ISO 27001
Is it Really Possible to Improve Information Security?

By Dave Ballai

It's no surprise to anyone working with electronic information today that the trends associated with data breach in the U.S. and abroad continue to unfold with alarming frequency and severity. Such breaches are escalating costs as organizations struggle to implement improved controls in their information systems. With pressure from stakeholders and legislators accelerating, many organizations are rightly moving to action by seeking to mitigate risks and to certify the security of their information systems against international standards. One such certification with global prominence is ISO 27001.

ISO/IEC 27001

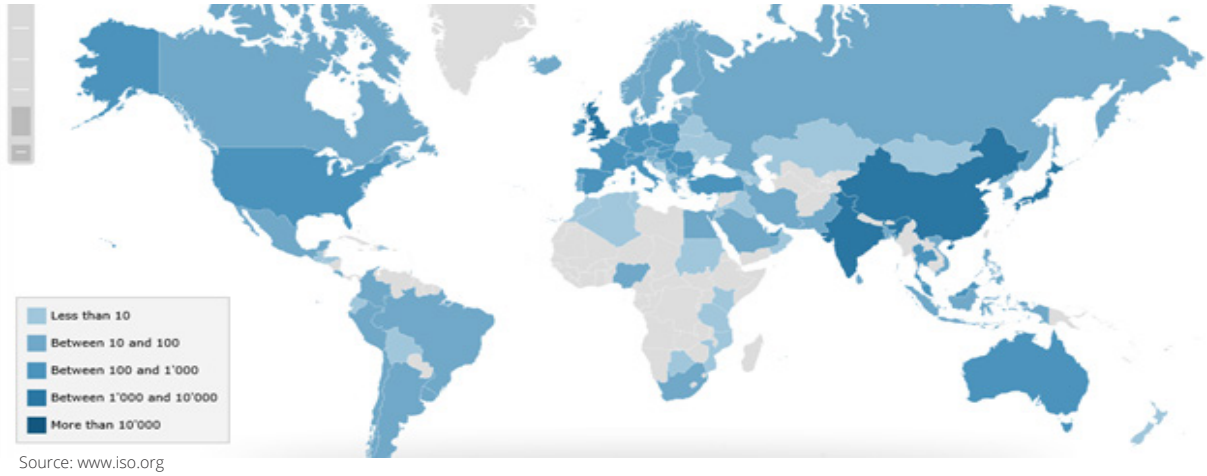
ISO/IEC 27001 *(for the sake of this article ISO 27k)* is the international standard that describes best practices for an Information Security Management System (ISMS). The ISO 27k standard replaces the previous internationally recognized British Standard, BS 7799. As with many certifications, ISO 27k incorporates a wide variety of acronyms, terms and phrases specific to the management of risks in operating any given information system. This certification ensures a systematic approach to managing confidential or sensitive corporate information so that it remains secure. The latest standard allows organizations to manage the confidentiality, and integrity, availability of their information assets. Certification to this standard helps organizations to protect and monitor information, and follows a continual improvement methodology, helping organizations to keep pace with emerging threats. It is important to understand that this certification by no means guarantees information security; it is up to the adopting organization to define the levels of risk it wants to mitigate. There are no absolutes in information security.

> "There are two types of companies: those that have been hacked, and those who don't know they have been hacked."
>
> **John Chambers,CEO, Cisco**

An ISO 27k compliant system helps you coordinate all your security efforts (technological, people-based and physical) coherently, consistently and cost-effectively. Because the system is constantly evolving, the ISO 27k program leverages a regular assessment of risks to ensure that threats are identified and treated promptly and effectively, in proportion to the organization's resources to control for such risk.

It is clear from the chart below that there has been a considerable adoption of the standard internationally through 2014, with several countries embracing the certification in large numbers:

Worldwide distribution of ISO/IEC 27001 certificates in 2014



Source: www.iso.org

Why do we need it?

We are witnessing an ever-escalating battle against cyber theft, cyber manipulation of content and in general, data breaches that often bring unknown consequences, some years after the breach event. In this ever-gyrating electronic environment, organizations are left to project the potential financial impacts, which include a broad array of response and mitigation activities, including: investigation, stakeholder impacts, system improvements, fines, and legal and marketing costs. Beyond these tangible costs are other factors that organizations need to consider in solidifying their information security posture. These include: insurance premium increases, potential business disruption, potential loss of intellectual property, customer relationships and contract revenue. "Hidden consequences can account for more than 90 percent of the total cost" according to recently published research from Deloitte Advisory's Cyber Risk Services, Forensics & Investigations, and Valuation teams. The study suggests many companies may be vastly underestimating the ramifications of a cyber attack on their businesses.

"The mantra of any good security engineer is: 'Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together."

Bruce Schneier

You don't have to search very hard to find an unnerving number of high-profile data breaches across a wide range of corporate and government entities. Here are just a few prominent entities with selected losses greater than 30,000 records in just the last 2 years:

- **Anthem** In February 2015, hackers walked away with >80,000,000 names, dates of birth, member IDs, social security numbers, addresses, phone numbers and emails at this, the second largest health insurer in the U.S.
- **Ebay** Hackers obtained log in credentials from a small number of employees and then used them to access a database containing all 145,000,000 user accounts, copying a large part of those credentials.
- **JP Morgan Chase** In July, 2014, hackers spirited away 76,000,000 names, addresses, phone numbers and emails of account holders at the largest bank in the U.S.
- **Sony** Three data breaches in one year, including the loss of 76,000,000 user account ids, and a very publicly embarrassing breach in 2014 with hackers spiriting away and then leaking confidential data. Data included personal information and emails about company executives, and then unreleased Sony films.
- **LinkedIn** Relatively new breach from 2012 just coming to light, impacting 117,000,000 user accounts.
- **US Department of Veterans Affairs** Officials at the VA took 3 weeks to report the loss of a stolen laptop containing some 26,500,000 veterans' personal information. Although the device was recovered, the VA was unable to say with certainty whether the information was compromised.
- **IRS** In early 2015, an unnamed group used an IRS app to download forms full of personal information. Posing as legitimate taxpayers, the crooks claimed some 15,000 tax refunds in other people's names.

With this as a backdrop, it is no wonder why many of the world's leading information organizations have adopted more rigorous information system security controls, including Google, Microsoft, Cisco and Verizon. These organizations understand the impact the ISO 27k controls have in supporting the highest security levels in their processes, people and systems.

"History has taught us: never underestimate the amount of money, time and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did."

Bruce Schneier

How it's done

The ISO 27k standard is composed of a broad range of elements that collectively make up the system that will ultimately be assessed through independent audit. Among the critical components in the process for attaining ISO 27k certification:

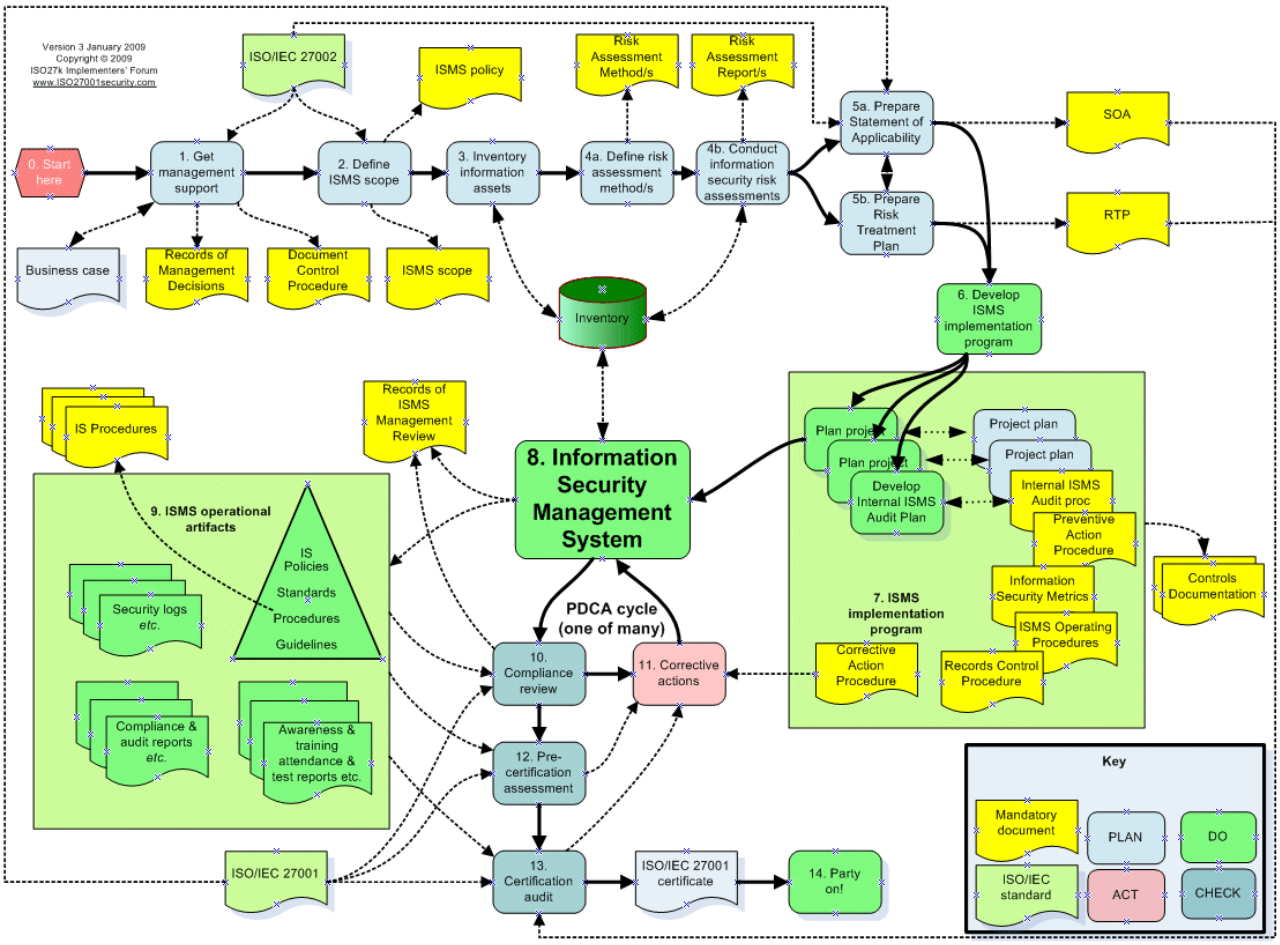
- Defining the scope of the system
- Defining management's roles and responsibilities
- Conducting periodic internal audits to ensure the system controls are resourced and functioning as documented
- Conducting annual management reviews
- Implementing the full range of security controls and their related procedures as relevant to the organization's business model
- Provisioning for security awareness training for employees with access and data management responsibilities. This is actually one of the largest fundamental shortcomings of all security technologies. Kevin Mitnick, one of the world's most prominent ethical hackers, has rightly observed that; "Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain"

Working through an organization's security posture in relation to the many control requirements of ISO 27k is by no means a minor undertaking. In fact, the preparation required across an organization to develop a well-honed security posture as defined by the ISO 27k program can take up to two years to accomplish, and requires ongoing maintenance and a continuous commitment from all levels of management. And the certification is not without cost.

There are three primary costs to becoming certified: internal costs (e.g., resource cost), consulting costs for preparation, and certification costs. The costs can vary notably based on the scope of the system, gap assessments, resource capabilities, and the project schedule.

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain"

Kevin Mitnick



Source: http://www.billslater.com/iso27001/ISO27k%20Process%20diag%20with%20PDCA%20full.gif

Any organization seeking ISO 27k certification is required to have an independent registrar audit the system each year. A "surveillance" audit is required in each of the first years following initial certification. In the third year, a more comprehensive "certification" audit is required. The cost of the surveillance audit is generally sixty to eighty percent of the certification audit. Organizations undergoing such audits must also demonstrate they are conducting internal audits annually. While this can be done with internal staff, most organizations favor having an independent entity conduct the audit.

It must be noted that in adopting ISO 27k, management teams are making risk decisions about the level of IT security desired relative to the organization needs and the capacity of the resources to leverage the controls associated with mitigating those risks. It is up to the organization to implement these controls. The risk assessment helps to provide a baseline against which to work in order to certify to the standard.

Finding Value

Creating an ISO 27k compliant information system introduces a material set of controls designed to avoid the types of reputational damage seen with increasing frequency among information processing organizations. Data breaches, large fines and brand damage are the natural result of catching an organization with inappropriate controls. While it is legitimately impractical to guarantee absolute lockdown on any information environment, organizations certified to the ISO 27k standard bring with them a materially higher degree of certainty that information under management is secure. The benefits of achieving certification (typically referred to as accredited registration) are many including:

- Increased security of valuable, sensitive and confidential information assets
- Proactive vs. reactive posture on information security management
- A credential positioned to convey to an organization's existing and potential customers that it has established and implemented best practice information security controls
- Checks off a critical box that an increasing number of clients require of information service providers. In fact, it is increasingly difficult to do business in international markets without an ISO 27k accreditation
- Reduces the risks of litigation and/or penalties levied by regulatory authorities due to data breach
- Demonstrates legislative, contractual and regulatory compliance
- Provides for independent review, yielding quality assurances on information security practices
- Implements processes which generate concrete metrics with which to justify organization security budgets

Will an ISO 27001 certification remove every possible risk associated with potential cybersecurity attacks? Of course not. We all realize there are no absolutes in information security in this era of internet-enabled access. However, this systematic approach materially reduces the risks of data breach and other potential impacts to data and systems by carefully exposing the many potential risks and introducing a set of rigorous controls to be maintained by the organization.

Organizations must weigh the value of their customers (and their own) mission-critical information against the costs and potential benefits associated with adopting certification programs such as ISO 27k. In this environment of increasing cyber terror, the smart move is to err on the side of caution.

"Ones only security in life comes from doing something uncommonly well."

Abraham Lincoln

LexisNexis® | REED TECH A LexisNexis® Company