

security healthcheck

[commissum - that which is entrusted]

The Security Healthcheck is a broad-spectrum assessment of security, using ISO27000/BS7799 as a guiding framework. The Healthcheck should be considered a minimum starting point for any organisation to ensure commercial and legal responsibilities are addressed

issues

Information security is a real issue, increasingly being recognised by both exposure in the press and hard lessons learned by organisations. Any organisation using modern networked Information Systems is at risk to some extent; the key is ensuring appropriate measures are taken to ensure that any risks are either accepted, reduced, or mitigated to a level that is appropriate to their business, taking into account:

- assets to be protected and their relative value to the organisation
- risks applicable to your business context
- understanding of the impact that risks may have on the confidentiality, integrity, or availability of Information Assets
- understanding the more intangible impact that risks may have on reputation, brand, or internal morale

It can be difficult for any enterprise to make objective, well informed decisions on how to address the need to adopt measures that strike an optimum balance between effectiveness and cost.

The Healthcheck enables an organisation to achieve this through a broad-spectrum assessment of security, using ISO27000/BS7799 as a guiding framework. The Healthcheck should be considered the minimum starting point for any organisation to ensure commercial and legal responsibilities are addressed.

approach

The Healthcheck combines inspection, interview and observation to draw up a cross enterprise picture of the effectiveness of a wide range of Information Security controls with recommendations for improvement.

The essential elements are:

- impact analysis - sets the standard for security achievement based on pain suffered if security fails
- interviews - meetings with key business staff to identify and evaluate security controls
- inspection - visit and review of significant locations and facilities
- documentation overview - completeness and effectiveness of policies and procedures
- analyse & report - analysis of data and findings followed by a report presenting conclusions and recommendations
- roadmap – assisting the enterprise in establishing a focused plan of action, addressing both short term essential remedial action and longer term establishment of a programme of continuous improvement

customer benefits

commissum provides you with an expert, independent assessment of how current practice and security measures match up to accepted good practice.

commissum consultants work with you to lay the essential early foundations for a sustainable, well planned, Information Security Management Programme, striking the balance between risk mitigation and business priorities.

- ISO27000/BS7799 provides a proven and comprehensive scoping framework
- statement of achievement and shortfall in ISO27001/BS7799 control areas relevant to the business
- objectives are set and agreed early in the exercise through the impact analysis
- targets for good security practice are defined – relevant to the organisation and its business environment
- standard **commissum** processes ensure a short, concise audit period, with minimal client disruption
- proven report formats provide focus, clarity and real business value
- collaborative approach maximises knowledge transfer

“Are you sure it’s safe?”

Dr William Palmer (1824 -1856)

Convicted of poisoning and sentenced to hang, as he stepped up to the gallows.