

**CISSP IS THE CERTIFICATION THAT INSPIRES
UTMOST CONFIDENCE
NEW HORIZONS BULGARIA,
SOFIA, SEPTEMBER 2010**



**IT Security Trainings in 2010:
CISSP: CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL**

**THE 2010 NEW HORIZONS TRAINING
INTEGRATED LEARNING APPROACH TO THE CISSP
(CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL)**

2010 CISSP includes instructor-led training, online training resources and mentored learning training to deliver the effective theoretical and practical knowledge for passing the **CISSP** certification exam.

2010 CISSP represents a **COMPLETE LEARNING LIFECYCLE**. It focuses on knowledge transfer and knowledge retention to enable students to obtain skills needed to work effectively and apply the knowledge obtained during training in **THE PRACTICAL ENVIRONMENT**.

The 2010 CISSP approach is designed for the adult learner who learns best by combining visual, audio, and hands-on learning methods throughout the overall experience. The approach is simple and comprehensive.

THE 2010 CISSP INTEGRATES 3 APPROACHES TO EFFECTIVE PREPARATION FOR THE CISSP EXAM:

APPROACH 1: TRADITIONAL CLASSROOM TRAINING: Instructor lecture and demonstration with Boris Goncharov
SCHEDULE: Fixed, September 27th 2010 – October 1st 2010
DURATION: 40 hours, 5 days

APPROACH 2: MENTORED LEARNING: Instructor lectures through Computer-Based-Training and mentor
Schedule: Flexible, individual
DURATION: 40 hours

APPROACH 3: WEB-BASED TRAINING: Online ANYTIME delivery method,
SCHEDULE: Delivery through web-based interface in flexible hours
DURATION: 390 hours of CBT in the area of Information Security, 1-year access

WHAT IS THE BENEFIT OF GETTING CERTIFIED AS CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP®)?

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the not-for-profit International Information Systems Security Certification Consortium, commonly known as (ISC)². The CISSP has been adopted as a baseline for the U.S. National Security Agency's ISSEP program.

The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

WHO SHOULD ATTEND?

Professionals with solid hands-on experience in IT and work experience in IT Security. Managers and owners responsible for the information security within the organization. Prerequisite for certification are five years of direct, full-time professional work experience in two or more of the [ten domains](#).

INSTRUCTOR:



BORIS GONCHAROV **CISSP CERTIFIED**

Areas of expertise:

- (*) Network and Systems Security
- (*) Research and Development
- (*) Regulatory Adherence
- (*) Security Policies & Procedures Development/Implementation
- (*) Data Integrity / Disaster Recovery
- (*) Risk Assessments / Impact Analysis
- (*) ISO 27001:2005
- (*) Contingency Planning
- (*) Technical Specifications Development
- (*) Team and Project Leadership
- (*) Information Systems Management
- (*) System Administration
- (*) .NET Programming
- (*) Security Systems Design
- (*) Alarm over IP (AOIP)



Boris Goncharov's professional experience

- ✓ The first IT manager to implement ISO 27001:2005 in Bulgaria
- ✓ Responsible for Corporate Information Security (IS) Program Management at G4S
- ✓ Coordinates the ISO 27001:2005 for Central and Southeast Europe at G4S
- ✓ Trainer at New Horizons Bulgaria since 2009

THE 2010 NEW HORIZONS TRAINING INTEGRATED LEARNING APPROACH TO THE CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL)

CONTENTS:

1. TRADITIONAL CLASSROOM TRAINING OUTLINE:

Certified System Security Professional: Classroom Training

Duration: 5 Days, 40 hours of training

Schedule: 5 Days, 8 hours/day

Delivery Method: Instructor-Led training in New Horizons Bulgaria

Trainer: Boris Goncharov, CISSP Certified, the first IT Manager in Bulgaria to implement ISO 27000

Outline:

This course addresses the essential elements of the 10 domains that comprise a Common Body of Knowledge. It offers a job-related approach to the security process, and provides basic skills required to prepare for CISSP certification. It gives valuable consultations/advises to help gather understanding on the practical side of CISSP.

- 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

2. MENTORED LEARNING TRAINING CONTENT OUTLINE:

Certified System Security Professional: Mentored Learning

Duration: 40 hours of training

Schedule: Flexible

Delivery Method: Individual, CBT course with individual consultation in New Horizons Bulgaria

Trainer: Shon Harris

Outline:

The Shon Harris CISSP Series brings together all the materials, tools, and study aids you need to pass the CISSP exam. Whether you are a security professional, a seasoned engineer, or are looking for a career change - this is the solution to bring your career to new heights! Our objective is to not just prepare you for CISSP Certification, but to also provide you with the practical, detailed understanding and knowledge of security topics that will be of valued use to you and your company. Our product focuses not only on the areas necessary for the CISSP examination, but also on a more detailed and practical perspective that will give you competitive skills in the real world as well.

Lesson 1: Information Systems Access Control

Data Access Principles
System Access and Authentication
Penetration Tests

Lesson 2: Security Architecture and Design

Security Models
Security Modes
System Assurance

Lesson 3: Network and Telecommunications Security

Data Network Design
Remote Data Access
Data Network Security
Data Network Management

Lesson 4: Information Security Management Goals

Organizational Security
The Application of Security Concepts

Lesson 5: Information Security Classification and Program Development

Information Classification
Security Program Development

Lesson 6: Risk Management and Ethics

Risk Management
Ethics

Lesson 7: Application Security

Software Configuration Management
Software Controls
Database System Security

Lesson 8: Cryptography

Ciphers and Cryptography
Symmetric-Key Cryptography
Asymmetric-Key Cryptography
Hashing and Message Digests
Email, Internet, and Wireless Security
Cryptographic Weaknesses

Lesson 9: Physical Security

Physical Access Control
Physical Access Monitoring
Physical Security Methods
Facilities Security

Lesson 10: Operations Security

Operations Security Control
Operations Security Auditing and Monitoring
Operational Threats and Violations

Lesson 11: Business Continuity and Disaster Recovery Planning

Business Continuity Plan Fundamentals
Business Continuity Plan Implementation
Disaster Recovery Plan Fundamentals
Disaster Recovery Plan Implementation

Lesson 12: Legal, Regulations, Compliance, and Investigations

Computer Crime Laws and Regulations
Computer Crime Incident Response

3. WEB-BASED TRAINING OUTLINE:

Information Security Library: Online

Duration: 380+ hours of training, 1 year access

Schedule: Flexible

Delivery Method: Individual, CBT course online

Outline:

1. A+ Certification (CompTIA), 56 hours of training

CompTIA® A+® Certification: A Comprehensive Approach for all Exam Objectives

2. Certified Ethical Hacker, 10 hours of training

Certified Ethical Hacker: Additional Hacking Tools

Certified Ethical Hacker: Hacking Process

Certified Ethical Hacker: Web Server Hacking

3. Certified Information Systems Security Professional (CISSP)®, 85 hours of training

4. Computer Hacking Forensic Investigator, 30 hours of training

Computer Hacking Forensics Investigator: File Systems and Operating Systems

Computer Hacking Forensics Investigator: Forensics Procedures from Start to Finish

Computer Hacking Forensics Investigator: Forensics Process and Procedures

5. Network Security, 143 hours of training

Advanced Security Implementation

Defending Against Intrusion

Defending Against Risks

Defending the Network

Enterprise Security Solutions

Firewall: A Network Security Measure

Hardening the Infrastructure

Network Defense and Countermeasures

Network Security Fundamentals

PKI and Biometrics Concepts and Planning

PKI and Biometrics Implementation

6. Security Awareness, 5 hours of training

Security Awareness (Second Edition) (Part 1): Protecting Information and Counteracting Social Engineering

Security Awareness (Second Edition) (Part 2): Maintaining Computer and File Security

Security Awareness (Second Edition) (Part 3): Promoting Email Security and Proper Responses to Security Incidents

Security Awareness (Third Edition)

7. Security+ Certification, 57 hours of training

CompTIA Security+® (2008 Objectives) (Comprehensive)

Security+® Certification: Public Key Infrastructure (Windows Server 2003)

Security+® Certification: Security Basics (Windows Server 2003)

Security+® Certification: Security Enforcement (Windows Server 2003)

Security+® Certification: System Hardening (Windows Server 2003)

Our next CISSP class is starting September 27th 2010, 9:00

CALL +359.42.100.40/44 FOR MORE INFORMATION