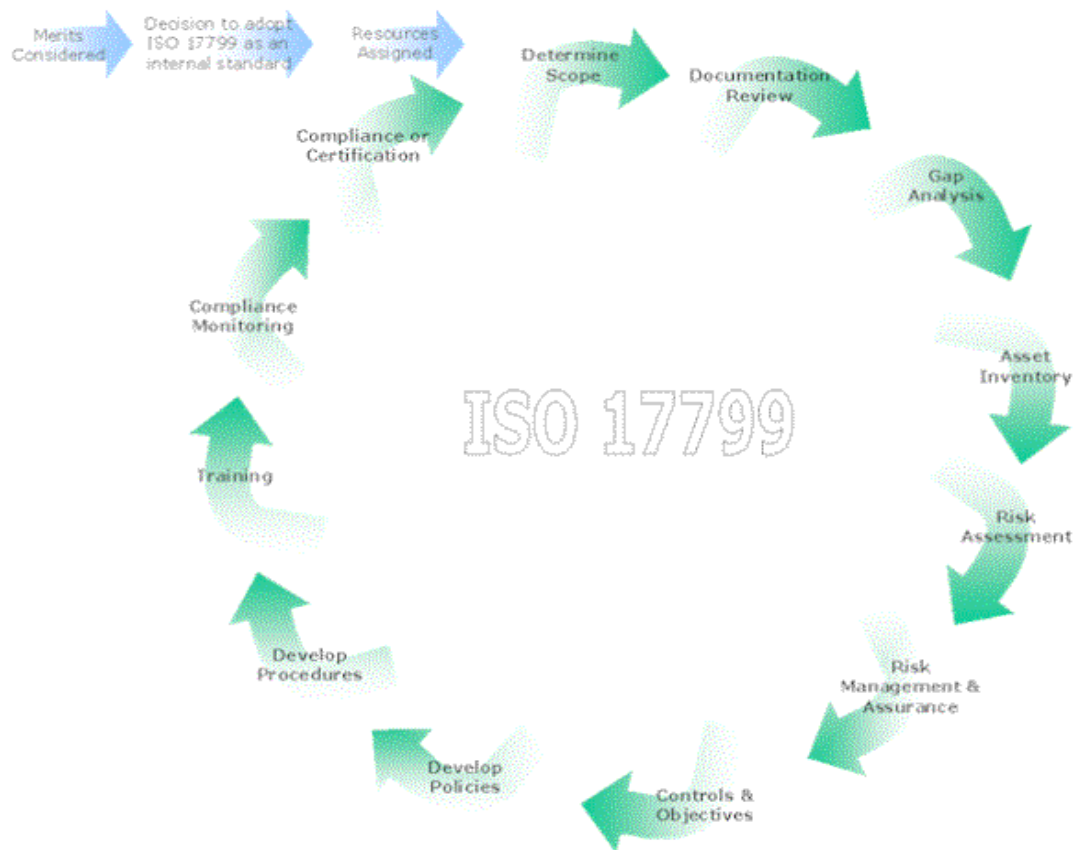


Full Cycle ISO 17799

T3i's Information Security White Pages Series
- September of 2005

The full cycle, from consideration of the standard's merits through to actual implementation, is depicted in figure 1 below.



The cycle depicted in figure 1 (above) outlines the typical stages that would be followed when adopting ISO 17799 as an internal standard. These stages are detailed in the points below:

- The merits of the standard are considered, such as enhancing the security of the organization, as well as the confidence of new/existing customers and business partners.
- A decision is made to implement ISO 17799. It may be the case that the organization wishes to simply become compliant by adhering to the standard, or it may mean that certification is sought.

- Resources in terms of people and time are allocated for the project. Assistance may be sought from an experienced ISO 17799 consultant at this stage.
- The scope of the ISMS is determined. This means that the area/s of the organization to be measured against the standard are selected. This should be a reasonable representation of the organization's activities.
- A review of existing documentation takes place to assess the extent of measures already in place, such as the ISO 9000 quality manual and security policies.
- A gap analysis is undertaken to identify the gaps between existing and required controls, processes and procedures.
- An inventory is taken of all relevant information assets.
- A risk assessment is carried out in order to determine the extent of risk to the ISMS, often comparing impact of risks with the likelihood of these risks actually occurring. A Risk Assessment document is the resulting deliverable.
- Once risks have been identified and established in the Risk Assessment document, the organization must decide how such risks are to be managed. From these decisions, responsibilities for managing these risks are determined and documented.
- Appropriate controls and objectives to be implemented are selected, either from the standard, or not, as the case may be. The standard does not contain an exhaustive list, and additional controls and objectives may be selected. A Statement of Applicability (SoA) is the resulting deliverable following selection of controls.
- Policies are created based on the SoA.
- Relevant procedures based on the policy definitions and guidelines are created and documented.
- A training program is undertaken to educate all employees to ensure that good practice for Information Security is adopted throughout the business.
- A program of compliance monitoring is implemented. This is to ensure that the good work achieved to date is maintained.
- Once compliance has been achieved, certification may be optionally sought from an accredited body. This requires an audit, which will examine the organization's adherence to the standard. A successful audit result will mean that the organization will gain certification.

About T3i, Inc. www.t3i.com

An Atlanta based company; T3i is a leading provider of services designed to protect information assets and critical infrastructure, as well as insure regulatory compliance as it pertains to information security. T3i's holistic approach to safeguarding information assets uses industry standards and best practices combined with a common sense approach to meeting regulatory requirements in a way that aligns with the needs of your business.