Thinking About ISO17799?

ISO17799 has been with us for a number of years now and provides a good basis for IT control within an organisation. In recent years, government departments have taken to specifying 'compliance with' the standard as a prerequisite in tenders, particularly in relation to IT systems and services.

Initially the standard was adopted by the financial sector, which traditionally has had information security to the fore of its business operations. However, of late more and more departments, and organisations in general, have embarked on the road to compliance with ISO17799 themselves.

So what does compliance, and indeed certification, with ISO17799 involve and more significantly, why undertake what can sometimes be viewed as an onerous task to take on?

Advantages of ISO17799

- Structured approach to risk assessment and management
- Constructive and logical way to identify and implement controls
- Effective and efficient auditing and monitoring of IT risks and controls
- Recognised standard by the Comptroller and Auditor General and both internal and external auditors
- If adopted will assist in legal and regulatory compliance such as Data Protection Act 1988/2003, Copyright and Related Acts 2000 and Sarbanes Oxley.

Implementing ISO17799

The important thing to keep in mind when considering ISO17799 is that you only need to implement those elements of the standard that are applicable to the organisation, department or function seeking compliance/certification.

One approach to starting ISO17799 is to complete a gap analysis of your current status against the standard. This can be as simple as compiling a spreadsheet of the controls outlined in the standard and traffic lighting the standards in terms of compliant, nearly compliant or non-compliant.

The next step is to identify action tasks to be completed for nearly and non-compliant items. These tasks would form the basis of a project plan against which resources and timescales can be assigned.

One overriding requirement of the standard is a formal approach to risk assessment and management. Firstly, It is imperative that you know the risks to the organisation that you need to eliminate or address with the implementation of appropriate controls and/or countermeasures. Secondly, you will need to put in place a risk management review process to ensure that the risks are being managed on an ongoing basis.

In summary, ISO17799 can be an effective and efficient way to implement risk management and formalise controls within an organisation. Completing an initial gap analysis is a good way to see how prepared you are. In general, organisations tend to have a certain level of controls currently in operation, and consequently the adoption of ISO17799 would not be such a significant task as it may initially appear. The standard will help in formalising these good practices and identifying any additional requirements.