

Certified Information Security Management (ISO 27001) Foundation

www.gsdcouncil.org / info@gsdcouncil.org

GSDC's Certified Information Security Management (ISO 27001) Foundation Certification has an end goal to share the knowledge about controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities.



ABOUT CERTIFICATION

By extension, ISM includes information risk management, a process that involves the assessment of the risks an organization must deal with in the management and protection of assets, as well as the dissemination of the risks to all appropriate stakeholders.

This requires proper asset identification and valuation steps, including evaluating the value of confidentiality, integrity, availability, and replacement of assets.

As part of information security management, an organization may implement an information security management system and other best practices found in the ISO/IEC 27001 standards on information security.

The Information Security Management (ISO 27001) Foundation is specially curated to shape the professionals in a way that they can handle threats, vulnerabilities, and mitigation. This certification empowers the participants to create, implement, communicate and evaluate any organization's security policies, procedures, and objectives in order to achieve a better guarantee of an organization's overall information security.

OBJECTIVES

Certified Information Security Management (ISO 27001) Foundation Certification's main objective is to provide the participants with an understanding of:

- The range of application for an ISMS
- Information security-related legislation applicable to the country(s) of operation
- Techniques and tools used in information security management
- The potential business impacts of ISMS
- Importance of asset and owner identification
- Control objectives and how these are addressed
- Risk assessment and identification
- Threats, vulnerabilities, and impacts
- Difference between risk assessment and risk evaluation
- The methodology of risk treatment, application, residual risk and review of the risk treatment plan
- Importance of the statement of applicability in the ISMS, and how it is used
- Difference between an IS event and incident.

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.

COURSE SYLLABUS

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

PRE-REQUISITES

There is no such recommended experience required for getting this certification, only five years of direct full-time security professional work experience is required.

BENEFITS

After the completion of this certification, the participants will have access to:

- ✓ Practical knowledge of information security.
- ✓ Better job opportunities with enhanced credibility and marketability.
- ✓ Valuable resources like peer networking and idea exchange.
- ✓ A network of globally accredited industries and subject matter experts.
- ✓ Security information resources.
- ✓ Business and technology orientation to risk management.

EXAMINATION

- There will be online training followed by a multiple-choice exam of 40 marks.
- You need to acquire 26+ marks to clear the exam. If you fail, you can retake the exam after one day.
- In case Participant does not score passing percentage then they will be granted a 2nd attempt at no additional cost.
- Re-examination can be taken up to 30 days from the date of the 1st exam attempt.



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.

Further Information:

Target Audience

- Network professionals
- Security professionals
- Executives and managers who want to implement a security solution at the organizational level
- IT professionals who want to know about cybersecurity fundamentals, threats, mitigating controls, and organizational responsibilities
- Anyone who is looking forward to starting a career in cybersecurity.

Certification Available:

- Ethereum developer
- Blockchain Architect
- Hyperledger Developer

You may also be interested in:

- Lean Six Sigma
- DevOps Practitioner

Find out more online at www.gsdccouncil.org