ISO 27001 Information Security Management Certification for Sri Lanka Telecom.

Sri Lanka Telecom PLC, the nation's number one integrated communications service provider and the leading broadband and backbone infrastructure services provider proudly announced the achievement of the globally recognized Information Security Management standard, ISO/IEC 27001:2005 awarded by the world renowned certification body, Bureau Veritas. The company received this accreditation for the third consecutive time on 8th April 2013.

The ISO 27001, which is the most stringent certification for information security controls, guarantees that ample information security controls and other forms of risk management are in place to enable an organization to assess its risk and implement appropriate controls to preserve confidentiality, integrity and availability of information assets. The certification also ensures that the maintenance for customer services meet international standards. The scope of certification spans across the company’s IT Operations including Systems Administration, Billing, Operational Support Systems, System Development, Network & End User Support, Network Operations such as SLT NOC and island-wide broadband network operations including IP-VPN/MPLS/Data services & Internet Service Provider (SLTNET) Broadband Services, Internet Data Centre (SLT iDC), Network Management & Network Security, Disaster Recovery Centre and core support services such as Power & AC operations and physical security management.

This accreditation verifies that the ISO 27001:2005 information security standard is now an integral component of Core IT & Network Operations within SLT and ensures compliance with ISMS policies, procedures and the institutionalization of ISO standard practices across the entire organization.

Sri Lanka Telecom is the first Company incorporated in Sri Lanka to achieve this security standard as well as to be listed in the prestigious Information Security Management System (ISMS) Registry since 2006.

Commenting on this achievement, Mr. Lalith De Silva, Group CEO of SLT PLC said "This is a significant achievement for SLT and demonstrates our continuous focus on improving our business and processes, especially in relation to our IT operations, which will give further assurance to our customers of the international standards maintained by our company in providing our services. As the national telecom service provider in the country, we embraced the responsibility to be first in the country to achieve this security standard with the expectation that our customers and employees will reap the benefits of this in the years to come.

**Introduction**

Information security is one of the central concerns of the modern organisation. The volume and value of data used in everyday business increasingly informs how organisations operate and how successful they are. In order to protect this information – and to be seen to be protecting it – more and more companies are becoming [ISO 27001](http://www.itgovernance.co.uk/iso27001.aspx?utm_source=green-paper&amp;utm_medium=infosec-iso27001&amp;utm_campaign=infosec-iso27001-green-paper) certified.

The main drivers for security are undoubtedly globalisation, government directives, terrorist activities and threats from hackers. Furthermore, organisations seeking opportunities to build markets in the UK are increasingly seeing ISO 27001 as a prerequisite for doing business. Certification is increasingly seen as a powerful assurance of your commitment to meet your obligations to customers and business partners.

In the United Kingdom, the Data Protection Act (DPA) requires businesses to secure their customers’ data, and hefty fines (up to £500,000) and sanctions can result from serious data breaches.

While the DPA offers no specific guidance to ensure the protection of data, ISO 27001 offers a set of specifications that describe the features of an effective information security management system (ISMS).

We realise that pursuing the right certification for your organisation can be overwhelming, particularly because there are so many variations. These variations are sometimes renamed or superseded by newer standards, which can cause some confusion. The purpose of this paper is to help you understand ISO27001 certification and explore the benefits of following the information security rules set by the Government.

**Overview**

 What is ISO 27001? How does this standard help organisations more effectively manage their information security?

 What is the relationship between ISO 27001 and [ISO 27002](http://www.itgovernance.co.uk/shop/p-721.aspx?utm_source=green-paper&amp;utm_medium=infosec-iso27001&amp;utm_campaign=infosec-iso27001-green-paper)?

 What is the value of ISO 27001 certification?

 How do these standards relate to [ISO](http://www.itgovernance.co.uk/shop/p-754.aspx?utm_source=green-paper&amp;utm_medium=infosec-iso27001&amp;utm_campaign=infosec-iso27001-green-paper) [9001](http://www.itgovernance.co.uk/shop/p-754.aspx?utm_source=green-paper&amp;utm_medium=infosec-iso27001&amp;utm_campaign=infosec-iso27001-green-paper)?

 What does someone need to know to initiate, or take on responsibility for, an organisational information security project and, specifically, one that is intended to lead to ISO 27001 certification?

**IT governance and information security**

The last few years have seen corporate governance requirements become increasingly more defined and specific. Information technology has become m o r e pervasive – underpinning and supporting almost every aspect of the organisation; manipulating and storing the information on which the organisation depends for its survival. The role of IT in corporate governance, in that case, has become more clearly defined, and IT governance is increasingly recognised as a specific area for board and corporate attention.

**The information security standards**

The ISO 27000 family of standards offers a set of specifications, codes of conduct and best practice guidelines for organisations to ensure strong IT service management. Of primary interest to information security are ISO 27001, ISO 27002 and ISO 27005.

ISO 27001 is a technology-neutral, vendor- neutral information management standard, but it is not a guide. Of the three parts to IT security governance, ISO 27001 offers the specification – a prescription of the features of an effective information security management system.

As the specification, ISO 27001 states what is expected of an ISMS. This means that, in order to receive certification or to pass an audit, your ISMS *must* conform to these requirements.

While ISO 27001 offers the specification, ISO 27002 provides the code of conduct –

guidance and recommended best practices that can be used to enforce the specification. ISO 27002, then, is the source of guidance for the selection and implementation of an effective ISMS. In effect, ISO 27002 is the second part of ISO

27001.

Just as ISO 27002 provides a set of guidelines for best practice in implementing an ISMS, ISO 27005 provides guidelines for risk management. As part of constructing a suitable and secure information management system, you must assess the risks to your information and be prepared to mitigate these risks.

**Certification vs conformance**

It is possible for an organisation to develop its ISMS in line with ISO 27002 only, because the good practice identified is universally applicable. Because it was not designed to be the basis of a certification scheme, however, it does not specify the system requirements with which an ISMS must be compliant in order to qualify for certification.

Those specifications are contained in ISO27001. In technical terms, this means that an organisation that is using ISO 27002 on its own can conform to the guidance of the code of practice, but it cannot get an outside body to verify that it is complying with the Standard. An organisation that is using ISO 27001 and ISO 27002 in conjunction with one another can design an ISMS that is in line with the specification and which follows the guidance of the code of practice and is, therefore, capable of achieving external certification. In order to achieve internationally recognised certification, your ISMS must be audited by an organisation approved by the appropriate body associated with the EA and IAF (in the UK, this is the United Kingdom Accreditation Service – UKAS). Furthermore, the auditing organisation cannot be your consultant – their whole involvement in your ISMS must be limited to their audit.

**Preparing for an ISMS project and the** **PDCA (Plan-Do-Check-Act) cycle**

An ISMS project can be a complex one. It is likely to encompass the entire organisation, and should involve everyone from the management down to the post room operatives. It may well take many months or, in some cases, years.

ISO 27001 certification is still relatively new and, as a result, hard experience of successful implementations is in short supply. This means that the handful of publications that describe, from a practical and pragmatic point of view, how to go about achieving certification should be studied at an early stage in the project planning process.

**Risk assessment and risk treatment plans**

An ISMS must be designed to meet the individual requirements of each organisation. Not only does every organisation have its own specific business model, objectives, unique selling features and culture, it also has its different appetites for risk. In other words, something that one organisation sees as a threat which it must deflect, another might see as an opportunity that it should grasp.

Similarly, one organisation may be less prepared to invest in defences against an identified risk than another. For this and other reasons, every organisation that implements an ISMS must do so against the results of a risk assessment whose methodology, findings and recommendations have been approved by the board of directors.

ISO 27001, in fact, requires a risk assessment to be carried out and, while it does not specify a methodology, it is very clear that this risk assessment must be based on identifying threats and vulnerabilities at an individual asset level and, from there, analysing and assessing risks.

While ISO 27001 offers no specific methodology for identifying risks, ISO

27005 is designed to assist the satisfactory implementation of information security based on a risk management approach. It supports the general concepts specified in ISO 27001 and offers a structured and rigorous process for analysing risks and creating the risk treatment plan.

Source:-

<http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf>

<https://www.slt.lk/en/content/slt-achieves-iso-27001-information-security-management-certification>