



SERVICE BRIEFING: ASSESSMENT & GAP ANALYSIS

Objectives

There are generally three objectives in this type of project:

- i. To assess the current state of the client's information security regime against an appropriate benchmark
- ii. To create a definitive gap analysis detailing any non compliance of the current state with the benchmark
- iii. To identify and document the smartest and most cost effective ways of closing the gaps

Scope

The scope of the assessment will cover all "controls" (both technical and procedural) necessary to ensure that an appropriate level of security is in place to protect the availability of critical IT systems and data, and to protect the confidentiality and integrity of data across the organisation. Where the benchmark for the assessment is mandated (e.g. ISO 17799) then this will determine the scope of the assessment.

The control functions examined will typically include (as a minimum) the following:

- Network access controls (internal & remote)
 - Patch management
 - Anti virus
 - Physical security controls
 - Security device configurations
 - Security incident management
 - IT asset management
 - Education and control of users
 - Information classification and associated controls
- Security incident management
- Network architecture and segmentation
 - Back up & DR procedures
 - Education and control of users
 - Procedures for ensuring the security of web applications & services

Methodology


The methodology will typically comprise the following steps:

- i. Review of existing documentation (policies and procedures, network diagrams, rule sets of security devices, logs etc.)
- ii. Structured interviews with key personnel responsible for the day to day implementation of security controls
- iii. Structured interviews with senior executives to determine the risk profile of the organisation
- iv. Running a series of tests to ascertain the effectiveness of critical technical controls across the organisation
- v. Writing and presenting report (with graphic gap analysis) to client and advising on issues arising

Deliverables

The deliverables will generally comprise

- i. an Executive Summary explaining the key findings of the assessment in plain English, written from a risk management perspective and aimed at non technical senior management
- ii. detailed findings arising from the assessment of each control, explaining and classifying the risks associated with each finding and recommending the smartest and most cost effective remediation steps
- iii. a graphic gap analysis clearly showing the gap between the current state and the benchmark state.



Regulators, legislators, stakeholders, and business partners now expect organisations to have an appropriate level of security in place. Where do you stand?

Contact Safecomms

Tel: +44 1223 576 044
Fax: +44 870 836 2157

info@safecomms.co.uk

16 Millers Yard,
Mill Lane
Cambridge, CB2 1RQ
United Kingdom

