ISO

Shweta A. Chawla
Founder & Investigator
SC Cyber Solutions

SC
Cyber Solutions

ISO

- International Organisation of Standards
- ISO is an independent organization
- Develops and publishes international standards
- Not linked to any government
- ISO comes from the Greek word '*isos*' meaning *equal*
- Includes national standards bodies from 162 countries (eg: Bureau of Indian Standards)
- Individuals or companies cannot become members of ISO

shweta@sccybersolutions.com

SC
Cyber Solutions

ISO/IEC 27000

- Family of standards for information security management systems (ISMS)
- More than a dozen standards
- Jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005
- Revised in 2013
- European update in 2017

shweta@sccybersolutions.com

SC
Cyber Solutions

ISO/IEC 27001

- ISO/IEC 27001 requires that management:
  - Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
  - Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
  - Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

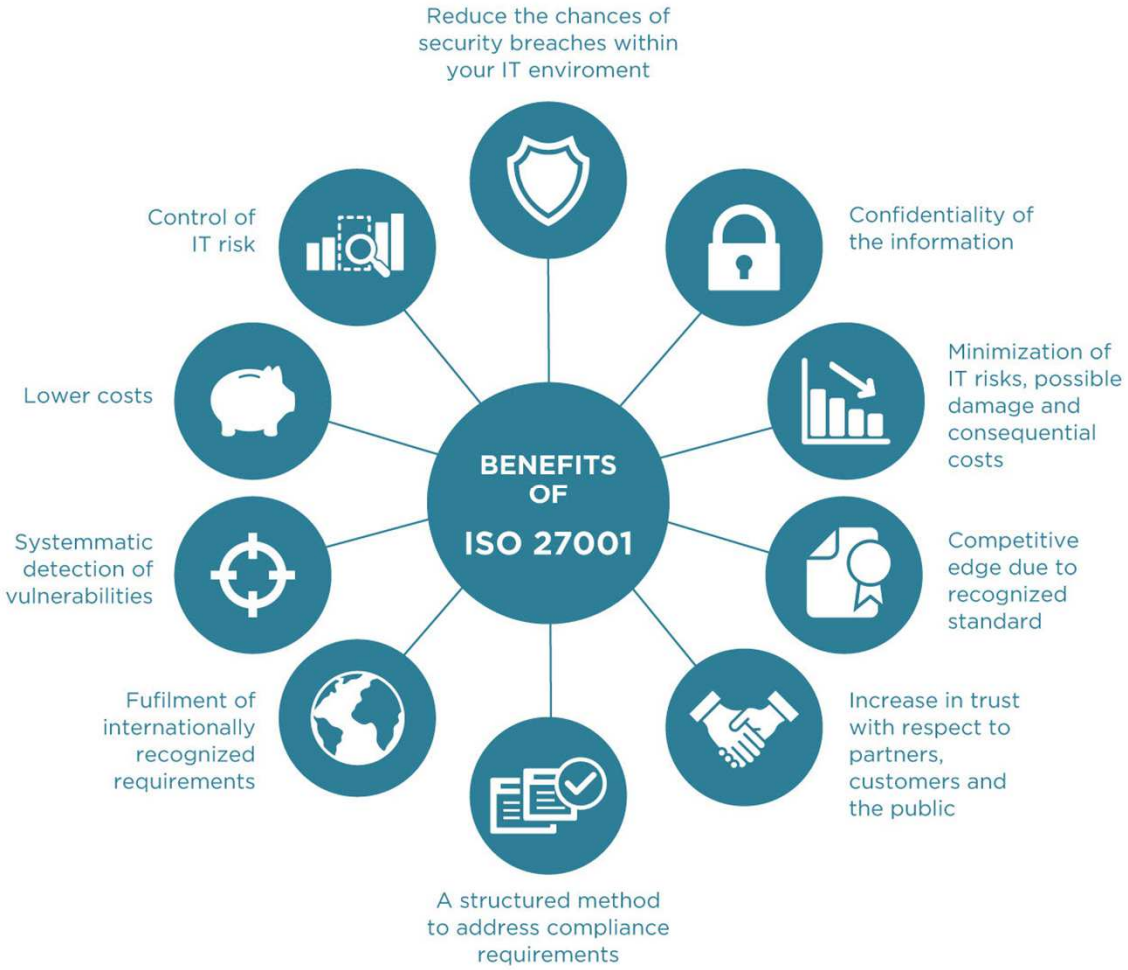
shweta@sccybersolutions.com

SC
Cyber Solutions

- Annex A of the standard provides a list of controls and their objectives
- 114 controls in 14 groups
- 35 control categories

shweta@sccybersolutions.com

SC
Cyber Solutions



shweta@sccybersolutions.com

SC
Cyber Solutions

- A.5: Information security policies (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security - 6 controls that are applied before, during, or after employment
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7 controls)
- A.14: System acquisition, development and maintenance (13 controls)
- A.15: Supplier relationships (5 controls)
- A.16: Information security incident management (7 controls)
- A.17: Information security aspects of business continuity management (4 controls)
- A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

shweta@sccybersolutions.com

SC
Cyber Solutions

shweta@sccybersolutions.com

SC Cyber Solutions

ISO/IEC 27001 Implementation Process

- Assemble an implementation team
- Develop the implementation plan
- Initiate the ISMS
- Define the ISMS scope
- Identify the security baseline
- Establish a risk management process
  - Establish a risk assessment framework
  - Identify risks
  - Analyse risks
  - Evaluate risks
  - Select risk management options
- Implement a risk treatment plan
- Measure, monitor and review
- Certify the ISMS

shweta@sccybersolutions.com

SC
Cyber Solutions

shweta@sccybersolutions.com

SC
Cyber Solutions

ISMS Methodology

shweta@sccybersolutions.com

Contact details:
Mob: +91 98230 80864
shweta@sccybersolutions.com
www.sccybersolutions.com
@sccs1300