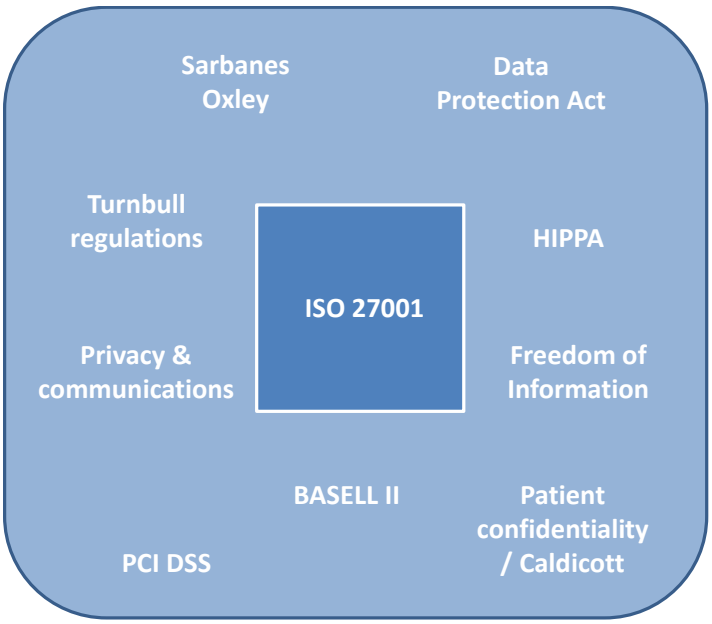
AdviSec Ltd

Compliance

Aims

The introduction of Information Communications Technology (ICT) into organisations over the last 20-30 years has resulted in many benefits to society. Moreover, organisations today are more reliant than ever on ICT to support 'front and back office' tasks, including exchanging information and transaction processing with regard to clients and suppliers.

Unfortunately, the growth in ICT has brought about increased opportunities to cause 'major' problems to business, Government, and the citizen. In response to these problems new legislation, regulations, standards and policies have been created with organisations obliged to comply and senior management held responsible for any failures.



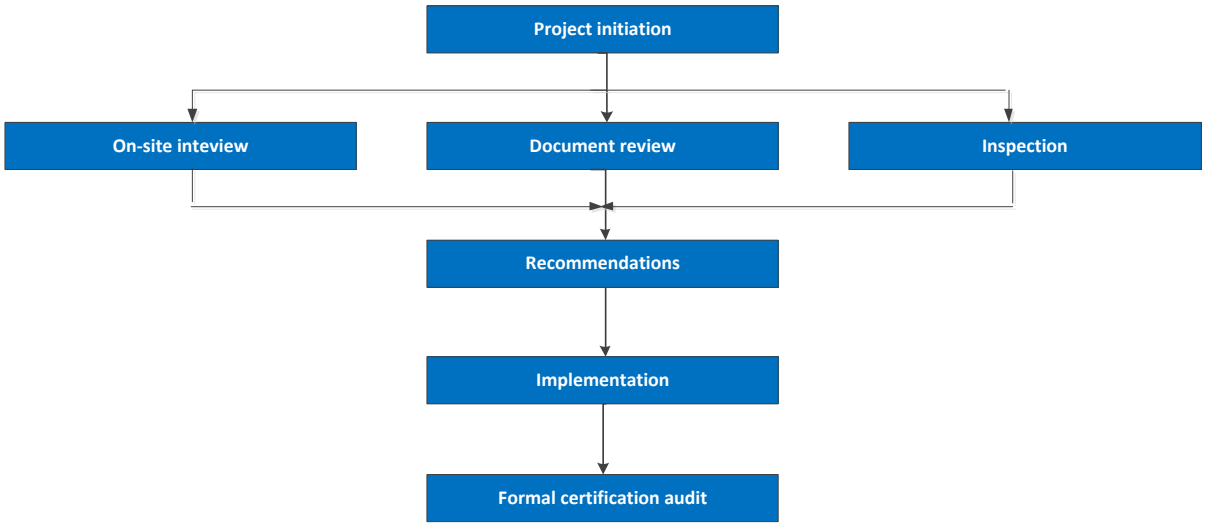
Whilst the aims and objectives of the legislation and regulations are admirable, it is the case that there is significant overlap between the different legislation and regulations. Moreover, organisations continue to spend large sums of money through separate compliance projects.

ISO 27001 is the foremost security standard available today. The standard is increasingly being referenced within legislation and regulations which serves to offer organisations the opportunity of addressing security requirements within a single project.

Advisec provides a compliance service for ISO 27001.

Client Engagement

At its simplest, undertaking a ISO 27001 compliance project involves the following tasks, as illustrated in the flow chart overleaf:



Experience has taught Advisec, however, that a more iterative and flexible approach is usually required, and this is based on the fact that a comprehensive gap analysis cannot be completed if there are a significant number of outstanding major non-compliances. Therefore, our consultants undertake an 'initial' gap analysis (two-three days) focusing on the requirements to which 'major' non-compliances could be attributable (e.g. management framework, security policy, organisation). At this point either:

- There are no 'major' non-compliances and the gap analysis continues

or

- Recommendations to address non compliances are identified, and then subsequently implemented. Only then does the gap analysis continue.

A gap analysis should take full account of the requirements for a management framework and security controls, which themselves are based on the outcome of a risk assessment. In addition, third party/outsourcing arrangements may also be included in the gap analysis (depending upon the proposed scope of the ISMS).

In preparing recommendations to address non-compliances, our consultants liaise with Client representatives to ensure that the following points are taken into account:

- Client ICT strategy
- Requirement to align with existing business processes and policy
- Requirement to 're-use' investment in existing technology, processes and procedures
- Resource constraints (i.e. people, money)
- Third party contracts
- Legislation and regulations.

Advisec offers a wide range of security related services and is ideally positioned to implement most recommendations, applying to both 'old' and 'new' technologies. Security-related services include:

- Secure design: Enabling the application of established and 'leading edge' technology by advising on the design and configuration of suitable security solutions
- Procurement services, including development and negotiation of security and BCP/DR schedules
- ICT infrastructure security reviews, i.e. gap analysis, penetration testing, network audit and risk assessment
- Accreditation services, for example GSI, CJX and NHSnet/N3
- Security policy, procedures and awareness/education
- Business Continuity and Disaster Recovery Planning.

Where the Client chooses to employ a third party to address non-compliances then Advisec will be pleased to recommend 'good quality' companies, together with an estimate of the cost(s) that the Client should expect to pay.

Outputs

The deliverables from this type of project are:

- ISO 27001 certificate (if applicable)
- Gap analysis report (including 'Statement of Applicability' and recommendations)
- Proposal(s) from Advisec to implement recommendations
- Results of implementing the proposal(s).

Benefits to Clients

Advisec delivers a professional service based on vendor independence, highly skilled consultants (CLAS, CISSP and BS7799 auditors), and underpinned by the knowledge and experience gained through having undertaken several engagements of this type.

Charging Basis

The following table indicates the effort required by organisations to comply with ISO 27001:

	CURRENT STANDARD OF SECURITY		
ORGANISATION	'Poor'	'Average'	'Good'
Multi-national (several sites) or >1001 staff	12	9	7
Single site or <50 staff	20	15	10
2-3 sites or 51-200 staff	35	25	20
>3 sites in the UK or 201-1000 staff	60	45	30

Contact us:

Further details, including case studies, presentations and references are available from Nigel Strutt. Please call 01869 388011 or 07780 526195. Head office; 41, Barry Avenue, Bicester, Oxfordshire. OX26 2DZ. Email: nigel.strutt@advisec.co.uk