AdviSec Ltd

Security Documentation

Aims

Many Government and commercial organisations operate a seemingly effective security solution, but without documenting their policy and procedures, or implementing a security awareness programme. Advisec Ltd believes this approach to be folly, and our position is based not only on the knowledge gained from investigating the cause(s) of actual security incidents, but also knowing that compliance with the ISO 27001 security standard necessitates having a comprehensive security documentation set, that is routinely disseminated to members of staff.

Client Engagement

This service is usually requested following the outcome of a security review or audit, and the identification of weaknesses with regard to the Client organisation's documentation set.

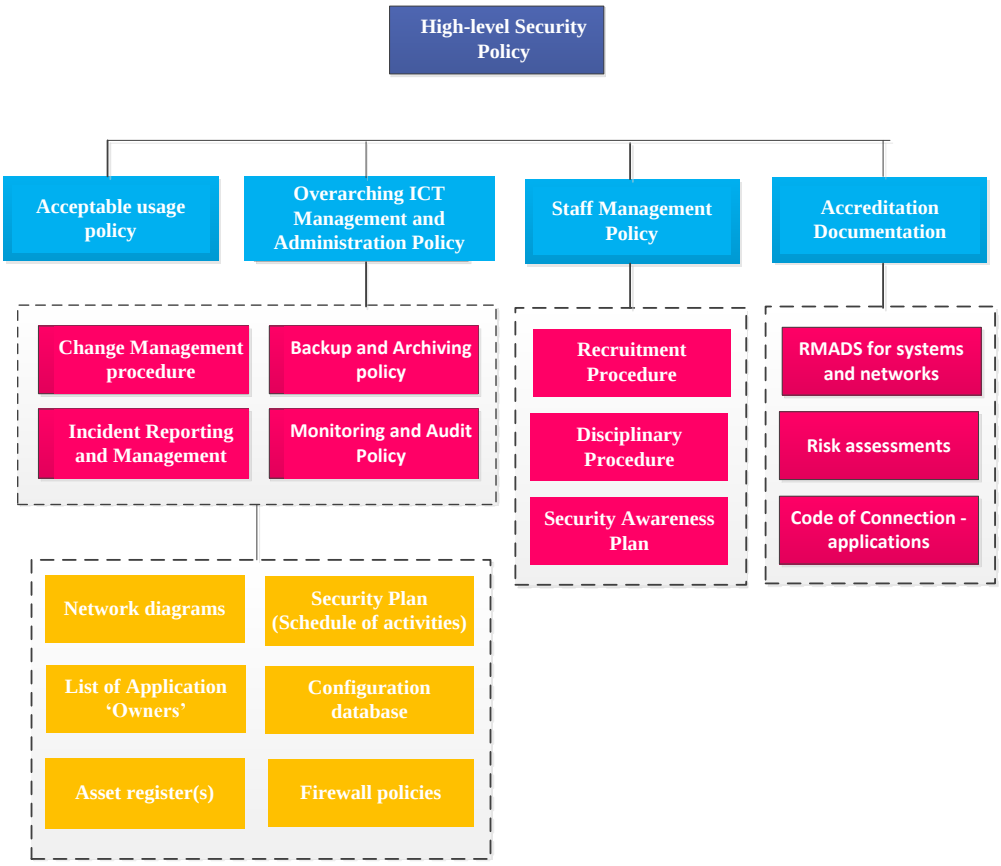
Our consultants have considerable experience in delivering this service across all business sectors (Enterprise, Public Sector and Telecoms), and together with its repository of templates, is ideally positioned to develop a documentation set in a timely and cost effective manner.

Key requirements:

- Re-use existing investment (if possible)
- Align documentation with the Client's organisational structure, and business processes (without contravening 'best practice')
- Content should comply with legislation and regulations
- Engage Client representatives during the development and review phases of the project
- Awareness methods reflect the opportunities and constraints to educate staff members.

Consideration of Business Issues

The following diagram illustrates a security documentation structure, however, it should be noted that this is not a 'one solution fits all' service.



Consideration of Technology Issues

Particularly with regard to the management and administration of ICT, there is a requirement to ensure that the procedures (and work instructions and check lists) are sufficiently detailed for tasks to be undertaken without employing the services of an 'expert'. Furthermore, the procedures should cover all business applications and ICT infrastructure components.

Process and Execution

Our consultants usually begin delivery of this service by requesting, and subsequently reviewing, any existing documentation made available by the Client. There then follows discussions with representatives from the Client organisation to define a security documentation structure, including:

- Senior representative from the Human Resources department
- ICT manager
- Information Security officer (ISO)
- Quality assurance department / Internal audit.

At this point consultants and the Client need to agree the resource provision to complete the project.

Consultants then set about producing the content, whilst working at least 50% of their time on-site. This step requires on-going consultation with Client representatives, and ultimately leads to the requirement for Client review and approval. Note several iterations of each document may be necessary before approval is granted.

There will be occasions when Client representatives are required to develop documentation in support of the overall project, and this typically will be at the 'work instruction' level, e.g. 'steps for building new Windows XP workstation', or 'steps for the daily checking of error logs for failures'. Advisec shall, of course, identify the required documentation, oversee its production, and undertake a quality review.

Outputs

A security documentation set which is sufficiently comprehensive to comply with ISO 27001 and PCI DSS.

Documentation will be made available via a secure FTP site and in hard copy format (if required).

Following the development of a documentation set our consultants will raise the matters of:

- Awareness, and in particular, the strategies and techniques available to disseminate key points contained in the likes of the ‘Acceptable Usage Policy’ to members of staff

- Advisec Ltd provides specialist advice and implementation services with regard to secure document management systems, and have done so for several ‘high profile’ Clients.

Further information is available on request.

Benefits to Clients

Advisec delivers a professional service based on vendor independence, highly skilled consultants (CLAS, CISSP and ISO 27001 auditors), and underpinned by the knowledge and experience gained through having undertaken several engagements of this type. The Client may rest assured of receiving a:

- High quality documentation set that is 'fit for purpose'
- Cost effective and timely service

Charging Basis

The table below indicates the effort required by Advisec to develop a security documentation set:

	Quality and Coverage of Existing Security Documentation		
ORGANISATION	'Poor'	'Average'	'Good'
Multi-national (several sites) or >1001 staff	12	9	5
Single site or <50 staff	16	12	7
2-3 sites or 51-200 staff	20	15	9
>3 sites in the UK or 201-1000 staff	24	18	11

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