



SERVICE BRIEFING: ISO 27001 & ISO 17799 COMPLIANCE

Why comply?

ISO 27001 and ISO 17799 are both internationally recognised standards for managing and implementing information security within an organisation, system or process.

Certification to the ISO 27001 standard provides an effective and recognised measure of how well an organisation manages its information security, perusing certification is not only useful as an internal gauge within your organisation but it is also an effective selling point, can be a deal breaker when tendering for contracts with customers, and can boost your organisation's image by demonstrating your organisation's commitment to effective security management (much like its counterpart standard ISO 9001 is for quality).

Our Approach

Safecomms UK has proven experience taking large to small organisations through the process of being compliant or certified to the ISO 27001 standard. We provide services to both assess the current compliance to the standard as well as helping the organisation plan and implement the actions necessary to become compliant or certified, This includes:

- Performing a gap analysis of the current infrastructure
- Establishing a sound scope for the ISMS (Information Security Management System)
- Performing a risk assessment and developing risk treatment plan
- Developing a Statement of Applicability (SoA)
- Producing and/or improving policies, procedures and standards
- Helping the organisation through the certification audit

By working with Safecomms your organisation can leverage the specialist knowledge of Safecomms' consultants, and minimise the time required to be complaint or certify to ISO 27001 and ISO 17799 by leveraging pre-made Safecomms material (e.g. policies, checklists etc.). Ultimately, working with Safecomms to achieve certification against ISO27001 can be more cost effective than trying to achieve compliance without help.

Understanding the various standards

Given the recent changes to the standards, it is easy to be confused as to exactly what one standard does and the differences between them. Here is a brief summary of the various standards:

BS7799 Part 1 – An old standard (superseded by ISO 17799) was developed by the British Standards Institute (BSI) to provided a comprehensive number of security controls for organisations (e.g. anti-virus, incident handling, business continuity planning).

ISO 17799 – This current standard is essentially an internationalised version of the BS7799 Part 1 standard (albeit with some minor changes).

BS7799 Part 2 – A retired standard (superseded by ISO 27001) which provided a framework on how an organisation should manage its information security (ISMS).

ISO 27001 – A new standard is based on BS 7799 Part 2, and like its ISO 17799 counterpart essentially has the same content as the BSI equivalent. ISO 27001 standard can be certified against by accredited auditors in the UK (i.e. enables the complaint organisation to claim to be certified against the standard)

Both ISO 27001 and ISO 17799 are companion standards: whilst ISO 27001 discussed how to manage information security, ISO 1779 discusses what is need in terms of actual security controls. Certification against ISO 27001 cannot be achieved without at least applying some of the controls outlined in ISO 17799.



Demonstrating compliance to ISO 17799 or certifying against ISO 2700 can be a difficult process, Safecomms has experienced security consultants to help you through.

Contact Safecomms

Tel: +44 1223 576 044
Fax: +44 870 836 2157

info@safecomms.co.uk

16 Millers Yard,
Mill Lane
Cambridge, CB2 1RQ
United Kingdom

