

TECHNOLOGY TRANSFER PRESENTS

CLEMENT DUPUIS

CISSP[®]

Preparation Class

APRIL 19-23, 2010
VISCONTI PALACE HOTEL - VIA FEDERICO CESI, 37
ROME (ITALY)



info@technologytransfer.it
www.technologytransfer.it

ABOUT THIS SEMINAR

Easy to understand CISSP® prep curriculum with intense (daily) online quizzes ensure you master the 10 domains *and* successfully pass the CISSP® exam the first time”. 99% Pass the first time, The SU CISSP® Prep class effectively prepares information security professionals to pass the rigorous six-hour Certified Information Systems Security Professional [CISSP®] examination. This SU CISSP® Prep program offers each student a zero-distraction, fully-immersed CISSP® CBK training and certification experience that employs accelerated learning techniques to minimize time-to-proficiency while maximizing retention.

- You are taught by CISSP Master Clement Dupuis, the father of the www.cccure.org Website
- More CISSP's pass the first time they take the exam
- Accelerated learning techniques to focus on long term information retention
- Multiple daily quizzes - approved www.cccure.org vendor
- Guarantees the highest quality of education and customer satisfaction
- Or return for free

What places this CISSP training above all others?

- With our CISSP Experts, instructors & Clement Dupuis, we have developed a reputation for excellence in training and prep for your CISSP exam
- Our daily quizzes and course materials are always updated with the latest information on the exam objectives
- Robust course materials that cater to your individual learning styles for a successful learning experience
- Build your “personal” exam prep guide” based on what you need to know to pass the exam the first time
- Expert mentoring by veteran security professionals before and after class guide you to success
- Quiz, engage in materials and Quiz again is the secret to your exam success
- 100+ retired exam questions to familiarize you with the exam style

WHAT YOU WILL LEARN

Tips for taking the Exam and SU Self Study Techniques

OUTLINE

1. Information Security and Risk Management

Identify an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines to identify risk.

- CIA
- Roles and Responsibilities - RACI
- Asset Management
- Taxonomy - Information Classification
- Risk Management
- Risk Analysis & Assessment
- Information Classification
- Policies, Procedures, Standards, Baselines & Guidelines
- Security Awareness Programs
- Certification and Accreditation

2. Access Control

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

- AAA
- Access to systems & data
- IPS intrusion prevention & IDS detection
- Audit trail monitoring
- Authentication Methods
- Authorization - DAC, RBAC, MAC
- Accounting - Logging, Monitoring, Auditing
- Central/Decentralized and Hybrid Management
- Single Sign-on - Kerberos, RADIUS, Diameter, TACACS
- Threats
- Vulnerabilities - Emanations, Impersonation, Rogue Infrastructure, Social Engineering

3 Cryptography

Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

- Terminology
- Cryptosystems
- Ciphers
- Algorithms
- Hashing
- Public Key Crypto
- Digital Signatures
- Symmetric/ Asymmetric
- PKI
- Internet Security
- Cryptosystems - SSL, S/MIME, PGP
- Cryptanalysis

4. Physical (Environmental) 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.

- Buildings, and related infrastructure against threats
- Terminology
- Technical controls - access controls, intrusion detection system, and monitoring system
- Supporting facilities - heating/cooling, electrical plant, and water system
- Facility Design
- Fire Safety
- Electrical Security
- HVAC
- Perimeter Security - Fences, Gates, Lighting
- Physical facility - buildings and structures housing computer facilities

- Physical Access Control - Transponders, Badges, Swipe Cards
- Theft
- Intrusion Detection - CCTV, Alarms, Guards, & Dogs

5. Security Architecture and Design

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.

- Identify the security issues and controls with architectures and designs
- Describe the principles of common computer and network organizations, Enterprise Architecture and designs
- Layering, Data Hiding and Abstraction
- Processors
- Memory - Segmentation/Rings, Types of Memory
- Operating Systems
- Defines and understand system models
- Assurance - TCSEC, ITSEC, CC
- Architecture Problems - Covert Channels + TOC/TOU, Object Reuse

6. Application Security

Addresses the important security concepts that apply to application software development and outlines the environment where software is designed and developed.

- General Security Principles
- Database
- Applications

- Artificial Intelligence Models
- SDL
- Programming/Data Attacks
- Malware
- Threats
- Real World Issues
- Change Management
- Database Security
- Mobil Code

7. Telecommunications and Network Security domain address

- Network Structures
- Transmission methodology
- Transport formats
- OSI/DoD TCP/IP Models
- TCP/UDP/ICMP/IP
- Ethernet
- Devices - Routers/Switches/Hubs
- Firewalls
- Wireless
- WAN Technologies - X.25/Frame Relay/ PPP /ISDN/DSL/Cable
- Voice - PBX/Cell Phones/VOIP
- IPSec
- Network Vulnerabilities

8. Legal, Regulations, Compliance, and Investigations domain addresses

- Computer crime laws and regulations
- The measures and technologies used to investigate computer crime incidents
- Ethics - Due Care/Due Diligence
- Intellectual Property
- Incident Response
- Forensics
- Evidence
- Laws - HIPAA, GLB, SOX

9. Business Continuity & Disaster Recovery Planning domain addresses Business operations in the event of outages

- Policy
- Roles and Teams
- Business Continuity Planning
- Business Impact Assessment
- Recovery Strategy
- Recovery Plan Development
- Emergency Response
- Data Backups, Vaulting, Journaling, Shadowing
- Backups & Off-Site Storage
- Software Escrow Arrangements
- External Communications
- Utilities
- Logistics & Supplies
- Emergency Response
- Required Notifications /Testing

10. Operations Security

- Identify the controls over hardware, media, and administration to any of these resources. And audit & monitoring that identify security events and subsequent actions.
- Change Control/Configuration Management
- Dual Control, Separation of Duties, Rotation of Duties
- Information Security Controls
- Violation analysis
- Audit trails/reporting
- Resource Protection
- Appropriate administrator/operator privilege
- Recovery procedures
- Attack methods
- Vulnerability Assessment and Pen-Testing

CERTIFICATION

CISSP® (Certified Information Systems Security Professional) Certifications is based on the CBK (Common Body of Knowledge) which comprises ten subject domains that is compiled and maintained through ongoing peer review by subject matter experts. requires exam candidates to have a minimum of five years of relevant work experience in two or more of the ten domains, 5 years of work experience with an applicable college degree, or a credential from the (ISC) 2 -approved list.

CISSP® is a registered trademark of (ISC)²® SU CISSP® classes are not endorsed, sponsored or delivered by (ISC)²®.

Disclaimer

CISSP® a registered trademark of (ISC)²® Inc (International Information Systems Security Certification Consortium) Inc. The materials for the Security University classes have been developed specifically for SU and is not endorsed, sponsored or delivered by (ISC)²®. The goal of the course is to prepare security professionals for the CISSP® exam by covering the ten domains defined by (ISC)²®

INFORMATION

<p>PARTICIPATION FEE</p> <p>€ 2000</p> <p>The fee includes all seminar documentation, luncheon and coffee breaks.</p> <p>VENUE</p> <p>Visconti Palace Hotel Via Federico Cesi, 37 Rome (Italy)</p> <p>SEMINAR TIMETABLE</p> <p>9.30 am - 1.00 pm 2.00 pm - 5.00 pm</p>	<p>HOW TO REGISTER</p> <p>You must send the registration form with the receipt of the payment to: TECHNOLOGY TRANSFER S.r.l. Piazza Cavour, 3 - 00193 Rome (Italy) Fax +39-06-6871102</p> <p>within April 6, 2010</p> <p>PAYMENT</p> <p>Wire transfer to: Technology Transfer S.r.l. Banca Intesa Sanpaolo S.p.A. Agenzia 6787 di Roma Iban Code: IT 34 Y 03069 05039 048890270110</p>	<p>GENERAL CONDITIONS</p> <p>GROUP DISCOUNT</p> <p>If a company registers 5 participants to the same seminar, it will pay only for 4. Those who benefit of this discount are not entitled to other discounts for the same seminar.</p> <p>EARLY REGISTRATION</p> <p>The participants who will register 30 days before the seminar are entitled to a 5% discount.</p> <p>CANCELLATION POLICY</p> <p>A full refund is given for any cancellation received more than 15 days before the seminar starts. Cancellations less than 15 days prior the event are liable for 50% of the fee. Cancellations less than one week prior to the event date will be liable for the full fee.</p> <p>CANCELLATION LIABILITY</p> <p>In the case of cancellation of an event for any reason, Technology Transfer's liability is limited to the return of the registration fee only.</p>
---	---	--

CLEMENT DUPUIS

CISSP® Preparation Class

April 19-23, 2010
Visconti Palace Hotel
Via Federico Cesi, 37
Rome (Italy)

Registration fee:
€ 2000

If registered participants are unable to attend, or in case of cancellation of the seminar, the general conditions mentioned before are applicable.

first name

surname

job title

organisation

address

postcode

city

country

telephone

fax

e-mail



Stamp and signature

Send your registration form with the receipt of the payment to:
Technology Transfer S.r.l.
Piazza Cavour, 3 - 00193 Rome (Italy)
Tel. +39-06-6832227 - Fax +39-06-6871102
info@technologytransfer.it
www.technologytransfer.it



Clement Dupuis

Security Instructor & Curriculum Manager, Instructor CISSP, Security+, Q/EH, Q/SA
Senior Security Evangelist and Security Curriculum Manager Security University
Owner and Maintainers of the CISSP Open Study Guides Web site at www.cccure.org

It's rare to find a true industry luminary and innovator teaching a certification boot camp class for "ordinary" professionals. But leader and standard-setter, Clément Dupuis, sees sharing his extensive knowledge and experience with his students as "a privilege and a responsibility."

"I come from a small lumberjack village in northern Quebec, Canada," he explains. "People there help each other. It's how we are. It's what we do." Even so, Mr. Dupuis's humble beginnings belie the tremendous contributions he has made – and continues to make – to the world of Internet technology and security. For 20 years, he served as a communication and IT Security specialist in the Canadian Department of National Defense (DND). "Where I was first stationed," he recalls, "there were three things to do in one's spare time – hunt, fish, or drink. There's only so much that anyone can do of any of these activities, so I bought my first computer to learn and explore on my own." He quickly became known for his expertise and became responsible for the first series of computers deployed within army field units ("they were big 65 pound tempest clunker with tons of screws – 42 to open the cover alone"). He also achieved the milestone of having built the first LAN and WAN ever deployed in an army operational unit. In the early 1990s, he supported NATO operations in Somalia and Rwanda, being one of the few people in the world who could build and support complex computer/satellite communication systems from scratch under the most austere conditions ever experienced by troops oversea.

Mr. Dupuis's knowledge and abilities became so deep and highly regarded by the Canadian military that his last two years within the Department of Defense were spent training others and passing along his huge amount of knowledge. He very actively participated in the development of the first version of the CISSP and GSEC course materials for the SANS Institute, he supervised the delivery of all security related classes at Vigilar Intense School, he is now exclusively teaching for Security University in the United States. He worked for the SANS institute for many years, he has delivered classes at all of the largest conferences such as Las Vegas and Orlando. Only the instructors who have achieved the highest student satisfaction score gets to present at those conferences. It is reserved for the best instructors of the faculty.

He is one of the companies most popular, most successful and often-requested instructors, which is due as much to his dry sense of humor and unassuming manner as to his extensive insights and experience. He is proud of the relationships he builds with his students and is pleased to advise them before, during, and even after they have completed their exams.