AFRICA
CENTRE FOR
WORK BASED
LEARNING

CYBER SECURITY / IT SECURITY MANAGEMENT CERTIFICATE

After successful completion of this program, candidates will also receive ICCP Certification!!!

Information technology security has been among the **top ten management concerns** since the 1980's. Technologies such as computer networks, PCs, the web, and more recently SMAC (Social, Mobile, Analytics, Cloud) along with SCADA/Internet of Things continually bring new security considerations to organizations.

These technologies in concert with changes in regulations, especially in light of the growth of valuable and sensitive information assets stored by organizations such as individuals' taxes, financial assets, medical records, job performance reviews, trade secrets, new product developments, and customer data, demand a strong focus on security management; the protection of data/information/knowledge. The threat of invasion by cyber criminals (e.g., governments, competitors, individuals) continues to grow.

No one can escape cyber-attacks, and the fact that it is hard to find trusted people who are expert in this new art of war has driven the demand for security professionals to an all-time high. Many companies are starting to address this issue with the new understanding that constant and ongoing vigilance is the only way to protect infrastructure and data in the long term.

The purpose of this certificate is to help organizations meet this increased demand for information security professionals by preparing attendees via a comprehensive, in-depth, practical set of courses addressing the entire infrastructure (e.g., data, network, web, applications, systems), as well as the management, organizational, and legal issues.

CISSP® | Certified Information Systems Security Professional

Upon completion of this Certificate, candidates will be more than prepared to pass the respective certification provided by

Select 4 courses from the following 12 (CISSP Course included); available face-to-face, online, blended/hybrid

1. **Foundations of Cyber Security**

This 24 hour introduction to information security provides the foundation for understanding the planning and implementation of policies and procedures for protecting information assets, determining the levels of protection and response to security threats and incidents, and designing an appropriate information security system. Candidates will gain an overview of the field of information security and assurance, and will also learn the necessary knowledge to engage in information assurance activities and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, examination of pre- and post-incident procedures, technical and managerial responses, and an overview of the information security planning and staffing functions. Instructors will also introduce the role of the Chief Information Security Management Officer (CISMO).

Candidates will also master risk management, security planning, and security policy enforcement and auditing activities. Candidates will learn about security guidelines, regulation and legal implications, and standards that apply in information security management, as well as information confidentiality, data integrity, and system availability. The course also presents related concepts such as privacy and business continuity planning. While emphasis is placed on managerial and operational security controls, the course also provides an overview of the current and emerging technical security controls applied to access control, operating systems, applications, networks/web, cryptographic solutions, intrusion detection systems, physical security, wireless security, VPNs, digital forensics, and related topics.

The primary objectives of the course are to:

- Understand the importance of information security in business continuity
- Critically analyze security threats and define appropriate technical and managerial controls for these threats
- Understand procedures for ensuring compliance with security policies and standards, establish appropriate systems and plans for security implementation
- Identify legal implications of security and standards for security management
- Recognize the management, organizational, and sourcing considerations for having an effective information security program
- Describe audit and recovery approaches for coping with security breaches

2. **Ethical Hacking**

This 40 hour course offers a comprehensive guide for ethical hacking. An ethical hacker is defined as someone who uses the same methods as criminal attackers use to exploit vulnerabilities in a network accessible to them. The difference is that an ethical hacker performs these “attacks” in order to document whether a network can be breached by known vulnerabilities in order to mitigate the attack vector they expose.

Topics covered include:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- System Hacking
- Trojans and Backdoors
- Viruses and Worms
- Sniffers
- Social Engineering
- Denial of Service
- Session Hijacking
- Hacking Webservers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Evading IDS, Firewalls, and Honeypots
- Buffer Overflow
- Cryptography
- Penetration Testing

3. Computer Hacking Forensic Investigation

This 40 hour course presents a detailed and methodological approach to computer forensics and evidence analysis. This will enable candidates to understand the often complex issues associated with investigating cybercrimes, handling of digital evidence, detection methods and proof, in a variety of digital forensic contexts, including computers, networks and portable digital devices. Each module will build upon the knowledge gained from previous modules. This course will introduce cutting edge technologies and methodologies, alongside fundamental building blocks, allowing candidates to simultaneously understand the theory and practical aspects in dealing with digital investigations.

The primary topics covered in the course are intended to prepare candidates to:

- Understand the function and limitations of forensic investigations.
- Understand procedures used in conducting forensic investigations.
- Guide first responders towards successful data acquisition and preservation.
- Describe digital forensics and relate it to an investigative process.
- Explain the legal issues of preparing for and performing digital forensic analysis. based on the investigator's position and duty.
- Be aware of (digital) evidence storage preparation and requirements.
- Perform basic digital forensic investigations.
- Demonstrate use of digital forensics tools and their underlying principles.
- Size and set up a digital forensic lab.
- Conduct simple binary analysis on files with unknown and possible malicious functionality.
- Recognize the state of the practice and the gaps in technology, policy, and legal issues.

4. Security Analysis and Penetration Testing

This 40 hour course provides an in-depth understanding of how to effectively protect computers and computer networks. Candidates will learn the tools and penetration testing methodologies used by penetration testers. In addition, the course provides a thorough discussion of what and who a penetration tester is and how important they are in protecting corporate and government data from cyber-attacks. Candidates will learn updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also covered is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking.

The primary objectives of the course are to ensure candidates understand how:

1. computer systems are attacked, and how to defend against those attacks.
2. to analyze legal questions, ethical dilemmas, and privacy issues related to computer security.
3. to use their knowledge of computer security to analyze and suggest means of securing information systems.
4. to use their knowledge of computer forensics technology and laws relevant to computer-based crime to analyze various technical challenges, scenarios and cases regarding computer crime.

5. Security Programming

The purpose of this 30 hour course (including either the .Net or Java course) is to provide candidates with a comprehensive understanding of what a Secure Development Process is. The candidates will learn secure programming concepts and techniques; learn how to identify key characteristics of secure code; learn how to use design patterns for secure code; learn how to build in a secure requirement process in the software life cycle from the beginning to the end; and learn how to write, test, and debug programs using secure programming techniques. Topics will include design principles, code snippets, and a simple explanation of each step as you work your way through the course.

The primary objectives of the course are to:

- Identify what secure programming is and why it is needed
- Work with principles associated with software engineering
- Understand principles of security and quality in the industry and how to use them
- Understand the Application Guide
- Learn how to understand, analyze, and interpret software requirements
- Design for quality using industry frameworks
- Know what industry design patterns are and how to carry them out
- Understand industry standard development tools
- Know how to produce secure code
- Sustain a formal development process

Security Considerations for Programming Language Courses (select 1 to be included with the Security Programming course):

6. .Net
7. Java

8. Incident Response Handling and Disaster Revovery

This 24 hour course examines detailed aspects of incident response and contingency planning consisting of incident response planning, disaster recovery planning, and business continuity planning. Developing and executing plans to deal with incidents in the organization is a critical function in information security. This course focuses on the planning processes for all three areas of contingency planning, incident response, disaster recovery and business continuity, and the execution of response to human and non-human incidents in compliance with these policies.

Topics covered include:

- An Overview of Information Security and Risk Management
- Planning for Organizational Readiness
- Contingency Strategies for IR/DR/BC
- Principles of Incident Response and Disaster Recovery
- Incident Response: Detection and Decision Making
- Incident Response: Organizing and Preparing the CSIRT
- Incident Response: Response Strategies
- Incident Response: Recovery and Maintenance
- Disaster Recovery: Preparation and Implementation
- Disaster Recovery: Operation and Maintenance
- Business Continuity Planning
- Crises Management and International Standards in IR/DR/BC

9. Disaster Recovery and Virtualization Planning

This 40 hour course provides an understanding of the various methods in identifying business and technology vulnerabilities. In addition, this course outlines the appropriate countermeasures to mitigate risks and prevent failure. This course is designed to develop a solid foundation to various disaster recovery and business continuity principles, including the assessment of risks, the preparation of a disaster recovery plan, the development of policies and procedures, and an understanding of the roles and relationships within an organization that are recovering from a disaster and the implementation of a plan.

As an important part of a flexible and highly efficient disaster recovery plan, this course addresses the use of virtualization techniques that will assist in the development of an enterprise approach for disaster recovery and business continuity. An introduction to these techniques will be covered, as well as the importance of securing the virtual environments.

The approach used in this course is enterprise-wide and provides the methods for developing a quality and efficient disaster recovery and business continuity plan including the creation and management a secure network environment, establishing procedures and policies and how to restore that network in the unfortunate event of a disaster.

The primary objectives of the course are:

- Understanding the importance of disaster recovery in the enterprise.
- Understanding how to create an enterprise disaster plan.
- Identifying strategies to develop a secure network.
- Understanding the importance of Policy and Procedure.
- Exploring virtualization technologies.
- Understanding the use of traditional and virtual technologies in disaster planning.

10. Network Security Administration

This 40 hour course offers a comprehensive guide for understanding information systems network security management. It provides an introduction to the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The course covers new topics in network security as well, including psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security.

Topics covered include:

- Introduction to Network Security
- Malware and Social Engineering Attacks
- Data Breaches
- Application and Networking-Based Attacks
- Host, Application, and Data Security
- Basic Cryptography
- Advanced Cryptography
- Network Security Fundamentals
- Administering a Secure Network
- Wireless Network Security
- Mobile Device Security
- Access Control Fundamentals
- Authentication and Account Management
- Business Continuity
- Risk Mitigation
- Vulnerability Assessment
- Legal, Ethical, and Organizational Factors

11. Managing Emerging Information Technology

IT organizations must be able to leverage new technologies. This course focuses on how organizations can effectively and efficiently assess trends and emerging SMAC (Social, Mobile, Analytics, Cloud) and security technologies. Participants will learn how to help their organization define, select, and adopt new information technologies, while understanding the respective security implications. This course will introduce candidates to new directions in information systems and effective approaches for evaluating their relevance and applicability to their business environments as well as the new challenges and problems that they present, especially as they pertain to security. Candidates will learn about emerging technologies and the latest design trends in data and knowledge, networks and applications in terms of what issues they address and in particular, how organizations can exploit them for competitive advantage.

Topics include: Creating a business case for an emerging information technology, identifying factors affecting the successful adoption of new information technologies, identifying the key attributes, business benefits, risks, security implications, and cost factors of a new technology, knowing how to effectively use advanced search and selection metrics for identifying and selecting new technology, describing technology trends that presently drive or are expected to drive the selection of new technologies over the next decade and providing organizational structures and frameworks that guide the enhanced adoption and capitalization related to what new technologies and approaches can offer.

CISSP | Certified Information Systems Security Professional

- **CISSP Certification Preparation**

This 8 hour course, after taking the respective GIIM asynchronous or face-to-face courses, prepares candidates to pass the CISSP certification examination.

Hence, students have the option of getting a GIIM Certificate, ICCP Certification, Master's Degree, and/or CISSP certification. This course does not count towards the GIIM Cyber Security Certificate.

The following four optional courses are available face-to-face/synchronously:

A. Architecting IT-Security Infrastructure

This course focuses on the analysis and management of the information security infrastructure. Information security infrastructure consist of the organizational, process, and technology (e.g., data, applications, network, web, systems, operations) domains. The integration and effective management of the IT architecture is essential to appropriately respond to technical risk dynamics. The course will focus on evaluating the architectural domains and their integration. The course will rely on management research on information security, risk, IT strategic planning, and distributed computing. Candidates will learn the relationships between business requirements, technical requirements, and technical risk, and how to make the appropriate choices for risk mitigation. The course will provide insights on the continuous management of the information security function in organizations.

Candidates will understand the most important issues and topics in the huge area of infrastructure security. Topics include: Web and Internet security; Firewalls and IDS; application and database servers; input validation; session management; URL hacking; cyber graffiti; e-shoplifting; session hijacking; impersonation, buffer overflows; virus and worm attacks; Encryption techniques, (DES, AES, Contemporary Symmetric Ciphers, Public Key Cryptography and RSA); message authentication and hash functions; digital signatures and authentication protocols; IP security (IPsec); SNMP; e-mail security; secure socket layer (SSL) and transport layer security; intruder management; malicious software; authentication, authorization, access, and integrity; important security technologies such as cryptographic algorithms (symmetric and asymmetric encryption), SCADA, PKI, and digital certificates.

The course focuses on the management issues of security policies and security administration and describes how various security technologies and approaches can be applied to cybersecurity.

B. Business Continuity and Disaster Recovery Planning

Recent natural, environmental, and “man-made” events have increased the need for organizations to develop strategies for mitigating, preparing for, responding to, and recovering from small and large scale emergencies (e.g., hurricanes, tsunamis, earthquakes, terrorism, unethical acts). In the context of a highly integrated global economy, nearly every business is likely to feel the effects of emergencies around the world, and in the face of intense competition, it is crucial that all businesses have a plan for continuing operations before, during, and after emergencies of all types.

This course presents the important considerations for business continuity and disaster recovery planning. It includes a comprehensive advanced business continuity planning and management workshop which is designed to teach practical methods to develop, test, and maintain a business continuity plan. This course is based on industry best practices and guidelines for business continuity, disaster recovery, and emergency management.

C. Legal, Ethical, and Compliance Concerns

The purpose of this course is to provide an overview of the security initiatives (legal, ethical, and compliance) required by the existing and emerging computing environment while evaluating the controls in place or planned for meeting those requirements. This course examines every major aspect of the relationship between information security and the law at a level suitable for information security specialists and senior managers who supervise information security operations.

The course focuses on the substantive legal principles relating to information security with regard to both industry and government perspectives. It explores information security considerations as the repository of information that may be at issue in legal proceedings. In the United States the government requires that all federal systems have a customized security plan. In addition, the National Training Standard for Information Systems Security (INFOSEC) Professionals requires programs that meet this standard to produce security professionals capable of developing and supporting a security plan.

This course provides an introduction to security planning as recommended by NIST guidelines for developing security plans. Candidates are required to conduct a case study where a security plan is developed for their organization.

D. Information Risk Management Game (optional)

This 1-day business simulation focuses on deriving an information risk management strategy to protect against predators like Oceans99! The story is about a large exhibition in the Tokyo Museum. An important Bank is sponsoring this challenging event. During the preparation of this exhibition there is a rumor Oceans99 has made plans to steal the precious objects. We don’t know how Oceans99 wants to do this but the challenge for the team is to analyze possible risks, protect against threats, and to make the exhibition a success. Participants are part of the international team that will transport the objects from Amsterdam, London, and Las Vegas to the local airports, then fly the objects to Tokyo and transport them to the Tokyo museum were the objects will be exhibited for 4 months. During the preparation the team will develop an information security strategy/policy. This document will define the objectives, the risks/threats, the measures, and activities to manage the protection of the objects against theft. The plans will be implemented and maintained to keep the assurance levels. Would Oceans99 be able to execute their plans?