

# Does your company comply with **current** security legislation?



Today, information is an important asset, which like other business assets, has a value to an organisation and therefore needs to be suitably protected.

Information leaks, to media and competitors, have become a widespread problem. These occur through members of the staff, the Internet, and many other sources. This happens despite the extensive measures implemented by companies and organizations to secure their computer systems. Approaching security from a technical perspective is usually not enough.

**News articles today** show an increase in the frequency of security breaches of confidential information.

- 153 million** User records.
- 412.2 million** User accounts.
- 137 million** User accounts.
- 145 million** Users accounts.
- 147.9 million** consumers

#### for information security...

Designed to protect something of value against unauthorized access and changes. ISO27001 refers to protection of information in terms of:

**Confidentiality** - only authorized users can gain access to relevant information.

**Integrity** - protection against unauthorized changes or damage; safeguarding the accuracy and completeness of the information.

**Availability** - information is available when required in the correct context.

#### ISO27001 an integrated service...

A company's management has always monitored its financial status. Lately, management systems for quality control, environmental and health & safety issues have also been implemented and followed up by management. Now, the time has come to add information security management.

#### ISO27001 benefits...

- Ensures** business continuity and minimizes business losses by protecting information from a wide range of threats.
- Demonstrates** compliance with the standard for information security in addition to helping companies safeguard vital information.
- Reputable** means for companies to benchmark their Information Security.
- Management** System (ISMS) through compliance.
- Brings** confidence to business partners who entrust information into the custody of the certified.
- Strengthens** the competitive edge of the company by creating trust in the firm, externally as well as internally.
- Motivates** management to demonstrate adherence to good security practice.

The central concepts of ISO27001 are to prevent, protect and record. The standard covers all types of information i.e., business-related as well as product-oriented. Digital information and paper documents are naturally included, but the individual person is also emphasized.

How does an organisation make sure that the competence of its staff is retained and developed? How does the company minimize loss of knowledge when someone leaves the company?

#### part 1: Requirements...

The primary objective of the management system is to safeguard information. The foundation of the process is to identify what information assets are to be protected and to what degree. The assets will include digital information, paper documents, and physical assets such as computers and networks, but the individual person must also be considered as an asset.

The following seven steps are required for Compliance or Certification:

- Developing an Information Security Policy.
- Defining a Scope Statement.
- Performing a Risk Assessment.
- Defining a Statement of Applicability.
- Developing a Business Continuity Plan.
- Developing and implementing the Management System.
- Completing a Compliance or Certification Audit.

#### part 2: Code of practice...

The following security controls are those that define the industry baseline of good security practice:

- Information security policies.
- Organization of information security.
- Human resource security.
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

#### your ISO27001 partner...

- We** have been involved with ISO27001 for 20 Years.
- All** our ISO27001 consultants are 3rd party auditors for the leading certification bodies.
- We** offer familiarization, implementation, and training in ISO27001 in addition to pre-audit assessments & gap analyses.
- We** have extensive experience in pre-assessment of ISMS.
- We** can assist in the selection of a certification body.

visit [www.parkinsonhowe.co.uk](http://www.parkinsonhowe.co.uk) for further information and case studies of previously completed projects.