Helping you piece IT together

ISO 27001-
A Standard to Maintain

(This article first appeared in the July/August edition of Knowledge Ireland magazine, published by Silicon Republic Publishing)

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 The information in this document may be updated from time to time and may at times be out of date.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. A Standard To Maintain

As a result of increasing regulatory and industry compliance requirements, information security is becoming a board level item that needs to be addressed. Even for companies not impacted by the US Sarbanes-Oxley Act or the Basel II accord, there are other requirements such as the Data Protection Act that need to be adhered to. Companies are now faced with the dilemma of ensuring their information is secure enough to be compliant. However, therein lies the rub. How secure is secure enough? Does being compliant mean that your information and systems are secure? Indeed does being secure mean that you are compliant?

Information security is not solely about compliance, demonstrating best practises or implementing the latest technical solutions. It is about managing the risks posed to the business by the accidental or deliberate misuse of confidential information. It is important to note that no matter what industry, the private or public sector, every organisation has confidential information it needs to protect. This information could be customer details, payroll information, credit card numbers, business plans, financial information or intellectual property to name but a few.

The problem many companies face is that there are no recommended benchmarks or minimum grades clearly stated in any of these compliance regulations. Those faced with the responsibility of securing a company's information are faced with the onerous task of trying to determine how best to implement effective security controls to not only ensure compliance, but also secures their systems and information.

The ISO 27001 Information Security Standard offers companies a way to address this problem. Formerly known as BS 7799, ISO 27001 is now a vendor and technology neutral internationally recognised standard which provides companies with a risk based approach to securing their information.

ISO 27001 provides organisations with independent third party verification that their Information Security Management System meets an internationally recognised standard. This provides a company, and its customers and partners, with the confidence that they are managing their security in accordance with recognised and audited best practises.

By adopting the risk and standards based approach to implementing an Information Security Management System in accordance with ISO 27001, companies can reap many advantages, not least being better able to demonstrate compliance with legal and industry regulatory requirements.

It is important to note that ISO 27001 can simply be used as a framework against which a company can implement and measure its Information Security Management System against, without necessarily having to be accredited. This is particularly useful for companies wishing to ensure they are implementing an effective ISMS but may not want the expense and overhead of being audited.

Another challenge facing companies when implementing an ISMS is quantifying the benefits the company can derive from it. While tangible results can be demonstrated from 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.

However companies that have implemented an ISO 27001 based ISMS can demonstrate many efficiencies and other benefits such as;

- **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.

Meeting the CIA goals of security 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 thereby increasing their availability and productivity. In addition to the above, a standards based approach to information security demonstrates to customers that the company can be trusted with their business. This can increase profitability by retaining existing, 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:**
  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.

- **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.

While not guaranteeing 100% security, no standard or system can, ISO 27001 allows a company to implement a qualitative approach to risk management whilst providing mechanisms to address, reduce and manage those risks. Companies serious about information security should take a long hard look at ISO 27001, it could help answer the question “how secure is secure enough?”

2. References

2.1 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

2.2 Knowledge Ireland Magazine

Knowledge Ireland delivers a combination of authoritative opinion from leaders and analysis from Ireland's leading technology journalists. It contains contributions from strategists in business, technology, academia, government and siliconrepublic.com's (http://www.siliconrepublic.com) award-winning journalists.

Knowledge Ireland offers readers the opportunity to read the thoughts and opinions of the leading thinkers and strategists of the knowledge economy. It is a must read for those involved in implementing a knowledge agenda in business, academia and government.

More details are available at http://www.knowledgeireland.ie

3. 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**