Business Solutions for Africa

CISSP BOOT CAMP
(Earn 35CPE)
29th June to 3rd July 2009 Hotel La Mada Nairobi Kenya

WHY CISSP?

The CISSP Common Body of Knowledge (CBK) review course covers the breadth of information security and prepares candidates for the CISSP examination. This course is suitable for individuals that intend for CISSP or Associate-CISSP certification.

CISSP Body of Knowledge (CBK) Areas include[1]:

1. Access Control Systems & Methodology
2. Applications & Systems Development
3. Business Continuity Planning
4. Cryptography
5. Legal, Regulations, Compliance and Investigations
6. Operations Security
7. Physical Security
8. Security Architecture & Models
9. Security Management Practices
10. Telecommunications, Network & Internet Security

Course Description
This Review Seminar is the most comprehensive, complete review course discussing the entire information system security common body of knowledge.

The benefit of the review seminar is, of course, to help the individual prepare for the exam. However, it also serves as a very good learning tool for concepts and topics, known as the Common Body of Knowledge (CBK), related to all aspects of information systems security. The CBK is the compilation and distillation of all information systems security material collected internationally of relevance to information system security professionals.

CBK Review Seminars are held regularly to ensure information system security professionals have an opportunity to review the CBK in-depth, in preparation for certification examinations and to stay current on the ever-evolving domains within the information system security field.

High-level review of the main topics.

Identifies topic areas students should study for exam preparation.

Provides an overview of the scope of the field.
A discussion of the topics, subtopics, and sub-subtopics of the CBK domains is provided during the five days. The material has been redesigned and updated to reflect the latest information system security issues, concerns, and countermeasures. An overview of the topics, subtopics, and sub-subtopics of the ten CBK domains are discussed during the five days.

Prerequisites
CBK Review Seminars are held regularly to ensure information system security professionals have an opportunity to review the CBK in-depth, in preparation for certification examinations and to stay current on the ever-evolving domains within the information system security field.

High-level review of the main topics.
Identifies topic areas students should study for exam preparation.
Provides an overview of the scope of the field.

What you will achieve

A discussion of the topics, subtopics, and sub-subtopics of the CBK domains is provided during the five days. The material has been redesigned and updated to reflect the latest information system security issues, concerns, and countermeasures. An overview of the topics, subtopics, and sub-subtopics of the ten CBK domains are discussed during the five days.

What you will learn

Security Management Practices

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

The Security Architecture and Models domain contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality.
Access Control Systems and Methodology

Access controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.
Application Development Security

This domain addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.
Operations Security

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

The physical security domain provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.
Cryptography

CISSP preparatory course deals with the security concepts to be mastered in order to obtain CISSP certification. In an accelerated but rigorous manner, the course prepares the student for the CISSP examination, covering the entirety of the Common Body of Knowledge about security (CBK) as defined by the ISC2®. The CBK covers ten security domains: 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, and Telecommunications and Network Security.

Curriculum

Day 1 :

- Information Security and Risk Management
- Operations Security

Day 2 :

- Security Architecture and Design
- Access Control

Day 3 :

- Cryptography
- Application Security

Day 4 :

- Telecommunications and Network Security

Day 5 :

- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Compliance and Investigations
- Physical Security

Prerequisites :

- Participants must possess a basic understanding of networks, operating systems and information security. The course is an intensive review in preparation for the examination, not basic training.

General information :

- The certification exam is not included with the course. To apply for the examination, go to the official web site of the ISC2 (www.isc2.org).
- CISSP certification is based on a multiple-choice exam consisting of 250 questions about the 10 domains of the CBK – Length: 6 hours. A score of 75% is required to pass the exam successfully.

Business Solutions for Africa

Instructor Profiles

Matunda Nyanchama, CISSP, PhD
Security Consultant, Trainer & Conference Speaker
Matunda@matunda.org

Biographical Summary

Matunda Nyanchama, Ph.D, CISSP has more than 10 years experience in IT security, both corporate and teaching. He has worked in various capacities including Delivery Project Executive (DPE) and Senior Program Manager at IBM Global Services with responsibilities for service delivery for outsourced contracts. Previously he held positions as Delivery Manager of security, privacy and identity consulting. Others include Senior Manager of Information Security and Risk Management at Moneris Solutions, a payment solutions company based in Toronto, Canada. Prior to that he was a Senior Advisor for Information Security Analytics at the Bank of Montreal Financial Group, where he focused on information security risk analytics, business strategy and security awareness. As a senior manager of Information Security at the Bank of Montreal, he established and operated the Information Protection Centre (IPC), the first of its kind in the financial sector in Canada. Dr Nyanchama has held a number of professional security positions, including Senior Security Consultant at Ernst & Young and Director of Security Architecture, Intellitactics Inc., a Canadian security software company.

Dr Nyanchama has also taught and designed university courses in IT security, is this respect he has taught in the Masters of Information Technology Security (MITS) program of the University of Ontario Institute Of Technology (UOIT), Ontario, Canada

Matunda holds masters and doctoral degrees in computer science from the University of Western Ontario in Canada, and an undergraduate electrical engineering degree from the University of Nairobi in Kenya. He is a Certified Information Systems Security Professional (CISSP). He has presented on the subject of Sarbanes-Oxley compliance and security and written about information security metrics. Dr Nyanchama has published a number of security management papers, including co-authoring a chapter in the Information Security Management Handbook the reference guide for CISSP. His doctoral work in Role-Based Access Control (RBAC) is widely cited in computer security literature.

Matunda is also listed in the *Who is Who in Black Canada*, 2006 edition. He is an active member in the African Diaspora community and a featured speaker in a number of events.

ENQUIRIES and REGISTRATIONS: Call or Write directly to

K-Ninety East Africa Ltd.
P.O. Box 3894-00100
Nairobi Kenya
Tel +254 20 608316
Fax +254 20 608318
Cell +254 722 77 14 78
Email: training@k-90ea.com
Web: www.k-90ea.com

Contact: **Loise**

Register by 19th June 2009