Slide 1: Title Slide

Title: ISO/IEC 27001: Information Security Management System (ISMS)
Subtitle: Global Standard for Managing Information Security

Slide 2: What is ISO 27001?

ISO/IEC 27001 is an international standard for managing information security.

Published by ISO and IEC.

Defines the requirements for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS).

Slide 3: Why is ISO 27001 Important?

Data breaches and cyberattacks are increasing.

Regulatory requirements (e.g., GDPR, HIPAA) demand secure practices.

Builds trust with stakeholders by demonstrating commitment to data security.

Helps identify and mitigate security risks.

Slide 4: Core Objectives of ISO 27001

Confidentiality – Only authorized users can access data.

Integrity – Data remains accurate and complete.

Availability – Information is accessible when needed.

These are known as the CIA Triad in cybersecurity.

Slide 5: Key Principles of ISMS

Risk-based approach
Top management involvement
Continuous improvement
Documented processes and policies
Security controls based on risk appetite

Slide 6: ISO 27001 Structure (Annex SL format)

Follows the High-Level Structure (HLS) common to all modern ISO standards:

Scope

Normative References
Terms and Definitions
Context of the Organization
Leadership
Planning
Support
Operation
Performance Evaluation
Improvement

Slide 7: Annex A – 114 Controls (Now 93 in 2022 version)

Grouped into 4 control themes in ISO 27001:2022:

Organizational Controls
People Controls
Physical Controls
Technological Controls

Each control helps mitigate specific information security risks.

Slide 8: Examples of ISO 27001 Controls

A.5.12 – Classification of Information
A.6.1 – Responsibility for Information Security
A.9.2 – User Access Management
A.12.1 – Operational Procedures and Responsibilities
A.18.1 – Compliance with Legal Requirements

Slide 9: Benefits of ISO 27001 Implementation

Reduces security breaches
Demonstrates compliance
Enhances customer trust
Supports continuous improvement
Helps in winning business contracts
Provides clear roles and responsibilities

Slide 10: Certification Process

Gap Analysis (optional)
ISMS Implementation
Internal Audit
Management Review
Stage 1 Audit – Readiness review
Stage 2 Audit – Full compliance audit
Certification Issued

Surveillance Audits (typically yearly)

Slide 11: Challenges in ISO 27001 Implementation

High initial resource requirement
Cultural resistance to change
Misunderstanding of control scope
Continuous documentation and audits
Integration with other standards (e.g., ISO 9001)

Slide 12: Who Should Implement ISO 27001?

IT and Software Companies
Financial Institutions
Healthcare Providers
Government and Defense Agencies
E-commerce and Cloud Services
Any organization handling sensitive data

Slide 13: What's New in ISO 27001:2022?

Fewer controls (93 vs 114)
Control themes introduced
Emphasis on cloud services, data masking, threat intelligence, etc.
Easier integration with ISO 9001 and ISO 27701

Slide 14: Summary & Takeaways

ISO 27001 helps build a resilient information security framework

Enables compliance, customer trust, and risk management

2022 revision makes it more relevant to today's digital threats

A must-have for any organization handling critical or sensitive data