AVTECH

COURSE SYLLABUS

CISSP Certification Training Program

50 Cragwood Rd, Suite 350
South Plainfield, NJ 07080

Victoria Commons, 613 Hope Rd Building #5,
Eatontown, NJ 07724

130 Clinton Rd,
Fairfield, NJ 07004

Avtech Institute of Technology Course

Instructor:
Course Duration: 50 Hours
Date/Time:
Training Location:

Course: CISSP

Text / Lab Books:

Course Description

A CISSP certification garners significant respect, signifying that the recipient has demonstrated a higher standard of knowledge, proficiency, and ethics. This course ensures that a student is fully prepared to face the exam's rigorous criteria. It is crafted to match the overall theme of the exam, which emphasizes a general, solutions-oriented knowledge of security that organizations want. The goal of this course is to provide information security professionals a fully immersed, zero-distraction, all-inclusive CISSP training and certification experience. Our CISSP Training course encompasses the CISSP review seminar and value-added instruction.

CISSP Exam Track:

The CISSP Certification examination consists of 250 multiple-choice questions. Candidates have up to 6 hours to complete the examination. Ten CISSP information systems security test domains are covered in the examination pertaining to the Common Body of Knowledge:

- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications, Network & Internet Security

Course Outline:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. Cryptography

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

8. Telecommunications, Network, and Internet Security

The telecommunications, network, and Internet security domain discusses the:

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

9. Business Continuity Planning

The Business Continuity Plan (BCP) domain addresses the preservation and recovery of business operations in the event of outages.

10. Law, Investigations, and Ethics

The Law, Investigations, and Ethics domain addresses:

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

To become a CISSP, a candidate must successfully complete two processes: **Examination** and **Certification**:

Examination

The eligibility requirements to sit for the CISSP examination are completely separate from the eligibility requirements necessary to be certified.

To sit for the CISSP examination, a candidate must:

- Submit the examination fee.
- Assert that he or she possesses a minimum of three years of professional experience in the information security field. (Please note that this requirement will increase to four years experience or three years plus a college degree for prospective candidates effective January 01, 2003).
- Complete the Candidate Agreement, attesting to the truth of his or her assertions regarding professional experience and legally commit to adhere to the CISSP Code of Ethics.

Successfully answer four questions regarding criminal history and related background.

Certification

To be issued a certificate, a candidate must:

- Pass the CISSP exam with a scaled score of 700 points or greater.
- Submit a properly completed and executed Endorsement Form.
- If the candidate is selected for audit, they must successfully pass that audit of their assertions regarding professional experience.

Endorsement

Once a candidate has been notified of passing the CISSP examination, he or she will be required to have his or her application endorsed by a CISSP before the credential can be awarded. If no

CISSP can be found, another qualified professional with knowledge of information systems or an officer of the candidates corporation can be used to validate the candidate's professional experience.

The endorser will attest that the candidate's assertions regarding professional experience are true to the best of their knowledge, and that the candidate is in good standing within the information security industry.

Upon receipt of the Endorsement Form and barring a random audit of the candidate's professional experience, the CISSP credential should be awarded within one business day, with a formal notification sent via e-mail.

Audit

A percentage of the candidates who pass the CISSP examination and submit endorsements will be randomly subjected to audit and required to submit a resume for formal review and investigation.

If audited (subject to results), the credential will be awarded within seven business days and notification sent via e-mail. Naturally, there may be some delays due to mail service or the number of forms received. Also, audits may require additional time for verifying information and/or contacting references.

Prerequisite

4 years of networking experience in the related field.

Contact Hours

______ Contact Hours   (Lecture ___ Hours / Lab ____ Hours)

Semester Credit Hours

__________ semester credit hours

Teaching Strategies

A variety of teaching strategies may be utilized in this course, including but not limited to, lecture, discussion, written classroom exercises, written lab exercises, performance based lab exercises, demonstrations, quizzes and examinations. Some quizzes may be entirely or contain lab based components. A mid-course and end course examination will be given.

Method of Evaluating Students

Grade Distribution

Class Attendance	10
Mid Term	30

Finals	50
Special Projects Makeup projects	10
Total	**100%**

Grading Policy

At the end of each course, each student is assigned a final grade as follows:

Point Range	Interpretation	Grade	Quality Points
90 – 100	Excellent	A	4.0
80 – 89	Very Good	B	3.0 – 3.9
70 – 79	Average	C	2.0 – 2.9
60 – 69	Poor	D	1.0 – 1.9
Below 60	Failure	F	0
N/A	Withdrawal	W	0
N/A	Pass	P	0
N/A	Incomplete	I	0

A student earning a grade of D or above is considered to have passed the course and is eligible to pursue further studies. A student receiving a grade of F has failed the course. A failed course must be repeated and passed to meet Avtech Institute's graduation requirements, in addition to an overall program GPA of 2.0.

Requirements for Successful Completion of the Course

At a minimum, students must achieve the following:

- A passing grade of **D** or above
- Completion of all required examinations
- Submission of all required lab exercises and projects and;
- Adherence to the school attendance policy.

Equipment Needed

Industry standard desktop computer for lab exercises.

Equipment Breakdown Lab room

Videos and Projector

Library Assignments

To be determined by the instructor.

Portfolio Assignment

Student program outcome portfolios are required to demonstrate student competencies. In conjunction with your course structure, please select a project/paper that best demonstrates what you have learned in this course and add it to your program portfolio.

Course Policies

Disruptive Behavior

Disruptive behavior is an activity that interferes with learning and teaching. Inappropriate talking during class, surfing inappropriate website, tardiness, cheating, alcohol or drug use, use of cell phone, playing lout music during class, etc. all disrupt the learning process.

Copyright Infringement

Specific exemptions to copyright infringement are made for student use in the context of learning activities. Graphic design students often download images from the Internet, or scan images from publications. As long as this work is for educational purpose, and subject to faculty permission, this is not a problem.

Plagiarism

Faculty cannot tolerate the ***misrepresentation of work as the student's own***. This often involves the use by one student or another student's design, whether voluntarily or involuntarily. In the event that plagiarism is evident and documented, all students involved in the conscious decision to misrepresent work must receive an F as the grade for the project. A second occurrence may result in suspension for the rest of the quarter, and return to the school only after a review by the Academic Standards Committee.

Attendance

Attendance and Lateness

In education and the workplace, regular attendance is necessary if individuals are to excel. There is a direct correlation between attendance and academic success. Attendance is mandatory. All students must arrive on time and prepared to learn at each class session. At the faculty member's discretion, students may be marked absent if they arrive more than 15 minutes late to any class. More that five absences in a class that meets twice per week or more that two absences in a class that meets once per week may result in a failure.

Make-Up Work

Late Projects and Homework

All projects and homework must be handed in on time. Homework should be emailed to your instructor if you are going to miss a class. Work that is submitted one week late will result in the loss of one full grade; and work that is submitted two weeks late will result in the loss of two full grades; more than two weeks late you will receive a failing grade on the project.