SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

4th Year

Enterprise Standards for Best Practices of IT Infrastructure

IT13115494

De Silva D.W.N

Assignment – Business Case(ISO27001)

ESBPII

ISO 27001 – Information Security Management

Introduction

Softlogic Holdings PLC, evaluated as one of Sri Lanka's most dynamic and presumed combinations, started operations in 1991 as a software developer with only 12 workers; now has extended its impression holding driving positions in residential development arranged segments, for example,

- ICT
- Healthcare
- Retail
- Financial Services
- Automobiles and Leisure.

The Group now gives business to more than 8,000 people producing a turnover of more than USD300 million. Softlogic Holdings PLC is one of the largest listed companies on the Colombo Stock Exchange in terms of market capitalization. The Group's representations and vital organizations together with presumed worldwide foundations and vast multinational companies affirm its unparalleled neighborhood stature. Softlogic Holdings PLC holds authority position in all its business circles, with development, predominant innovation arrangements and world-class client administration serving as impetuses for growth.

Numerous companies like consumer services, Financials, Industrials and other monetary companies has executed ISO 27001 in their organizations since they needed to actualize exceptionally strict information security and business progression methodology and shields. Also, this is precisely why Softlogic Holdings PLC ought to consider adjusting to ISO 27001. These are a portion of the potential reasons why the organization may guarantee in ISO 27001.

ISO 27001 covers all types of organizations and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization’s overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual’s organizations or part thereof. Also it is designed to

ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

An information security management system is an arrangement of approaches worried with information security management or IT related risks. The government standard behind an ISMS is that an association ought to plan, execute and keep up a rational arrangement of approaches, procedures and systems to oversee risks to its information resources, consequently guaranteeing adequate levels of information security hazard. So if the organization has better information security, it will decrease the danger of occurrences, cutting episode related losses and expenses. What's more, if there is ISMS in an organization there are such a large number of advantages and expenses to the organization.

Just the universal standard for information security management conveys clear business returns. What's more, if there is ISMS in your organization it's a protection for your profitable information and licensed innovation. What's more, it will win new business and hold our current client base. Likewise, it maintains a strategic distance from the money related punishments and misfortunes connected with information ruptures.

Benefits of the ISMS

These are the courses in which an ISO27001 ISMS will commonly benefit the association.

- Information security risk reduction
- Benefits of standardization
- Benefits of a structured approach
- Benefits of certification
- Benefits of compliance

Information security risk reduction

- Expands company capacity to exchange certain risks specifically to back up plans or other outsiders, and may encourage arranging diminished protection premiums as key controls are actualized and oversaw

- Extensive, very much organized methodology improves the probability that all applicable information security dangers, vulnerabilities and effects will be recognized, evaluated and treated rationally
- Supervisors and staff turn out to be progressively acquainted with information security terms, risks and controls

Benefits of standardization

- Abstains from specifying the same fundamental controls over and over in each circumstance.
- Is for the most part material and thus re-usable over different divisions, capacities, specialty units and associations without critical.
- In view of internationally perceived and very much regarded security standards

Benefits of a structured approach

- Gives a component to measuring execution and incrementally raising the information security status over the long haul.
- Gives an intelligently steady and sensibly far reaching system/structure for unique information security controls.
- Manufactures a lucid arrangement of information security strategies, systems and rules, custom fitted to the association and formally affirmed by management.

Benefits of certification

- Positions the association as a safe, dependable and very much oversaw business.
- Exhibits management's reasonable responsibility to information security for corporate administration, consistence or due industriousness purposes.
- Formal affirmation by a free, skillful assessor that the association's ISMS satisfies the prerequisites of ISO/IEC 27001.

ISMS Costs

- ISMS implementation project management costs
- Other ISMS implementation costs
- Certification costs
- Ongoing ISMS operation and maintenance costs

ISMS implementation project management costs

- Get management endorsement to apportion the assets important to set up the execution venture group.
- Plan the implementation project.
- Hold consistent undertaking management gatherings including key partners.

Certification costs

- Survey and select an appropriate affirmation body.
- Staff/management time exhausted amid yearly observation visits.
- Danger of neglecting to accomplish affirmation at first.

Ongoing ISMS operation and maintenance costs

- Intermittent ISMS interior reviews to watch that ISMS techniques are being taken after effectively.
- Complete preventive and remedial activities to address potential and real issues.
- Occasional audit and support of information security strategies, benchmarks, techniques, rules, legally binding terms and so forth.

Conclusion

The eventual assurance of certification for information security and security risk management lies with the usage of proactive systems, based upon globally perceived guidelines. By giving solid, hazard driven, and prepare based information security hones in a way that is bundled for achievement, the association can accomplish the accompanying objectives:

- Expanded capacity to acquire and keep up business from its clients
- The capacity to separate its administrations from those of its rivals
- Better arrangement with management necessities and designated assets
- More thorough and continuous administration over outsider administrations
- Solid measurements to legitimize security spending plans

Because of these benefits Softlogic Holdings PLC which has full attention to get the ISO 27001 certification for further development of the company.