

# Official Certified Information Systems Security Professional® (CISSP®) CBK® Review Course



CISSP® certification is for the individual who provides the highest standard of information security for an organisation's customers, employees, stakeholders & organisational information assets & / or assesses whether the information systems meets these expectations & best practices. CISSP® certification promotes international practices & provides executive management with assurance that those earning the designation have the required experience & knowledge to provide a solutions-orientation based on the broader understanding of the (ISC)<sup>2</sup> CBK®.

The CISSP® credential is more than an entry-level certification & is a much sought-after designation for mid- & senior-level managers who are working towards a globally recognised standard of achievement as security professionals. It has often been looked upon as a mandatory qualification for the information security practitioner & is specifically developed for the information systems professional who has acquired experience working on the front lines of all aspects of information systems or managing those who do. Individuals with five years or more of experience managing information systems security will find CISSP® tailored to their expertise & the increasing global demand for high standards of certified professionalism.

## Course Objectives

This official (ISC)<sup>2</sup> CISSP® CBK® practical five-day, authorised instructor-led course is designed to ensure that the delegates:

- Obtain the skills & knowledge of the core competencies required of an information systems security professional whether planning to sit for the examination or not, which they will have achieved in a structured learning environment
- Gain practical insight into the 10 CISSP® domains of the Common Body of Knowledge & have thoroughly prepared for the certification examination in a systematic way
- Master the concepts & topics related to all aspects of information systems security

## Course Objectives by Audience:

- Information systems professionals with at least 5 years of information systems security experience
- Information systems security managers or those with management responsibilities
- Information systems security staff & other information security assurance providers who require & in-depth understanding of information systems security management

During the program, students will learn about & prepare for the certification examination. This learning programme employs outcome-based delivery that focuses on preparing you for the skills required to pass the rigorous CISSP® examination. You will work through a series of sample exam questions & mock tests in order to strengthen your ability in preparing for & undertaking the examination.

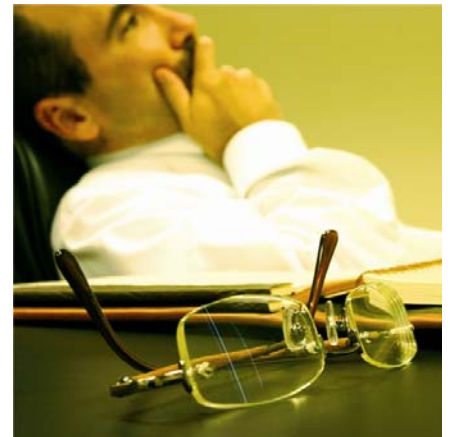
## In-house Training

All Analytix Courses are available in-house, should your organisation have a number of people or multiple sets to train. The cost advantages & the ability to discuss & resolve organisational issues are two major attractions of such training.

## Who will benefit?

The course is aimed at preparing candidates for the CISSP® examination by providing them with the knowledge and understanding they require to pass the exam, as defined by (ISC)<sup>2</sup> such as:

- IT Systems Security Professionals
- Information Security Managers/Officers/Professionals
- Auditors involved in Information Security
- Financial and Operational Auditors
- Security Professionals who are preparing for the CISSP® examination



## What you will learn

On completion of the course, delegates will be able to enhance their preparation for the CISSP® exam by learning about the 10 domains of the information security practice:

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

## Pre-requisites

It is recommended that candidates attending this course and who wish to enter the CISSP® exam have some prior knowledge of security principles or experience of working in the security field.



## Course Content

**Access Control** - a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

**Application Security** - addresses the important security concepts that apply to application software development. It outlines the environment where software is designed & developed & explains the critical role software plays in providing information system security.

**Business Continuity & Disaster Recovery Planning** – for the preservation & recovery of business operations in the event of outages.

**Cryptography** - the principles, means, & methods of disguising information to ensure its integrity, confidentiality & authenticity.

**Information Security & Risk Management** - the identification of an organization's information assets & the development, documentation, & implementation of policies, standards, procedures, & guidelines. Management tools such as data classification & risk assessment/analysis are used to identify threats, classify assets, & to rate system vulnerabilities so that effective controls can be implemented.

### **Legal, Regulations, Compliance & Investigation**

- Computer crime laws & regulations
- The measures & technologies used to investigate computer crime incidents

**Operations Security** - used to identify the controls over hardware, media, & the operators & administrators with access privileges to any of these resources. Audit & monitoring are the mechanisms, tools, & facilities that permit the identification of security events & subsequent actions to identify the key elements & report the pertinent information to the appropriate individual, group, or process.

**Physical (Environmental) Security** - provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.

**Security Architecture & Design** - contains the concepts, principles, structures, & standards used to design, monitor, & secure operating systems, equipment, networks, applications & those controls used to enforce various levels of availability, integrity, & confidentiality.

### **Telecommunications & Network Security**

- Network structures
- Transmission methods
- Transport formats
- Security measures used to provide availability, integrity, & confidentiality
- Authentication for transmissions over private & public communications networks & media

## **Register Today**

To register, or for more information, please contact us:

**Tel: 0861 ANALYTIX or 0861 262 598**

**Fax: +27 (011) 447 4192**

**Email: [info@analytix.co.za](mailto:info@analytix.co.za)**

**Web site: [www.analytix.co.za](http://www.analytix.co.za)**



## Approach, Deliverables & Method

### **The practical hands-on course provides:**

- Cross referencing & alignment to (ISC)<sup>2</sup> CISSP® Review Manual
- Instruction from a certified CISSP® trainer with extensive operational experience across a broad range of public & private sector organisations

### **Course Deliverables:**

- Comprehensive course notes & advice on further sources of information
- CISSP® presentation manual, test exam paper, (ISC)<sup>2</sup> Resource Guide
- Certificate of attendance upon completion of the course

### **Delivery Method:**

- Classroom style - combining lecture, discussion, practical examination tips & case studies utilising course materials, digital projector & flipchart
- Delegates are encouraged to bring their copy of the CISSP® Study Guide as issued by (ISC)<sup>2</sup> to the course

## Consulting Services

Analytix's Consulting Services include, among others, Business Continuity Management, Corporate & IT Governance, ISO 27001 compliant ISMS implementation, IT maturity assessments, security certification assistance & performance management.

## Examination Objectives – Scoring & Format

The CISSP® Examination follows a multiple-choice format & consists of one six-hour paper containing 250 multiple-choice questions with four choices each. The examination tests a candidate's knowledge of IS audit principles & practices as well as technical content areas. The exam covers the ten content areas (domains) & those tasks that are routinely performed by a CISSP®. The passing grade required is a scale score of 700 out of a possible 1000 points on the grading scale.

In order to qualify to sit for the examination, the candidate should have at least four full years of experience in information security or three years of professional in the information security field & a university degree.

All exam fees, queries & registrations can be directed to Lindsay Drabwell ([ldrabwell@isc2.org](mailto:ldrabwell@isc2.org)) & Ben Roberts ([broberts@isc2.org](mailto:broberts@isc2.org)) at (ISC)<sup>2</sup>.

## Benefits of Attending this (ISC)<sup>2</sup> CISSP® 5-Day Seminar

- Five 8 hour days of practical sessions
- The only official (ISC)<sup>2</sup> practice CISSP® exam review seminar
- Practice exam evaluation
- 100% revised, updated or new material
- Extensive work from certified CISSP®s / (ISC)<sup>2</sup> Instructors & subject-matter experts in developing material & presentation
- Identifies topic areas students should study for exam preparation
- Provides an overview of the scope of the information systems security field

**ANALYTIX CONSULTING (PTY) LTD**

MLC House • 1st Floor • 50 Sixth Road • Hyde Park • 2196

PO Box 413988 • Craighall • 2024

[www.analytix.co.za](http://www.analytix.co.za) • [info@analytix.co.za](mailto:info@analytix.co.za)