrity (e.g., hashing)
- Understand methods of cryptanalytic attacks
  - Brute force
  - Ciphertext only
  - Known plaintext
  - Frequency analysis
  - Chosen ciphertext
  - Implementation attacks
  - Side-channel
  - Fault injection
  - Timing
  - Man-in-the-Middle (MITM)
  - Pass the hash
  - Kerberos exploitation
  - Ransomware
- Apply security principles to site and facility design
- Design site and facility security controls
  - Wiring closets/intermediate distribution facilities
  - Server rooms/data centers
  - Media storage facilities
  - Evidence storage
  - Restricted and work area security
  - Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
  - Environmental issues
  - Fire prevention, detection, and suppression
  - Power (e.g., redundant, backup)

Module 4: Communication and Network Security

- Assess and implement secure design principles in network architectures
  - Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
  - Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6)
  - Secure protocols
  - Implications of multi-layer protocols
  - Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP))
  - Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD-WAN))
  - Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite)
  - Cellular networks (e.g., 4G, 5G)
  - Content Distribution Networks (CDN)
- Secure network components
  - Operation of hardware (e.g., redundant power, warranty, support)
  - Network Access Control (NAC) devices
  - Transmission media
  - Endpoint security
- Implement secure communication channels according to the design
  - Voice
  - Multimedia collaboration
  - Remote access
  - Data communications
  - Virtualized networks
  - Third-party connectivity

Detailed Curriculum: Modules

Module 5: Identity and Access Management (IAM)

- Control physical and logical access to assets
  - Information
  - Systems
  - Devices
  - Facilities
  - Applications
- Manage identification and authentication of people, devices, and services
  - Identity Management (IdM) implementation
  - Single/Multi-Factor Authentication (MFA)
  - Accountability
  - Session management
  - Registration, proofing, and establishment of identity
  - Federated Identity Management (FIM)
  - Credential management systems
  - Single Sign-On (SSO)
  - Just-In-Time (JIT)
- Federated identity with third-party service
  - On-premise
  - Cloud
  - Hybrid
- Implement and manage authorization mechanisms
  - Role-Based Access Control (RBAC)
  - Rule-Based Access Control
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Attribute-Based Access Control (ABAC)
  - Risk-Based Access Control
- Manage the identity and access provisioning lifecycle
  - Account access review (e.g., user, system service)
  - Provisioning and de-provisioning (e.g., on/off-boarding and transfers)
  - Role definition (e.g., people assigned to new roles)
  - Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)
- Implement authentication systems
  - OpenID Connect (OIDC)/Open Authorization (OAuth)
  - Security Assertion Markup Language (SAML)
  - Kerberos
  - Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)

Module 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
  - Internal
  - External
  - Third-party
- Conduct security control testing
  - Vulnerability assessment
  - Penetration testing
  - Log reviews
  - Synthetic transactions
  - Code review and testing
  - Misuse case testing
  - Test coverage analysis
  - Interface testing
  - Breach attack simulations
  - Compliance checks
- Collect security process data (e.g., technical, and administrative)
  - Account management
  - Management review and approval
  - Key performance and risk indicators
  - Backup verification data
  - Training and awareness
  - Disaster Recovery (DR) and Business Continuity (BC)

Detailed Curriculum: Modules

Module 6: Security Assessment and Testing

- Analyze test output and generate reports
  - Remediation
  - Exception handling
  - Ethical disclosure
- Conduct or facilitate security audits
  - Internal
  - External
  - Third-party

Module 7: Security Operations

- Understand and comply with investigations
  - Evidence collecting and handling
  - Reporting and documentation
  - Investigative techniques
  - Digital forensic tools, tactics, and procedures
  - Artifacts (e.g., computer, network, mobile devices)
- Conduct logging and monitoring activities
  - Intrusion detection and prevention
  - Security Information and Event Management (SIEM)
  - Continuous monitoring
  - Egress monitoring
  - Log management
  - Threat intelligence (e.g., threat feeds, threat hunting)
  - User and Entity Behavior Analytics (UEBA)
- Perform Configuration Management (CM)(e.g., provisioning, baselining, automation)
- Apply foundational security operations concepts
  - Need-to-know/least privilege
  - Separation of Duties (SoD) and responsibilities
  - Privileged account management
  - Job rotation
  - Service Level Agreements (SLAs)
- Apply resource protection
  - Media management
  - Media protection techniques
- Conduct incident management
  - Detection
  - Response
  - Mitigation
  - Reporting
  - Recovery
  - Remediation
  - Lessons learned
- Operate and maintain detective and preventative measures
  - Firewalls (e.g., next-generation, web application, network)
  - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
  - Whitelisting/blacklisting
  - Third-party provided security services
  - Sandboxing
  - Honeypots/honeynets
  - Anti-malware
  - Machine learning and artificial intelligence-based tools
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
  - Backup storage strategies
  - Recovery site strategies
  - Multiple processing strategies
  - System resilience, High availability (HA), Quality of Service (QoS), and fault tolerance
- Implement Disaster Recovery (DR) processes
  - Response
  - Personnel
  - Communications

Detailed Curriculum: Modules

Module 7: Security Operations

  - Assessment
  - Restoration
  - Training & awareness
  - Lessons learned
- Test Disaster Recovery Plans (DRP)
  - Read-through/tabletop
  - Walkthrough
  - Simulation
  - Parallel
  - Full interruption
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
  - Perimeter security controls
  - Internal security controls
- Address personnel safety and security concerns
  - Travel
  - Security training and awareness
  - Emergency management
  - Duress

Module 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
  - Development methodologies (e.g., Agile, Waterfall DevOps, DevSecOps)
  - Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
  - Operation and maintenance
  - Integrated Product Team (IPT)
- Identify and apply security controls in software development ecosystems
  - Programming languages
  - Libraries
  - Toolsets
  - Integrated Development Environment (IDE)
  - Runtime
  - Continuous Integration and Continuous Delivery (CI/CD)
  - Security Orchestration, Automation, and Response (SOAR)
  - Software Configuration Management (SCM)
  - Code repositories
  - Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))
- Assess the effectiveness of software security
  - Auditing and logging of changes
  - Risk analysis and mitigation
- Assess the security impact of acquired software
  - Commercial-off-the-shelf (COTS)
  - Open-source
  - Third-party
  - Managed Services (e.g., SaaS, IaaS, PaaS)
- Define and apply secure coding guidelines and standards
  - Security weaknesses and vulnerabilities at the source-code level
  - Security of Application Programming Interfaces (APIs)
  - Secure coding practices
  - Software-defined security

Cognixia USPs

- LIFETIME LMS ACCESS
- 24 x 7 SUPPORT
- REAL-LIFE PROJECTS & CASE STUDIES
- INDUSTRY EXPERTS AS TRAINERS
- INDUSTRY STANDARD CERTIFICATE

POTENTIAL CAREER OPTIONS

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

Certified Information Systems Security Professional (CISSP)

To learn more visit
www.cognixia.com