AdviSec Ltd

Initial risk assessment & Gap analysis

Aims

This service represents a ‘quick’ assessment of the protection afforded by ICT infrastructure operated by Government sector and Emergency Service organisations, to safeguard information and application assets. The assessment is based on Infosec Standard No. 1, and includes

- Gap analysis with regard to the ‘Baseline Countermeasure Set’ (for systems up to RESTRICTED)
- Risk assessment where ‘gaps’ are identified
- Identification of recommendations to mitigate any risks at ‘Medium’ and above.

Process and Execution

Step 1

In conducting this type of engagement it is important to understand the business objectives and the processes that are in-place to achieve those objectives. Next it is important to understand ‘how’ the business processes are currently implemented, and in particular what ICT infrastructure is used.

This information is gathered through a series of stakeholder meetings.

Step 2

Complete a ‘gap analysis’ with respect to the Baseline Countermeasure Set which is required for systems operating at RESTRICTED, for example:

ISO27001 Security Objective	Control for Baseline Level - Implementation Guidance	Compliance	Residual risk	Scope for concern (if applicable)
5 Security Policy	**Baseline Set**			
5.1 Information security policy				
5.1.1 Information security policy document	An Information security policy document **must** be developed and implemented. This **must** be made available internally within the organisation and referenced in the overall business plan in accordance with the SPF Mandatory Requirement (MR) 6. Further guidance on the development of an Information Security Policy is provided in IS 2.	Partial Compliance	Medium	General

Where gaps do exist (i.e. non or partial compliances) assess the risk and the scope of the concern.

Step 3 (if appropriate)

Complete a 'gap analysis' with respect to the Segmentation model at 'Detect and Resist' which is required for systems operating at CONFIDENTIAL.

Step 4

Make recommendation for security controls to address risks at Medium and above, structuring the recommendations under the following headings:

- Organisation
- Documentation
- Physical
- Personnel
- Technical
- Review and audit

Step 5

Draft report ……. ensuring that the stakeholder feedback is anonymous.

Seek reviews and 'buy-in' from the Client organisation.

Outputs

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

Benefits to Clients

Advisec delivers a professional service based on vendor independence, highly skilled consultants (CLAS, CISSP, Certified Ethical Hackers (CEH) and ISO 27001 auditors), and underpinned by the knowledge and experience gained through having undertaken several engagements of this type.

The report provides a valuable insight into the 'major' non-compliances / issues and risks that exist within the Client organisation, together with recommendations.

Charging Basis

Six days effort required.

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