Blackmores

ISO 27001 Information Security

Information Security affects the very core of a business. Customer records, financial information and intellectual property must be protected from loss, theft and damage. ISO 27001 provides the controls and processes your business needs.

Adopted by thousands of organisations across the world ISO 27001 is an auditable standard.
As well as delivering security improvements, auditing your processes has additional and valuable benefits:

- **Credibility, trust and confidence** - your customers can feel confident of your commitment to keeping their information safe.
- **Cost Savings** - the cost of a single information security breach can be significant. Registration reduces the risk of such cost being incurred and this is important to stakeholders and other investors in your business.
- **Compliance** - registration helps to show the authorities that you comply with the relevant laws and regulations.
- **Commitment** - registration helps to ensure and demonstrate commitment at all levels of the organisation.

Who is it relevant to?

The framework and processes deployed can be tuned to reflect different business needs. The value of information is different for every company large or small. The loss of a single piece of information could be insignificant or catastrophic, it is only by defining the true value of any potential loss and the value of access, that a balance can be struck. Controls and processes can be defined that mitigate any threat yet ensuring access is available and controlled to those who need it.

Large organisations such as banks and telecommunication companies will often hold detailed information on millions of customers, individuals or businesses. Keeping that information both secure from theft but accessible for day to day use are conflicting requirements. A smaller organisation may value a single customer record very highly. The issue of information security sees all organisations of all sizes and from all sectors with an identical problem – their inherent vulnerability.

ISO 27001 can be adopted by any organisation wishing to implement a formal procedure, which will help improve your physical and environmental security, delivering cost savings through a commitment to keeping your information safe and your customers confident of this fact. The standard is currently being driven typically by two areas of business - the public sector and the financial sector. Both are naturally concerned for the security of their information which may be held by their suppliers and partners.

A summary of ISO 27001

Put simply it's the most widely adopted security standard in the world.

ISO 27001 covers known security issues, containing many well considered control requirements and steers companies along a quantifiable path of assessments and improvements. Compliance shows that information security is being taken seriously and that effective steps are in place.

All organisations need to keep information safe and secure, some more than others. Comprehensive Information Security policies within organisations allow rules and procedures to be developed, safeguarding information such as corporate information and customer information. An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information, ensuring it remains both secure and available. It encompasses people, processes and IT systems.

ISO 27001 is a standard setting out the requirements for an Information Security Management System. It helps identify, manage and quantify the range of threats to which information is regularly subjected.

Annex A of ISO 27001 identifies 10 controls:

- Security policy - This provides management direction and support for information security
- Organisation of assets and resources - To help you manage information security within the organisation
- Asset classification and control - To help you identify your assets and appropriately protect them
- Personnel security - To reduce the risks of human error, theft, fraud or misuse of facilities
- Physical and environmental security - To prevent unauthorised access, damage and interference to business premises and information
- Communications and operations management - To ensure the correct and secure operation of information processing facilities
- Access control - To control access to information
- Systems development and maintenance - To ensure that security is built into information systems
- Business continuity management - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
- Compliance - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement