

SAPPHIRE

## Information Security Management: the importance of ISO 27001 compliance

### What is ISO 27001?

ISO 27001 2005 is the de-facto international standard on establishing, maintaining and improving an Information Security Management System (ISMS) for both public and private sector organisations.

What is the Standard designed to do?

- Identify an organisation's information assets
- Identify the threats to those assets
- Identify the vulnerabilities that might be exploited by those threats
- Identify the impact on an organisation if the loss of confidentiality, integrity or availability (CIA) of any asset was to occur.

If an organisation works towards compliance with ISO 27001 appropriate controls can be identified and implemented to **manage the vulnerability** and lower the risk of the threat to the organisation's assets.

### What does committing to establishing an ISMS involve?

By developing an ISMS an organisation expresses its commitment to establishing an appropriate information security framework that:

- ensures that a high level information security policy is written
- creates an organisational structure to ensure that roles and responsibilities are established
- assures the organisation that personnel security issues are highlighted
- confirms that an information assets register is created
- validates the adequacy of physical & environmental security arrangements
- substantiates the adequacy of IT technical security measures – including communications and operational procedures; logical access controls; systems development/maintenance arrangements; and vulnerability management
- establishes an effective incident management process
- validates the existence or adequacy of business continuity arrangements
- ensures that there is an ongoing compliance and monitoring mechanism in place

### What

ISO/IEC 27001 is the certification process for the Code of Practice on Information Security Management.

### Who

All organisations, in public or private sectors are increasingly required to prove that they take information security seriously.

### Why

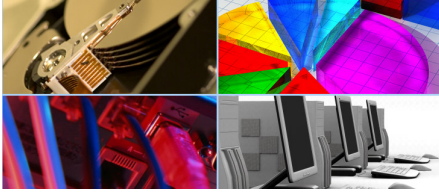
ISO/IEC 27001 is respected as the 'de facto' standard and will soon become a contractual or service level agreement requirement.

### *What our clients say*

*"Do not rely on a slice of luck to protect your IS or hook into bad procedures. Use best practice standards for an assured result."*

**Harvey Mattinson,**  
*Head of Accreditation,  
Cabinet Office*

Sapphire  
Globe House  
Stockton-on-Tees  
Cleveland  
TS20 2AB  
01642 702100



## Why compliance is important for business or service benefit?

1. By having a formal documented ISMS which has been independently assessed, an organisation can demonstrate to its customers and clients that they are committed to security, and have the ability to handle information in a secure manner.
2. This in turn may negate the need for their customers to spend time and allocate resources in carrying out their own independent audits. Equally customer confidence can improve, thereby increasing trust in your brand or image.
3. There may also be contractual or service level requirements that an organisation works in accordance with ISO 27001.
4. In respect to public sector bodies, there is a requirement for government bodies to have their critical systems compliant and for other public organisations, the government are persuading them to become compliant.
5. The ability to respond quickly to any information security breaches or incidents is one of the key clauses in ISO27001. The ability to minimise the opportunity to incidents to occur is a major advantage for business/service resilience. It also links closely with IT Disaster and Business Continuity work

## The Future

Organisations need to realise the information risks is the fastest growing risk issue. Continuous monitoring for constant vigilance is now a business or service necessity and a culture of security is vital for organisations to survive in the modern world.

A government survey shows that the number of malicious security breaches on websites by cyber attackers has almost doubled in the last year - 2005 DTI Information Security Breaches Survey found that 44% of organisations questioned had been attacked. This compares to 24% who reported security breaches in 2004.

Therefore, gaining compliance to ISO27001 ensures that you can prove that confidentiality, integrity and availability of information is adequately addressed – to be seen as a trusted organisation is proving crucial in our fast moving world.