ISO/IEC 27001: The future of infosec certification

By Taiye Lambo

ISO/IEC certification allows organizations to build an effective Information Security Program that addresses current and future regulatory compliance requirements in a sustainable and cost-effective fashion.

Information security is about more, so much more than compliance, security and survival – it's about sharpening your competitive edge for battle in the information-driven age by achieving certification and accreditation.

Ensuring the Confidentiality, Integrity and Availability (CIA) of vital information assets is very important to the survival of most organizations, and allows them to remain competitive in an increasingly information-driven age. Vital information assets may consist of intellectual property and trade secrets, various forms of internal communications, and non-public information (NPI) entrusted to the organization by customers, business partners and other third parties.

For organizations seeking to balance business requirements with Information Security (IS) needs, achieving ISO/IEC 27001 certification makes good business sense, especially because ISO/IEC 27001 controls can actually be mapped directly to multiple regulatory compliance controls, thereby reducing unnecessary overlaps. It allows organizations to build an effective Information Security Program that addresses current and future regulatory compliance requirements pertaining to IS in a sustainable and cost-effective fashion.

The challenge

In the past three years, organizations on both sides of the Atlantic have felt the increased pressure resulting from the introduction of various government regulations and fiduciary requirements pertaining to corporate governance, including IS governance. These requirements include the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), Visa CISP/PCI, the Fair and Accurate Credit Transactions Act (FACT), the Gramm-Leach-Bliley Act (GLBA), California SB-1386 and other state government derivatives, FISMA/NIST SP 800-53/FIPS 200, Basel II, the UK Data Protection Act, the EU Directive on the Protection of Personal Data, and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), to name a few.

These Information Security requirements actually represent a knee-jerk reaction on the part of regulators and industry groups in response to corporate mishaps and high-impact security breaches. The intention is to instill corporate accountability and minimize IS breaches. Most of these regulations are really stipulating commonsense best practices and are asking organizations to do the right thing, which they should have been doing anyway. In 2005 there were over 200 documented high-profile security breaches that made national headlines in the US, highlighting a trend that got regulators and industry groups extremely concerned about the protection of personally identifiable information (PII) belonging to customers, business partners and employees alike. The threat posed by identity theft, including stolen company identities, has also raised the stakes for IS, making it evolve from an "IT" problem to a business problem, serious enough to keep your average corporate executive up at night for fear of his or her company becoming the next victim of IS breaches.

Organizations are now struggling to keep up with the latest external and internal threats as well as regulatory compliance requirements. As demonstrated by the attempted $400 million heist at the London branch of the Japanese Sumitomo Bank, the bad guys are getting smarter and more determined, especially as cybercrime becomes more profitable, as a white-collar crime. It is only a matter of time before drug lords and sophisticated gangs turn to cybercrime as the next low-risk, high-return venture. The target is corporate assets, which include financial and identity data. Speed of execution is of the essence, as they will typically target organizations with the least point of resistance. Organizational security weaknesses continue to arm external and internal personnel with tools to perform malicious activity.

Leading software vendors such as ISS, McAfee and Microsoft are increasingly echoing the same warning that technology software alone cannot protect organizations from these threats. We are learning that organizations now need hardened security processes, procedures and stated policies that are based on internationally accepted best practices, to solidify their IS defenses and meet legal, contractual and regulatory requirements.

The cost

Organizations face increasing costs (both tangible and intangible) as a result of Information Security breaches and regulatory non-compliance, including heavy fines, loss of customer confidence, loss of reputation, regulatory scrutiny, loss of market share and criminal/civil litigation.

Particularly in the IS world it appears that, given the recent spate of high-profile breaches and subsequent hefty penalties handed down by regulators, return on investment (ROI) is taking on new meanings like "risk of imprisonment," "risk of investigation," "return on insurance," "reduction of incidents," and what have you.

A recent survey completed by IDC indicates that organizations that take a more integrated approach to security and compliance issues can achieve tremendous cost savings[1]. The days of addressing security and compliance requirements in silos are over.

The opportunity

As a result of the momentum gained by its parent standard BS 7799-1, which was first published in February 1995, leading to the first publication of ISO/IEC 17799 in December 2000, the ISO/IEC 17799 code of practice has now gained international acceptance as the most comprehensive best practices framework available for IS Management. Up until October 2005, organizations could only get certified against BS 7799-2 and not ISO 17799. In October 2005, industry received the long-awaited ISO/IEC 27001:2005, just four months after the publication of the significantly revised version of ISO/IEC 17799. Organizations worldwide can now get certified against ISO/IEC 27001:2005, which is titled "Information technology – Security techniques – Information security management systems Requirements."

Unlike ISO/IEC 17799, which is a "Code of practice," ISO/IEC 27001:2005 is a certifiable standard, intended to provide the foundation for third-party audit, and is "harmonized" with other management standards such as ISO 9001 (quality management) and ISO 14001 (environmental management). In other words, an Information Security Management System (ISMS) developed for ISO/IEC 27001 certification can be integrated with existing management systems, within the organization.

Unlike such existing security-related certifications as SAS 70 and WebTrust, ISO/IEC 27001:2005 certification is much more comprehensive, and specifically focused on IS management.

ISO/IEC 27001 certification enables organizations to clearly demonstrate that their IS programs are not only effective, but also regularly reviewed and updated based on the plan-do-check-act (PDCA) process model, covering performance, effectiveness monitoring and review, and continual improvement.

Benefits of pursuing certification to ISO/IEC 27001:2005 include:

- Certification allows organizations to mitigate the risk of IS breaches
- Certification allows organizations to mitigate the impact of IS breaches when they do occur
- In the event of a security breach, certification should reduce the penalty imposed by regulators, since the organization's security and record-handling procedures will be seen as following internationally accepted best practices
- Certification allows organizations to demonstrate due diligence and due care to shareholders, customers and business partners, through strategic thinking
- Certification allows organizations to demonstrate proactive compliance to legal, regulatory and contractual requirements, as opposed to taking a reactive approach
- Certification provides independent third-party validation of an organization's ISMS
- ISO/IEC 27001 is the most comprehensive IS management certification that is internationally accepted

Certification programs such as SAS 70 and WebTrust cannot provide all the benefits listed above, due to their limited scope.

Implementation tips

These are some of the critical tasks required for implementing an effective ISMS when pursuing ISO/IEC 27001 certification:

- Procure the ISO/IEC 27001:2005 standard
- Obtain full executive management support
- Consider consulting options, e.g., Big Four consultants versus BSI Associate Consultancies
- Define the scope and boundary of the ISMS, working in conjunction with your certification body
- Consider legal, contractual and regulatory requirements
- Define an ISMS Policy
- Define the risk assessment approach
- Identify, analyze and evaluate the risks
- Identify and evaluate risk treatment options
- Select controls and control objectives, and reasons for selection
- Obtain management approval of the proposed residual risks
- Obtain management authorization to implement and operate the ISMS
- Prepare a "statement of applicability"

Conclusion

Now that the dust is starting to settle after the "regulatory compliance mayhem," organizations are starting to take more of a checkbox approach to compliance, especially as they are finding it hard to derive real business value from compliance spending.

A more pragmatic approach, going forward, is for organizations to seek independent certification to ISO/IEC 27001, which helps to address current and future regulatory compliance requirements in a proactive, cost-effective and sustainable manner.

If the rapid uptake of ISO 9001 certification for Quality Management in the 80s and 90s is anything to go by, the uptake of ISO/IEC 27001 certification for IS Management is likely to be more rapid than that of ISO 9001. And the current business driver for effective IS Management is not just competitive advantage. We now have legal, contractual and regulatory requirements as additional drivers. That is why ISO/IEC 27001 is the future of infosec certification.

About the Author

Taiye Lambo, founder & CTO of eFortresses, Inc. has dual expertise as a hybrid technical and business information security expert with a pragmatic holistic approach to the management of information security and regulatory compliance, and a subject-matter expert on information security governance and compliance relating to major regulatory requirements. He is the innovator behind the eFortresses (www.eFortresses.com) flagship product, Compliantz, and the Holistic Information Security Practitioner (HISP) Certification Program (www.hispcertification.org). He can be contacted at tlambo@eFortresses.com. eFortresses is also a "ISO 27001 Associate Consultancy" of BSI Americas.

[1] http://whitepapers.zdnet.com/whitepaper.aspx?scid=1048&docid=244541&part=rss&tag=rss&subj=ZDNet&promo=100112