

Evolution of an International Information Security Standard

An Executive Update

Volume 2 Number 2

April 2009

With public awareness of breaches such as the Heartland Payment Systems compromise of tens of millions of credit and debit card transactions, the electronic theft of engineering details about the Pentagon's Joint Strike Fighter project and the penetration of the U.S. electrical grid, the casual observer might come to the conclusion that information security has only recently become a topic of broad interest.

On the contrary, the security of information has been an area of interest and concern for nearly as long as the digital age.

The Result of Sixteen Years of Validation and Refinement: International Standard ISO 27001

This standard is now being used as the guideline for implementing a comprehensive Information Security Management System (ISMS)

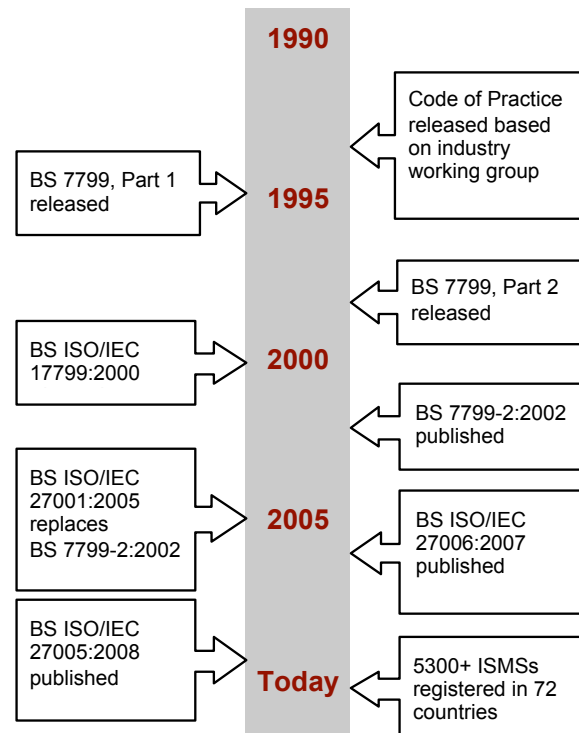
The International Organization for Standardization (ISO) has provided guidance for businesses, customers, governments, trade officials and developing countries since its formation in 1947. All of that experience goes into the development of new standards and the evolution and improvement of existing standards. ISO 9000, the quality management standard, is still perhaps the most familiar ISO standard to American businesses because of its impact in the US during the late 1980's and early 1990's.

The information security standard has matured since the early efforts of an industry working group back in 1993. Over the next twelve years, the development of an information security standard continued to evolve and mature; there is ongoing work to advance this area of standardization. The current version of the standard, ISO 27001:2005, is now used as a basis for internationally recognized ISMS certification.

continued on page 2

An Historical Timeline of the Standard

It all started in 1993 when the British Standards Institute sponsored an industry working group of information security professionals from the public and private sectors who met in the UK.



“Because ISO 27001 is an internationally recognized information security standard, companies in the global marketplace can quickly demonstrate due diligence to prospective customers via certification.”

ISO 27001 provides guidance in the following areas:

- Management oversight, policy and governance
- Legal and regulatory compliance
- Business compatible risk management
- Processes and technology
- Training, awareness and competency

The standard itself outlines 11 control areas, 39 control objectives and 133 specific controls for implementing a comprehensive Information Security Management System.

What's Next?

An entire 27000 series is planned to cover multiple aspects of information security and risk management:

- ISO 27000 – Information Security techniques, fundamentals and vocabulary
- ISO 27001 – Information Security Management System Requirements (released 10/2005)
- ISO 27002 – Code of Practice (released 06/2005)
- ISO 27003 – Proposed ISMS Implementation
- ISO 27004 – Guide for Information Security Management Metrics and Measurement
- ISO 27005 – Guide for Risk Management (released 06/2008)
- ISO 27006 – International Accreditation Requirements (released 03/2007)

Companies and organizations that have implemented an ISMS and received independent third-party certification of their information security programs have recognized several strategic advantages.

Companies dealing with multiple legal and regulatory compliance hurdles have realized that a comprehensive approach to information security is a far more effective use of time and resources than a non-holistic approach. There are also productivity gains in minimizing the impact of responding to security incidents and breaches. Most companies work very hard to establish and maintain a reputation of delivering quality products and services. Avoiding the negative publicity of a loss of customer or proprietary information has a qualitative impact on the bottom line as well.

With the experience of industry experts behind the standard and the strong history of continuous improvement, using ISO 27001 as the foundation for an information security management system is just good business. ■

“If there were no standards, we would soon notice...”

We are usually unaware of the role played by standards in raising levels of quality, safety, reliability, efficiency and interchangeability - as well as in providing such benefits at an economical cost.”

International Organization for Standardization web site, “Why Standards Matter, Overview of the ISO System”, 2007

FOR MORE INFORMATION...

JBW Group International

P.O. Box 19373

Minneapolis,

Minnesota 55419 USA

www.jbwgroup.com

Email: info@jbwgroup.com

1.877.97.27001