

Daily Lesson Plan

KEY DATA

Course Name: CISSP/ISSO

Duration: 5 days

Language: English

Format:

- Instructor-led classroom
- Computer Based Training
- Live Virtual Training

Prerequisites:

- Experience in the 10 domains of the CBK would be beneficial

Student Materials:

- 10 modules covering each of the 10 CBK domains
- Professionally developed graphics and 3-D animations that enhance the understanding of complex concepts
- Extensive notes accompanying each slide, including Configuration Steps, Hints, Warnings, Tips, Tables, etc
- Quick Tips section, Summary section, Terminology section and 20 question and answers for each module



Introduction

Case Study #1

Building a Successful Security Infrastructure

Domain 1

Information Security and Risk Management

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Domain 2

Access Control

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Domain 3

Cryptography

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Domain 4

Physical (Environmental) Security

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test



Also available as..

Live Virtual Training (LVT)

bringing live instructors to you anywhere.....

Features:

- Live presentations & powerful functionality delivering our proprietary slides, documents, virtual whiteboards, and a media-center through an easy-to-use toolbar.
- Application, file, and desktop sharing.
- One dedicated high-spec remote PC per student with full access as if sitting in our classroom.
- Instructors view your remote session when you perform hands on labs.
- Instructor can access your remote system to demonstrate or assist! Real classroom style mentoring.
- Public and private text chat for increased interactivity between participants and easily saved to file.

Domain 5

Security Architecture and Design

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Domain 6

Business Continuity and Disaster Recovery Planning

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Domain 7

Telecommunications and Network Security

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Day 1 – Session 1

Check-in:

Accept incoming students, verify identity and resolve last minute lodging issues, pass-out course materials, ensure quality of presentation facility.

Introduction and Orientation:

Introduce instructor, explain the facilities layout, policies and procedures, emergency procedures, and location of refreshments and restrooms.

Overview and Course Description:

Explain the benefits of the respective certifications explain the layout of the course and set expectations. Log on to the certification web site and familiarize students with the application process. Discuss best strategies for filling out the security work history portion of the application for examination.

Objective of Case Study #1:

Demonstrate to students that Security is not only about Technology. CISSPs & ISSOs can create state-of-the-art infrastructures to protect confidential data but if final users are not trained accordantly, the whole strategy is a waste of money and time. The user is the weakest link in any Security Strategy.

Domain 8

Application Security

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Domain 9

Operations Security

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Domain 10

Legal, Regulations, Compliance, and Investigations

- Presentation (Lecture)
- Practice / Exercise / Labs / Demos
- Apply your knowledge
- Practice Test

Day 1 – Session 2

Information Security and Risk Management

Overview

Security management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify assets, and to rate their vulnerabilities so that effective security controls can be implemented. Risk management is the identification, measurement, control, and minimization of loss associated with uncertain events or risks. It includes overall security review, risk analysis; selection and evaluation of safeguards, cost benefit analysis, management decision, safeguard implementation, and effectiveness review.

From the ISC2

“The candidate will be expected to understand the planning, organization, and roles of individuals in identifying and securing an organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security awareness training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; employment agreements; employee hiring and termination practices; and risk management practices and tools to identify, rate, and reduce the risk to specific resources.”

Case Studies

- Implementing a Successful Security Assessment Process

https://www2.sans.org/reading_room/whitepapers/basics/450.php?id=450&cat=basics

Day 2 – Session 1

Access Control

Overview

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system. The candidate should fully understand access control concepts, methodologies and implementation within centralized and decentralized environments across the enterprise's computer systems. Access control techniques, detective and corrective measures should be studied to understand the potential risks, vulnerabilities, and exposures.

Case Studies

- Identity Authentication Management (IAM)
 - <http://www.indigovision.com/learnabout-iaminipvideo.php>
- Cisco Systems Network Admission Control (NAC) Presentation
 - http://www.cisco.com/cdc_content_elements/flash/nac/demo.htm

Day 2 – Session 2

Cryptography

Overview

The Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity. The candidate will be expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; and the applications, construction and use of digital signatures to provide authenticity of electronic transactions, and non-repudiation of the parties involved.

Case Studies

- AXA Technology Services Reduces Data Security Costs with Public Key Infrastructure
- <http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000000819>

Day 2 – Session 2

Physical (Environmental) Security

Overview

The Physical Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

From the ISC2

“The candidate will be expected to know the elements involved in choosing a secure site, its design and configuration, and the methods for securing the facility against unauthorized access, theft of equipment and information, and the environmental and safety measures needed to protect people, the facility, and its resources.”

Case Studies

- Data Center Physical Security Checklist
- https://www2.sans.org/reading_room/whitepapers/awareness/416.php?id=416&cat=awareness

Day 3 – Session 1

Security Architecture and Design

Overview

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

The candidate should understand security models in terms of confidentiality, integrity, information flow, commercial vs. government requirements; system models in terms of the Common Criteria, international (ITSEC), United States Department of Defense (TCSEC), and Internet (IETF IPSEC); technical platforms in terms of hardware, firmware, and software; and system security techniques in terms of preventative, detective, and corrective controls.

Case Studies

- Villagemall.com
- <http://www.microsoft.com/resources/casestudies/CaseStudy.asp?CaseStudyID=11040>

Day 3 – Session 2

Business Continuity & Disaster Recovery Planning

Overview

The Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and DRP involve the preparation, testing and updating of specific actions to protect critical business processes from the effect of major system and network failures. Business Continuity Plans counteract interruptions to business activities and should be available to protect critical business processes from the effects of major failures or disasters. It deals with the natural and man-made events and the consequences if not dealt with promptly and effectively. Business Impact Assessment determines the proportion of impact an individual business unit would sustain subsequent to a significant interruption of computing or telecommunication services. These impacts may be financial, in terms of monetary loss, or operational, in terms of inability to deliver.

Disaster Recovery Plans contain procedures for emergency response, extended backup operation and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objective of the Disaster Recovery Plan is to provide the capability to process mission-essential applications, in a degraded mode, and return to normal mode of operation within a reasonable amount of time.

From the ISC2

“The candidate will be expected to know the difference between business continuity planning and disaster recovery; business continuity planning in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development, and implementation. The candidate should understand disaster recovery in terms of recovery plan development, implementation and restoration.”

Day 4 – Session 1

Telecommunication & Network Security

Overview

Telecommunications and Network Security domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media. The candidate is expected to demonstrate an understanding of communications and network security as it relates to voice communications; data communications in terms of local area, wide area, and remote access; Internet/Intranet/Extranet in terms of Firewalls, Routers, and TCP/IP; and communications security management and techniques in terms of preventive, detective and corrective measures.

Case Studies

- The Case of Brazil
- <http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.15.pdf>

Day 4 – Session 2

Application Security

Overview

Applications and systems development security refers to the controls that are included within systems and applications software and the steps used in their development. Applications refer to agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

From the ISC2

“The candidate should fully understand the security and controls of the systems development process, system life cycle, application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces, and concepts used to ensure data and application integrity, security, and availability.”

Day 5 – Session 1

Operations Security

Overview

Operations Security is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources. Audit and monitoring is 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. Operations Security covers the knowledge of what resources must be protected, what privileges should be restricted, the control mechanisms available, the potential for abuse of access, the appropriate controls, and the principles of good practice.

Case Studies

QualysGuard Free Trial and Guides

<http://www.qualys.com/products/trials/>

QualysGuard Demos

<http://www.qualysguard.com/products/demos/>

Penetration Test Automation

http://www.coresecurity.com/files/attachments/CORE_IMPACT-WhitePaper.pdf

Social Engineering Workshop Introduction:

Discuss social engineering and its impact on operational security. Discuss what the workshop will entail.

Day 5 – Session 2

Legal, Regulations, Compliance and Investigation

Overview

The Law, Investigations, and Ethics domain addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed, methods to gather evidence if it has, as well as the ethical issues and code of conduct for the security professional.

Incident handling provides the ability to react quickly and efficiently to malicious technical threats or incidents.

From the ISC2

“The candidate will be expected to know the methods for determining whether a computer crime has been committed; the laws that would be applicable for the crime; laws prohibiting specific types of computer crime; methods to gather and preserve evidence of a computer crime, investigative methods and techniques; and ways in which RFC 1087 and the (ISC) 2™ Code of Ethics can be applied to resolve ethical dilemmas.”

Case Studies

International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime

- http://www.business.com/search/rslt_default.asp?vt=all&query=computer+crime&type=web

Final Review Test:

Students will take a 50 question final review test, covering all the CBK,

Review Test Scoring and Q & A:

Grade tests out loud for self-check assessment. Field questions and clarification for areas not understood by students. Suggest areas of further study for those that need it.

Closure and Instructor Review: Hand out an Instructor Evaluation form for the students to fill out, say thanks, and wish them luck.