

ISO/IEC 27032 Cyber Security Course

Course Duration: 40 Hrs.

Course Code: ISO27032-CSC

Course Overview

The ISO/IEC 27032 Cyber Security Course provides a comprehensive understanding of the international guidelines for cybersecurity based on ISO/IEC 27032. It equips participants with the knowledge to address modern cyber threats, safeguard critical information assets, and build trust in cyberspace. The course emphasizes the establishment of a robust cybersecurity framework that complements other security domains such as information security, network security, internet security, and critical information infrastructure protection.

What you'll learn?

Participants will gain insights into the fundamentals of cybersecurity, risk management, threat identification, and mitigation strategies. They will learn to implement ISO/IEC 27032 guidelines, coordinate incident response, develop cybersecurity strategies, and integrate best practices into organizational security frameworks. The course also covers collaboration between stakeholders to strengthen cyber resilience.

Target Audience

This course is designed for cybersecurity professionals, information security officers, IT managers, risk managers, consultants, and anyone responsible for protecting organizational assets against cyber threats. It is also suitable for professionals seeking to enhance their understanding of ISO/IEC 27032 and its practical application.

Pre-Requisites

A basic understanding of information security and risk management concepts is recommended. Prior experience in cybersecurity, IT governance, or related domains will be beneficial but not mandatory.

Course Content

Module 1: Introduction to ISO/IEC 27032 and cybersecurity fundamentals

Module 2: Cybersecurity principles, scope, and relationship with other security domains

Module 3: Identifying, analyzing, and managing cyber threats

Module 4: Risk assessment, mitigation, and security controls

Module 5: Cybersecurity policies, frameworks, and strategies

Module 6: Incident detection, response, and recovery planning

Module 7: Stakeholder collaboration and communication in cybersecurity

Module 8: Building trust, resilience, and continual improvement in cyberspace

Module 9: Case studies and practical applications of ISO/IEC 27032