Certified Information Security Management Practitioner

GSDC's Certified
Information Security
Management Practitioner
certification empowers
you to handle the security
management practices of
an organization.

GSDC
Global Skill Development Council

CISMP

CERTIFIED

Certified Information Security Management Practitioner

ABOUT CERTIFICATION

The way all the technologies are working together to make an organization's workflow easy, it is also creating a goldmine for hackers and cybercriminals. Information Security Management Practitioners take care of vulnerabilities and potential information threats in order to stop it.

Information Security typically involves preventing or at least reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents.

As a globally accredited qualification, the Certified Information Security Management Practitioner provides a perfect starting point for those who want to get into Information Security management, or for those who want to progress within their present role.

OBJECTIVES

The objective of Certified Information Security Management Practitioner Certification is to share a deep understanding of:

1. The benefits of Information Security Management
2. The need for Information security management
3. Information risk management
4. Information Security organization and responsibilities, legal and regulatory obligations
5. Policies, standards & procedures of delivering a balanced ISMS
6. Security procedures of a balanced ISMS
7. Information Security Governance, Policy reviews, security audits
8. Security incident management
9. Objectives and stages of incident management
10. Information Security implementation
11. Legal framework, Processing personal data, employment issues, computer misuse, intellectual property rights, Data Protection Act
12. Security standards and procedures: ISO/IEC 27002 and ISO/IEC 15408
13. Threats to, and vulnerabilities of, Information Systems

Our Accreditation:

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

COURSE SYLLABUS

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
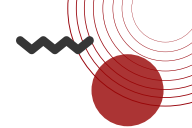
GSDC Technical Advisory Board :

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

Target Audience

- IT professionals
- Professionals working in the public sector
- Business professionals who require a deeper understanding of information security as part of their wider business knowledge

Pre-requisites

Certified Information Security Management Practitioner Certification demands no prerequisite as such.

Find out more online at
www.gsdcouncil.org