IT NEXT

MEDIA FOR THE NEXT GENERATION OF CIOs

MARCH 2011 / ₹ 75
VOLUME 02 / ISSUE 02

SECURITY: Benefits of ISO 27001 certification for the enterprise 32

VDI: Virtualisation on the desktop makes good business sense 42

INTERVIEW: Sudhir Narang on transforming IT into Business Center 46

BOSS TALK Managing people effectively Pg 04

SEE THE FUTURE

IT managers share their experiences and insights in **DEPLOYING & IMPLEMENTING TECHNOLOGY SOLUTIONS**, while industry analysts examine the road ahead. Pg 14

+

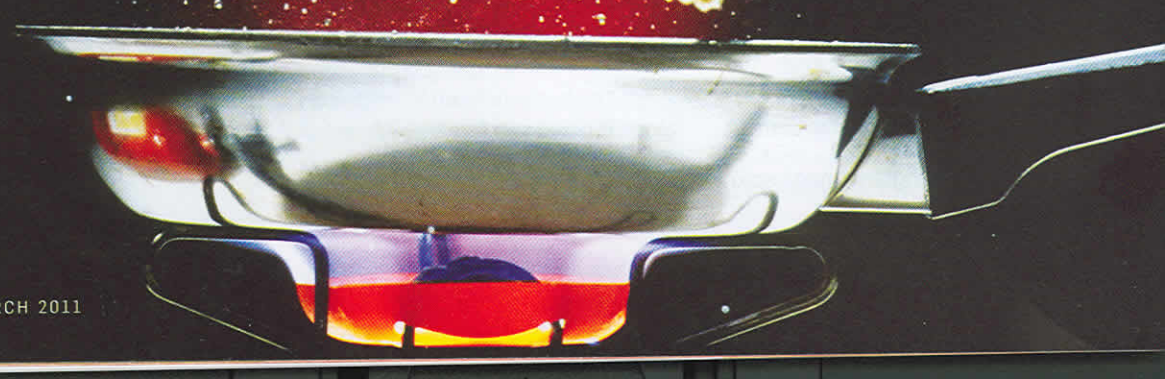
Case Studies on Lowe Lintas & Usha Martin Pg 26

A 9.9 Media Publication

ISO 27001 The Recipe FOR Success

The benefits of obtaining an ISO 27001 certification go far beyond the obvious. It could even be your USP, giving you that extra edge in these competitive times.

BY BERJES ERIC SHROFF



For most organisations today, information is the most vital asset. Information security can be described as the conservation of confidentiality, integrity and the availability of this information — the three pillars of the IT Security Triad. ISO 27001 is an international standard forinformation security best practice. The standard can be implemented in, and is applicable for all types of organisations, including commercial enterprises, government bodies and not-for-profit organisations,for designing a compliant Information Security Management System (ISMS). The standard provides the framework for a vendor-neutral, technology-neutral management system, that assures an organisation and its stakeholders that its information security measures are in place and are effective.

THE ISO 27001 CERTIFICATION GIVES YOU THE EDGE OVER A FIRM THAT IS NOT CERTIFIED, AND IT COULD BECOME YOUR UNIQUE SELLING POINT, ESPECIALLY IF YOU HANDLE CUSTOMER SENSITIVE DATA.

The structure of the standard

ISO 27001 has five main clauses (mandatory controls), 11 domains, 39 control objectives and 133 controls. The mandatory clauses include:

- Establishing the ISMS
- Management commitment
- Internal ISMS audits
- Management review of the ISMS
- ISMS improvement.

A fundamental tenet of ISO 27001 is the 'Deming Cycle' of plan, do, check and act. The 11 domains covered under the standard include:

- Security policy
- Organisation of information security
- Asset management
- Human resource security
- Physical and environmental security
- Communications and operations management
- Network access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Albeit the standard does not touch upon areas such as 'green computing' or 'wireless technology' per se, there is nothing stopping you from including this in your list of controls.

In fact, the controls cited in the standard are general guidelines to ensure that the important areas under these domains are not erroneously omitted.

5800 companies worlwide are certified under **ISO 27001** standard

Hence, it affords you the freedom of including your own controls to address the technology rolled out in the organisation. Having said that, it is important to note, that the reason for the omission of any controls cited in the standard, must be mentioned in the Statement of Applicability (SOA).

So what is the recipe to ensure the ISO 27001's success in an organisation? The first and foremost ingredient is to understandthe culture of the organisation, business objectives and garnertop management support. Management support and commitment in terms of manpower resources and financial resources are critical. Recognition of information security as being a priority by top management still remains one of the biggest challenges for CIOs / IT managers, worldwide. The second biggest challenge happens to be,getting sufficient resources. Information security is not only about IT — it is also about, amongst other things, organisational and cultural issues and human resource management. So if your management feels that the IT department can handle this without support from top management and other resources (manpower and financial) or support from other departments, the project is doomed from the beginning.

The next step usually involves identifying the scope forISO 27001 compliance. This is a crucial element else it will adversely affect the cost and ROI of ISO 27001 implementation.More often than not, it is not necessary for an enterprise to adopt a companywide implementation of the standard. If need be, this can be extended or staggered to other divisions / business units, at a later stage.

Once the scope has been identified, it is crucial to have a plan in place for

implementation. Although this is not part of the standard, it can be one of the major pitfalls — failing to plan means planning to fail. If youthink you will be able to roll this out in two to three months, then you will land up with a pile of procedures, polices and other documentation, which nobody will care about. The standard is not just about documentation — but you should be able to implement and measure the documented procedures and processes as well.

The backbone of a majority of, if not all, information security standards, is decision-making based on risk assessment. The ISO 27001 is no exception to this rule. In fact, the standard explicitly states the requirement of a risk assessment to be conducted prior to the selection of any controls.

From a business, compliance or contractual perspective, the risk assessment exercise mustidentify the threat and vulnerability for each asset, which has a likelihood of impacting the information security triad of confidentiality, integrity or availability. This also makes business sense, since the organisation would be able to divert its funds towards addressing the most critical risks identified.

The risk assessment process would also enable the management to identify ways of addressing this risk — whether the risk needs to be mitigated, avoided, transferred or accepted.

Building a good team is another crucial ingredient for success. In my experience, involving cross-functional teams, including legal and HR professionals is absolutely necessary, especially when it involves framing policies and penalties for violation of the policies. A CIO / IT manager cannot be expected to frame these policies without seeking guidance from these functional areas. Compliance (Domain 11) mandated by law applicable to the organisation for example, need to be addressed by involving the legal team.

The costs involved for implementation and certification need to be conveyed to the top management, as well as the ROI. Some of the costs which could come into play are - cost of internal resources to produce policies and procedures, cost of external consultants, cost of registration for certification, etc.

So what is the ROI for an organisation implementing ISO 27001? Is being ISO 27001 certified just a marketing gimmick?

The ISO 27001 certification does definitely give you the edge over an organisation that is not certified, and it could become your unique selling point, especially if you handle customer sensitive data. The ISO 27001 certification instils confidence in your customers that their personal information is protected.

Obtaining an ISO 27001 certification demonstrates that you have addressed, implemented and controlled the security of your information. From the firm's perspective, it can lead to cost savings. Imagine the loss to an organisation because of a leakage of company confidential data, for instance, business strategy, the loss of reputation built over the years, the cost of the customer's private data being compromised and subsequent law suits, etc. By obtaining the certification, you effectively establish that relevant laws and regulations have been addressed. ITNEXT

Berjes Eric Shroff is Manager IT, Tata Services

What is an ISO 27001?

ISO 27001 is aimed at organisations who wish to assess their information security risks and implement ways of addressing them. The ISO 27001 standard requires management to:

Systematically examine the organisation's information security risks, taking account of the threats, vulnerabilities and impacts;Design and implement a coherent and comprehensive suite of information security controls and/ or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

Adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

The benefits

ISO 27001 shares many benefits with other m anagement standards, like ISO 9001 and 14001.

- By having documented procedures and processes in place, the greater efficiency and transparency from their implementation reduces risk of mistakes and the consequent cost of re-work.
- These benefits are even more apparent in larger organisations where the clear channels of communication improve utilisation of time and resources.
- With all of this in place, employees can feel more at ease and confident in their roles.
- A knock-on effect is happier clients too, because you will reduce mistakes and have traceability if things were to go wrong.
- Importantly, ISO 27001 will ensure you meet current legislation. With rules changing regularly, it's important that this aspect is kept on top of.
- By using a Certification Body that will re-audit you each year, you're safe in the knowledge that you are meeting all legal requirements.
- Because you're reducing risk and demonstrating professionalism and accountability, your organisation can also benefit from reduced insurance premiums and better credit terms.