SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

**4th Year 2nd Semester 2016**


Name: **K.G.Bandulasena**

SLIIT ID: **IT13510954**

Group Number: -


Practical Session: **WE Tuesday**

Practical Number: **ISO_27001_Business_Case**

Date of Submission: **2nd September 2016**

Date of Evaluation : _____

Evaluators Signature : _____

# Commercial Bank of Ceylon PLC| Sri Lanka

## About the Commercial Bank

- Having set a benchmark in private sector banking in Sri Lanka we have set standards, created an identity and forged an unsurpassable trend. Recognized as trend setter we have maintained our cultural identity while providing a range of products and services. Powered by state-of-the-art technology and driven by a team of highly motivated, dynamic individuals we have become the leaders in private banking in Sri Lanka.

## Our Vision

- "To be the most technologically advanced, innovative and customer friendly financial services organization in Sri Lanka, poised for further expansion in South Asia".

## Our Mission

- "Providing reliable, innovative, customer friendly financial services, utilizing cutting edge technology and focusing continuously on productivity improvement whilst developing our staff and acquiring necessary expertise to expand locally and regionally"

# What is ISO 27001?

- ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it describes how to manage information security in a company. The latest revision of this standard was published in 2013, and its full title is now ISO/IEC 27001:2013. The first revision of the standard was published in 2005, and it was developed based on the British standard BS 7799-2.
- ISO 27001 can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large. It was written by the world's best experts in the field of information security and provides methodology for the implementation of information security management in an organization. It also enables companies to become certified, which means that an independent certification body has confirmed that an organization has implemented information security compliant with ISO 27001.
- ISO 27001 uses a top down, risk-based approach and is technology-neutral. The specification defines a **six-part planning process**:

1. Define a security policy.
2. Define the scope of the ISMS.
3. Conduct a risk assessment.
4. Manage identified risks.
5. Select control objectives and controls to be implemented.
6. Prepare a statement of applicability.

- **ISO 27002 contains 12 main sections:**

1. Risk assessment
2. Security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

- Organizations are required to apply these controls appropriately in line with their specific risks. Third-party accredited certification is recommended for ISO 27001 conformance.
- Other standards being developed in the 27000 family are:

✓ 27003 – Implementation guidance.
✓ 27004 - An information security management measurement standard suggesting metrics to help improve the effectiveness of an ISMS.
✓ 27005 – An information security risk management standard. (Published in 2008)
✓ 27006 - A guide to the certification or registration process for accredited ISMS certification or registration bodies. (Published in 2007)
✓ 27007 – ISMS auditing guideline.

# Why Commercial Bank of Ceylon PLC| Sri Lanka need the ISM ISO 27001 certificate.

## Benefits of Certification

### 1. Market Differentiation

The ISO 27001 certification is accepted globally, and its adoption rate in the U.S., while still not comparable to some other nations, is on the rise. There is increasing pressure from current customers, potential customers, and regulators to adopt a defensible, risk-based Information Security Management System, not just an ongoing reliance on vague “best practices” or other standards that aren’t specific to information security, like SAS 70 Type II. The effort involved in raising the maturity of the security program to certifiable levels is proof to clients and potential clients that your organization is actively managing and maintaining its information security posture.

**Benefit:**

The ability to stand apart from your competition. Attaining ISO 27001 certification means joining a small and exclusive group of companies and is a highly effective market differentiator for your company. Your competitors are most likely already looking at or moving toward ISO 27001 certification. You can get there first.

**Bottom Line Impact:**

Increased selling opportunities by offering a mature and capable ISMS certified to an international standard. A greater potential to land business where touting your company’s Security is a critical element, including opportunities to work with clients seeking to do business with a company that has a certified security program in place, as well as multi-national corporations.

## 2. Proactive vs. Reactive Security Management

ISO 27001 provides a set of criteria in the form of management system requirements and control objectives, based on best practice from various industries and countries. Organizations can then use these criteria as the basis to determine what they should be doing to manage Information Security, and the flexibility to decide on how. This allows the information security function to be proactive in developing, deploying, managing and maintaining an Information Security program. Information security is no longer forced into a constant "fire-fighting" mode and its corresponding lack of efficiency. In turn, a proactive, defensible approach to information security yields a reduction in response effort to the rising volume of information security questionnaires received from clients and potential clients. Given the increasingly cumbersome regulatory environment, detailed inquiries are often defended as due diligence, even though such inquiries impose a significant burden. With proactive information security management, the organization has a ready answer to security questions and has no need to "re-invent the wheel" every time a new inquiry is received. Often, customers are willing to accept the ISO 27001 certification in lieu of answering a lengthy and proprietary questionnaire.

**Benefit:**

Holding an ISO 27001 certification is widely accepted proof of a reliable, defensible, standards-based information security posture. It confirms to both management and clients that your organization is proactively managing its security responsibilities.

**Bottom Line Impact:**

Reduced effort and time to respond to inquiries, shortening the sales cycle and reducing the number of audit or review cycles (i.e. increased efficiency).

## 3. Information Risk Management

ISO 27001, with its process-based and risk-driven approach, provides a mechanism to integrate information security into your company's overall risk management strategy. Using the common language of risk management, business executives can now be presented with information security in its proper context of asset protection and risk mitigation, without a need to explain the intricacies or jargon of the discipline.

**Benefit:**

By making information security decisions on the defensible basis of risk management, the information security practitioner and business manager can employ a common terminology. In addition, the information security function becomes more integrated with the organization as a whole.

**Bottom Line Impact:**

Increased understanding and acceptance of the role of information security in the organization's overall risk management strategy.

## 4. Time Based Assurance

Adoption of the ISO standard requires implementation of an ongoing management component, or "Continuous Process Improvement." Organizations are required to not only identify what is in place now, but monitor, review, and change controls if the environment dictates such change. ISO 27001, like other ISO management standards, is based on the W. Edwards Deming model of Plan, Do, Check, Act to achieve continuous improvement.

If your organization must respond to customer security inquiries, there is nearly always a requirement for annual renewal or periodic re-review. Once certified under ISO, the ISMS will be subject to annual surveillance audits and re-certification every three years. These independent audits, performed by the Certifying Authority, offer proof to your management

and your clients that the ISMS is operating in a satisfactory manner with continuous improvement.

**Benefit:**

ISO 27001 certification is a dynamic process, requiring at least annual audits and periodic renewal of the certification. This offers independent proof of ISMS adequacy and the ongoing benefit of continuous process improvement. It offers clients and management proof that the ISMS continues to meet its security responsibilities.

**Bottom Line Impact:**

Proves to management that the program is operating effectively and has a positive return on investment. Reduces effort to provide ongoing compliance assurance to customers and regulators.

## 5. Process Definition and Metrics

Another benefit of ISO 27001 is its requirement to define information security services and the supporting processes. For some organizations, it will be the first time they have thoroughly addressed and defined the structure of their information security group. In other cases, the implementation of the standard yields defined process flows and assigned responsibilities for services delivered both to "customers" within the organization and for services delivered to information security by other parts of the organization, such as IT, Human Resources, and Legal. By defining process, inputs, outputs, and responsibilities, the role of information security is emphasized and awareness is increased across the organization .Process definition also yields an unambiguous basis for security metrics. These metrics are essential to measure both the effectiveness of the program and its progress through the PDCA, or continuous improvement, cycle.

**Benefit:**

Management gains a clear window into the results of its security investment, and better insight into which security processes are working well and which need improvement. This increased

visibility helps to make the case for the information security group and often can serve as a model for other parts of the organization.

**Bottom Line Impact:**

Concrete results and metrics help to justify security budgets. Better management understanding of the challenges and opportunities faced by information security leads potentially to both a larger role in the organization and the ability to at least sustain, and possibly increase, management funding. Moreover, metrics can be used to demonstrate opportunities to streamline processes and make more efficient use of available resources.

## 6. Consistent Third-Party Governance, Risk, and Compliance (GRC) Management

Consistency between internal and external parties is another challenge organizations face today, and the problem is only getting worse. How can you make sure that your requirements are being implemented, measured, managed, and communicated? Contract or service agreement language often does not address specific requirements for the preservation of information confidentiality, integrity and availability. A supplier risk assessment or audit can check to see if security expectations are adequately met, but by itself this activity does not communicate the actual requirements or criteria. With an ISO 27001 based ISMS, third party requirements, specifications, empowerment, and communication are an integral part of the system. These elements can then be provided to the third parties or service providers. What does this mean? It means that you can raise your level of assurance by knowing that the third parties are "on the same page" as your company. Suppliers are able to deliver services at desired levels and with processes and security measures which are defined, visible, and accountable to you.

**Benefit:**

Clear communication of security requirements to third parties and scheduled periodic reviews of compliance with such requirements.

**Bottom Line Impact:**

Third parties with a full understanding of requirements can provide more accurate pricing for services and are not “surprised” near the end of the contract process with unanticipated demands. Periodic compliance assessments become a scheduled part of third party governance, with specific stated objectives and increased focus on defined remediation tasks where necessary.

## 7. Legal and Regulatory Compliance

The legal and regulatory environment is increasingly more rigorous, and unfortunately, increasingly more burdensome. Recently introduced law and regulation often requires a risk-based approach and informed-choice decision making to achieve compliance. Both of these qualities are inherent in an ISO 27001 ISMS, along with a defined responsibility for the Legal department to advise security of pending legislation. A risk-based, structured approach to security management, policies and standards, means accommodating shifts in the regulatory environment can often be accomplished as part of the normal review and update cycle rather than in ad hoc, reactive mode. When changes are required, they can be accomplished incrementally rather than as a major overhaul.

**Benefit:**

The risk-based decision making inherent in an ISO 27001 ISMS means the system shares a common basis with many new legal requirements. Changes to the ISMS can be made in an orderly, incremental fashion.

**Bottom Line Impact:**

Legal and regulatory compliance is accomplished through an ongoing change process, often using maintenance cycles rather than unplanned efforts or forced reaction. Disruption to the

business is lessened, and compliance is achieved through simple alignment rather than repetitive and unplanned re-engineering of security policies, standards and practices.

## 8. Defensibility

ISO 27001 begins by requiring organizations to define a risk methodology, then to perform an assessment on their security practices based on the methodology. With the risk assessment in hand, information security and management together make informed choices regarding which controls must be applied, and justify those choices. The list of controls in Annex A of the standard are not simply "best practices" but rather a set of independent, reasoned choices formulated and signed off by more than 170 countries. Within the context of the ISMS, each choice can be defended on the basis of evaluated risks and defined controls. There is no "gray area," and no reliance on individual interpretations of security practices, no matter how well intended.

**Benefit:**

Referencing decision making to an independent standard and valid risk assessment means the organization can easily defend and justify its choices to management, customers and regulators.

**Bottom Line Impact:**

Using a defined and defensible set of information security controls means reduced effort and confusion in explaining security choices. This can shorten audit cycles and provide important reassurance to both management and clients that information security is based on informed-choice decisions, not just common practices.