Helping you piece IT together

BS 7799 Becomes ISO 27001

Copyright Notice
© 2005 BH Consulting IT Ltd. trading as BH Consulting, All rights reserved. This whitepaper is protected by copyright. Any reproduction of material of this whitepaper must be requested and authorised in writing from BH Consulting. Authorised reproduction of material must include all copyright and proprietary notices in the same form and manner as the original, and must not be modified in any way. Acknowledgement of the source of the material must also be included in all references. BH Consulting reserves the right to revoke such authorisation at any time, and any such use must be discontinued immediately upon notice from BH Consulting.

Disclaimer:
BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

Table of Contents

1. BS 7799 to become ISO 27001

The BS 7799 standard was originally developed and published by the British Standards Institution and is now an internationally recognised standard for implementing an Information Security Management System. BS 7799 is currently broken into two parts. The first part is intended as a set of "best practices" for information security. Part 1 of the standard is also divided up into ten sections covering the following areas:

- Security Policy
- Security Organisation
- Physical & Environmental
- Asset Classification
- Personnel Security
- Access Control
- System Development and Maintenance
- Communications and Operations Management
- Business Continuity Planning
- Compliance

The second part of the BS 7799 standard outlines 127 controls that an organisation can implement to achieve the standard. It is against part 2 of the standard that a company can be independently audited and subsequently certified to be compliant with the standard.

ISO 17799 describes a code of best practise that should be implemented. As such there is no third party auditing against ISO 17799. Instead, the BS 7799 standard is a recognised standard that can be audited against, providing organisations with independent third party verification that their Information Security Management System meets an internationally recognised standard.

Since it's first publication there have been many changes in the technical, business, regulatory and legal landscape within which the standard operates. To this end there have been a number of changes to ISO 17799 and a new information systems security standard is in the process of being published. This new standard, ISO27001, is more closely aligned with the new and updated ISO 17799 code of best practise.

As such the BS 7799 standard will now be replaced by the ISO 27001 standard upon its final publication, expected sometime towards the end of 2005.

The new ISO 27001 standard, while still in draft format has incorporated a number of significant changes from the BS 7799 standard. Firstly it is more aligned with ISO 17799 (2005), it also builds more on the PDCA model (Plan Do Check Act) and takes a similar approach to other recognised standards such as ISO 9001.

The ISO 27000 series has been set aside for publications in information security management. ISO 27001 is the first publication within this series. ISO 17799 (2005) will eventually be renumbered to ISO 27002. Other proposed publications in the series include ISO 2003 which will contain implementation guidelines, ISO 27004 which will be a new information security management and metrics standard and the proposed ISO 27005 publication will be a new information security risk management standard.

2. The Benefits of a Standards Based Approach to Information Security.

It can often be difficult to quantify the benefits that a company can derive from implementing an Information Security Management System based on a standard such as BS 7799 or ISO 27001. While tangible results can be demonstrated on investing in new hardware or in staff, it can be quite difficult to demonstrate to senior management the benefits from investing time, resources and money in an Information Security Management System.

Below are some of the benefits that we feel will benefit a company from implementing an Information Security Management System based on the BS 7799 or the ISO 27001 standard.

- **Increased reliability and security of systems:**
  Security is often defined as protecting the Confidentiality, Integrity and Availability of an asset. Using a standards based approach, which ensures that adequate controls, processes and procedures are in place will ensure that the above goals are met. By meeting the CIA goals of security you will also by default improve the reliability, availability and stability of systems.

- **Increased profits:**
  Having stable, secure and reliable systems ensures that interruptions to those systems are minimised. Minimising interruptions to critical systems increases their availability and therefore increases productivity. In addition to the above, a standards based approach to information security demonstrates to your customers that you can be trusted with their business. This can increase profitability by retaining existing customers and attracting new customers.

- **Reduced Costs:**
  A standards based approach to information security ensures that all controls are measured and managed in a structured manner. This ensures that processes and procedures are more streamlined and effective thus reducing costs.

  Some companies have found they can better manage the tools they have in place by consolidating redundant systems or re-assigning other systems from assets with low risk to those with higher risk.

- **Compliance with legislation:**
  Many companies are increasingly being required to comply with legal, industrial and regulatory compliance requirements. Having a structured Information Security Management System in place makes the task of compliance much easier.

- **Improved Management:**
  Knowing what is in place and how it should be managed and secured makes it easier to manage information resources within a company. BS 7799/ ISO 27001 ensures that management are involved in the Information Security Management System making for better management.

- **Improved Customer and Partner Relationships**.
  By demonstrating the company takes information security seriously, customers and trading partners can deal with the company confidently knowing that the company has taken an independently verifiable approach to information security risk management.

3. Official Sources for the Standard

- SNV: The Swiss national standards body, SNV, offer ISO 27001 FDIS from the following site:
  http://www.standards-online.net/InformationSecurityStandard.htm

- BSI: Through the StandardsDirect outlet, BSI offer the draft standard from the following page:
  http://www.standardsdirect.org/iso27001.htm

4. Contact Us

Helping you piece IT together

If you wish to contact us or provide any feedback on this whitepaper you may do so using the following contact details.

Telephone : **+353-(0)1- 4404065**
Website : **http://www.bhconsulting.ie**
Email : **info@bhconsulting.ie**