



CERTIFIED INTERNATIONAL INFORMATION SYSTEM SECURITY PROFESSIONAL (CISSP)

Course	Maintenance Management
Instructor	Certified American Academy Instructor
Recognition	CHEA, ICE, ANSI, ACBSP, DIKTI
Descriptions	Along with the increasing dependence of organizations on information technology and awareness of the importance of data in information systems, the need for information system security also increases. This is where the important role of CISSP because it covers various fields quite deeply, technical and non-technical. Extensive and in-depth knowledge in various fields (domains) of information security is needed because CISSP is intended to be in a middle management position which requires it to be able to work with Top Management, Users, to IT Engineers, each of whom has a different point of view, approach and "language". In addition, information security cannot be viewed only from the point of view of a particular domain. Certified International Information Systems Security Professional (CISSP) is a global certification in the field of IT Security managed by the International Board of Standards which does not refer to a specific product (vendor neutral) and covers all aspects of security ranging from information security management, security physical to very technical such as how network protocols and asynchronous encryption algorithms work. The American Academy CISSP program is the leading credential for certifying the knowledge, skills and abilities of maintenance, reliability and physical asset management professionals. The CISSP exam is a thorough test of a broad scope of expertise measured against the universal standard. It The American Academy Information System Security training and certifications based on the approach from this high-level perspective and given adequate time, attention and resources, and without these things, the results which are looked for will

	be missing out on a tremendous opportunity for the participants organizations. American Academy offers a full array of CISSP unique professional certificate courses to start or enhance participants career in Information System Security Architecture. Designation program is nationally recognized as the industry leader for professional development training in the field of security architecture. It balances scientifically supported information system security theory with practical application. Participants will learn the latest in information system security architecture and how to apply it in a practical manner at any workplace. The AAPM[®] certification process, administered by GAFM Board, identifies to the public that those individuals who have been authorized to use the AAPM[®] certification marks in the globe have met rigorous professional standards and have agreed to adhere to the principles of integrity, objectivity, competence, fairness, confidentiality, professionalism and diligence when dealing with clients.
Target Audience	Individuals involving in the information system security activities and has strong inclination to certify their professional competence based on International Board of Standards (IBS).
Duration	3 Days
Objectives	Upon the completion of the course the participants will have the following mastership and knowledge competency such as: • Have greater understanding of security concepts and practices • Understand the interrelationships among the areas of information system security architecture • Know what level of understanding is required to pass the CISSP exam • Upon completion of this course, participants will be better prepared to take the CISSP exam, and will have a balanced exposure to key security principals and practices

- **Cryptography**
This domain examines methods and techniques for disguising data for protection purposes. This involves cryptography techniques, approaches, and technologies. Some of the topics covered include:
 - Symmetric versus asymmetric algorithms and uses
 - Public key infrastructure (PKI) and hashing functions
 - Encryption protocols and implementation
 - Attack methods
- **Security Architecture and Models**
This domain examines concepts, principles, and standards for designing and implementing secure applications, operating systems, and systems. This covers international security measurement standards and their meaning for different types of platforms. Some of the topics covered include:
 - Operating states, kernel functions, and memory mapping
 - Security models, architectures, and evaluations
 - Evaluation criteria: Trusted Computer Security Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), and Common Criteria
 - Common flaws in applications and systems
 - Certification and accreditation
- **Operations Security**
This domain examines controls over personnel, hardware, systems, and auditing and monitoring techniques. This also covers possible abuse channels and how to recognize and address them. Some of the topics covered include:
 - Administrative responsibilities pertaining to personnel and job functions
 - Maintenance concepts of antivirus, training, auditing, and resource protection activities
 - Preventive, detective, corrective, and recovery controls
 - Standards, compliance, and due care concepts
 - Security and fault tolerance technologies
- **Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)**
This domain examines the preservation of business activities when faced with disruptions or disasters. This involves the identification of real risks, proper risk assessment, and countermeasure implementation. Some of the topics covered include:
 - Business resource identification and value assignment
 - Business impact analysis and prediction of possible losses
 - Unit priorities and crisis management

	- Plan development, implementation, and maintenance - Evidence types and admissibility into court - Incident handling • Laws, Investigation, and Ethics This domain examines computer crimes, laws, and regulations. This includes techniques in investigating a crime, gathering Evidence, and handling procedures. It also covers how to develop and implement an incident-handling program. Some of the topics covered include: - Types of laws, regulations, and crimes - Licensing and software piracy - Export and import laws and issues - Evidence types and admissibility into court - Incident handling • Physical Security This domain examines threats, risks, and countermeasure to protect facilities, hardware, data, media, and personnel. This involves facility selection, authorized entry methods, and environmental and safety procedures. Some of the topics covered include: - Restricted areas, authorization methods, and controls - Motion detectors, sensors, and alarms - Intrusion detection - Fire detection, prevention, and suppression - Fencing, security guards, and security badge types
Case Studies	Specific information system security cases will be analysed and assessed to provide technical and process analytical capability to the participants to assist them in coping with actual situation in their information system security assessment and evaluation.