

Certified Information Security Management (ISO 27001) Foundation



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.

Certified Information Security Management (ISO 27001) Foundation

ABOUT CERTIFICATION

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:

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

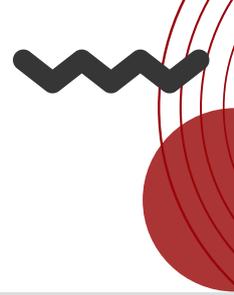
Our Accreditation:



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.

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 ABICB accredited member. Accreditation Board For International Certification Bodies's accreditation is globally recognized as the highest certification for training institutes as it is an independent autonomous body





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





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

- ISMS auditors, such as those employed/contracted by third-party certification/registration bodies and those involved in first or second-party ISMS audits.
- Information security practitioners, such as information security consultants, IT security managers and IT personnel.
- Employees conducting ISMS audits within their own organization (internal audits).

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.

Find out more online at
www.gsdccouncil.org

