Global Skill Development Council

Certified Information Security Officer

Certified Information Security Officer certification aspires to build the future experts who will be able to monitor the organization's IT system and look after the security threats.

www.gsdcouncil.org
admin@gsdcouncil.org

Certified Information Security Officer

ABOUT CERTIFICATION

Information security is the practice of protecting information by mitigating information risks. It can be determined as a part of information risk management. When organizations are focusing more and more into continuous delivery lately, the entire process is becoming faster and much more vulnerable day by day. Certified Information Security Officers can help in reducing the vulnerability of a system by establishing protocols for identifying and neutralizing threats.

An Information Security Officer is the one who is responsible for protecting an organization's Information Technology (IT) programs from internal and external threats. Specifically, IT officers are charged with the task of making sure viruses, spyware, bots, or other harmful programs are not used to compromise an organization's computer system. Information security analysts with experience and an advanced degree like Information Security Officer Certification can grab career opportunities as a chief security officer, an information technology manager, or an information systems manager. It is obvious for any organization with a computer system to actively protect the data of its clients and employees.

Our Accreditation:

ANSI
American National Standards Institute

The Global Skill Development Council (GSDC) is the leading third-party, Vendor neutral, international credentialing and certification organization. The Global Skill Development Council (GSDC) is proud to be ANSI Accredited Member.
The American National Standards Institute (ANSI) is a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system.

The Global Skill Development Council (GSDC) is the leading third-party, vendor-neutral, Intern-ational credentialing and certification organization. The Global Skill Development Council (GSDC) is proud to be ABICB accredited member.Accreditation Board For Inter- national Certification Bodies's accrediation is globally recognized as the highest certificati- on for training institutes as it is an independent autonomous body

ABICB

COURSE SYLLABUS

CISMF

1.What is Information Security?:

- Understand the requirements of ISO 27001(ISMS)
- Understand the advantages of ISMS
- Understand the purpose of ISO 27001
- Information Security: Who is responsible?
- Information Asset Classification
- Password Security
- Spam & Malware Protection
- Email Security
- Clear Desk & Clear Screen
- Mobile Usage: Best Practices
- Social Media Usage: Best Practices
- Social Engineering
- Phishing
- Physical Security
- Information Security Incidents

CCSF

1. Introduction to Cyber Security Management

- Concepts and definitions
- Benefits and requirements of Cyber security

2.Introduction to Information Risk Management

- Information risk management terminology
- Risk management in the business context
- Information risk management fundamentals

3.Introduction to Business Continuity Management

- Need for business continuity management
- Business continuity management in the business
- Business continuity lifecycle

4.Cyber Security Architecture

- Concepts of Cyber Security Architecture
- The Role of a Security Architect
- Security Design Principles

5.Soft Skills and Incident Management

- Topics and Learning Outcomes
- Engagement lifecycle management
- Advantages and utility of incident response to the client.
- Awareness potential incidents.
- Organizational frameworks for incident response activities encompass pertinent protocols and procedures.
- Understanding limitations of system logs.
- Timelines to analyse event data
- Time zone issues
- System interpretation of timestamps with images

6. Law & Compliance

- Regulation of Investigatory Powers Act 2000
- Criminal Justice Act 2008
- Protection of Children Act 1978
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Police and Justice Act 2006
- Sexual Offences Act 2008
- Engaging law enforcement
- CERTS and their role and jurisdiction

CDSOE

1. Overview

- What is DevOps?
- What is DevSecOps?
- Tracing the origins of these practices
- Exploring related concepts
- Examining the advantages of DevSecOps
- Benefits of DevSecOps
- Identifying the guiding principles of DevOps

2. Modern Application Development: A Summary :

- The rise of Microservices architecture
- Comparing Microservices with Monoliths
- Exploring the Relationship between Microservices and APIs
- Advantages and disadvantages of adopting Microservices

3. Containerization: An Overview:

- What are Docker Containers?
- Developing applications using Containerization
- Advantages of Containerization
- Drawbacks of Containerization

4. Information Security: A Summary:

- Distinguishing Ethical Hacking, Cyber Security, and Information Security
- Essential Concepts of Information Security
- Career opportunities in Information Security
- Encryption techniques to protect sensitive data
- Effective Policy Management
- Password Management
- Implementing Secure Development LifeCycles
- Adhering to Standards, Best Practices, and Regulations
- Conducting Threat Modeling and Risk Management

5. Cloud Computing and Infrastructure as Code: A Summary:

- What is Cloud?
- What is Cloud Computing?
- Cloud Service Providers and their offerings
- Advantages of Cloud Computing
- Various Cloud Service Models
- Different Cloud Deployment Models

6. Continuous Integration/Continuous Deployment: A Summary:

- Understanding the Software Development Life Cycle (SDLC)
- Defining Integration, Delivery, and Deployment
- What is Continuous Integration/Continuous Deployment (CI/CD)?

CEHF

1.Introduction to Ethical Hacking:

- Hacking Ethics
- Legal implications of hacking.
- Types of hackers
- Basic Principles
- White and black box test
- Phases in the hacking process

1.Introduction to Ethical Hacking:

- Hacking Ethics
- Legal implications of hacking.
- Types of hackers
- Basic Principles
- White and black box test
- Phases in the hacking process

2.Network Sniffing:

- Tools for Network Sniffing
- Tools for Network Sniffing
- Extracting Information
- The function of HTTP headers
- Extract information from HTTP headers

3.Hacking Wireless Networks:

- Aircrack-NG
- Airodump-NG
- Functions of tools within Aircrack.
- ESSID&BSSID means

4.System Penetration:

- Intel Gathering
- Information on a target online
- Information on a target within a network
- Software Tools (Nmap, Metasploit)
- Can scan a target
- How to combine tools
- Fingerprinting and Vulnerabilities
- Fingerprinting and Vulnerabilities
- How to find vulnerabilities based on scanning results
- Manual fingerprinting
- Exploitation and Post Exploitation
- Vulnerability with Metasploit
- System information after exploitation

5.Dimensionality Reduction:

- Database Attacks
- Test for SQLi vulnerabilities
- Extracting data with SQLi
- CONCAT, LOAD_FILE, UNION, SELECT,
- @version, ORDER BY, LIMIT
- Client-Side Attacks
- Create an XSS PoC (Proof of Concept)
- Basics of session hijacking i/c/w XSS
- Basic XSS filters
- Server Side Attacks
- RFI
- PHP shells such as r57 and c99
- Bind & Back connect shells

CISMP

1. Introduction & Overview:

- The business interest of information security.
- Customer perspective on governance.
- Supplier's responsibilities in security assurance.

2.Information Security Governance:

- Challenges and opportunities of effectively governing an organization's information security requirements and resources.
- Information security governance lays out the vision for the information security program.
- Security governance, and the development of an effective information security strategy and policy.
- how to improve information security accountability, regulatory compliance, and maturity

3.Risk Management:

- Principles of risk management.
- Risk Control factors
- Dealing with the remaining risks.

4. Developing a Security Strategy:

- How to develop an information security strategy
- Factors affecting Information security strategy
- Information security Management Responsibilities

5.Policies, Procedures, Standards & Guidelines:

- Introduction and Liability
- Policy Basics
- Policy Lifecycle
- Best Practices and Guidelines

6.Information Security Technology:

- Introduction to information security technology
- Trusted vs Untrusted technologies
- VLANs
- Information Encryptions

7.Incident Management:

- Overview of Information Security incident management
- Incident management response lifecycle preparation
- Intrusion detection technologies and systems
- Security incident response

8. Business Continuity & Disaster Recovery:

- Business continuity phases
- Disaster recovery
- Recovery strategies

9. Privacy & Data Protection Foundation:

- Privacy & Data Protection Fundamentals and Regulations
- Organizing Data Protection
- The practice of Data Protection

GSDC Technical Advisory Board :

The GSDC is the leading certification association which brings together innovative organizations and founding thought-leaders as Technical Advisors from over 40 countries to design curriculum on Blockchain, Devops, Six Sigma & Agile Certifications.

Our Future Information

Find out more online at www.gsdcouncil.org