

ISO27000/BS7799

[commissum - that which is entrusted]

commissum works with you to provide expert independent assessment, mentoring and support to establish a security management framework based upon an implementation of ISO27000/BS7799 appropriate to your organisation

issues

ISO27000/BS7799 is the internationally accepted set of standards for Information Security Management. Organisations of all sizes have identified the value of compliance, either pursuing formal certification through accreditation agencies, or adopting the standard through implementing ISO27000/BS7799 as their guiding framework for internal security management.

This has been reinforced by a number of regulating agencies declaring ISO27000/BS7799 as their benchmark for prudent and competent practice, including the UK Data Protection Commissioner. There is also growing support within government contracting circles for ISO27000/BS7799 as a preferred standard; that this may in future be mandated should also be considered in some sectors.

It can be difficult for an enterprise to make objective, well informed decisions about how to cost effectively adopt the standard and whether to seek formal certification. It is a sensible first step to engage **commissum** to conduct an independent, expert review to assess how current practices match up to the standard and compare with accepted industry practice.

Combining extensive cross-industry experience with a collaborative approach, **commissum** is then able to assist the organisation in establishing an Information Security Management Framework that is appropriate to their business needs. Support is available as long as required, with the organisation becoming empowered through skills transfer to manage security internally.

approach

The pressures are obviously building to comply with ISO27000, but the scope is wide, and experienced, professional interpretation and guidance is essential for effective and economical application. An assignment usually starts with a state of readiness assessment and report; essentially a top level audit to identify an implementation of ISO27000/BS7799 appropriate to the organisation; outlining improvements required to achieve this. This is followed by a plan of action that establishes a roadmap to the level of compliance required with short term remedial actions to address any higher priority risks identified.

- review business drivers and risk posture of organisation
- advise on & agree the scope of the Information Security Management System (ISMS)
- identification of business critical assets & a risk assessment against these
- review controls (interview, observation, inspection) i.e. gap analysis
- information Security Management status report & findings workshop – agree gap analysis
- establish roadmap and risk treatment plan; including identification of appropriate control objectives
- define Statement of Applicability
- support through implementing a programme of improvement to establish a formal ISO27000/BS7799 based ISMS

customer benefits

Provision of an expert, independent assessment of the gap between current Security Management and an implementation of ISO27000/BS7799 appropriate to the customer's organisation.

- recommendations on business areas, systems and processes requiring improvements in security based upon industry best practice
- statement of achievement and shortfall in ISO27001/BS7799 control areas relevant to the business
- roadmap and plan of activities for ISO27001/BS7799 compliance
- expert comment on the advisability of seeking formal ISO27001/BS7799 certification
- ongoing support through establishing a formalised Information Security Management System (ISMS)
- mentoring and guidance to empower the client's staff to establish an effective security culture

“Are you sure it's safe?”

Dr William Palmer (1824 -1856)
Convicted of poisoning and sentenced to hang, as he stepped up to the gallows.