SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

IT12142910

Sarathchandra W.A.L

About The Company

Maliban Biscuits Manufactories (Pvt) Ltd is biscuit manufacturing company in Sri Lanka over fifty years of success profile. Maliban is the one of Sri Lanka’s most recognized brand. Maliban’s brand value Centre on its core values of heritage, trust, quality, taste and nutrition. Maliban Company has two key products; biscuits and milk. In the case of biscuits company have 26 varieties under 46 different sizes and in milk and also have full cream, non-fat, and high-Cal with milk calcium.

The different product line of Maliban such as Cracker, Savory, Sweets, Creams, Cookies and even private labels have targeted sophisticated customers through 74000 outlets in Sri Lanka and it has strong export marketing even in international markets. Today, consumers are intelligent when they come to buy of food products and they are confident about their superior quality. Because of that consumers are shifting to Maliban brand and have a high brand loyalty. All their decisions are consumer centric.

Maliban needs to decide on a risk method and implement a risk assessment, select your security controls and ensure that these are adequate to meet the security needs of your organization. . This requires information risk management and security expertise to implement. So ISO 27001 avoid the essential security threats for the company. Therefore it is a best practice to use ISO 27001 for the company for the safety of all liable parties. It is perfectly possible to implement an ISO 27001-compliant information security management system (ISMS) without adequately addressing information security.

What does ISO 27001 give you?

ISO 27001 gives you a best practice management framework for implementing and maintaining security. It also gives you a baseline against which to work either to show compliance or for external certification against the standard.

ISMS Benefits

Information security risk reduction

- Manage the information security within the organization

  The organization should protect the details of the liable parties who are engage with a relevant product feed. It should protect their privacy. Also this should keep secure the parties who gave the information for particular item. Their privacy details should be protected if they do not want to reveals themselves.
- Commitment to information security

  The management should have taken only the correct and clear information for publication. The product should publish under their acknowledgment and there should be a relevant party who get the responsibility of that item.
- Information security coordination

  Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. Everyone who is engaged with the process must provide their identity. Those details should be maintaining under an authorized person and it should be checked whether the provided details are accurate.
- Authorization process for information processing facilities

  The information within the organization such as the details of the employees, their attendance, leave details, salary details should only be managed by some authorized party. The access to those details should be given only for them.
- Confidentiality agreements

  Requirements for confidentiality or non-disclosure agreements are reflecting the organization’s needs for the protection of information and that should be identified and regularly reviewed. Also the appropriate contacts with relevant authorities should be maintained within the organization.

- Independent review of information security

  The organization's approach to managing information security and its implementation such as control objectives, controls, policies and procedures for information security shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

- Media handling

  This is to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse. Media should dispose of securely and safely when no longer required, using formal procedures.

- Addressing security when dealing with customers

  All identified security requirements should be addressed before giving customers access to the organization's information or assets. Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

- Terms and conditions of employment

  As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract. That should state their and the organization's responsibilities for information security. The employees Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

- Equipment security

It prevents loss, damage, theft or compromise of assets and interruption to the organization’s activities. Equipment should protect from power failures and other disruptions caused by failures in supporting utilities. Power and telecommunications cabling carrying data or supporting information services should protect from interception or damage. They should correctly maintain to ensure its continued availability and integrity. Equipment, information or software shall not be taken off-site without prior authorization.

- Back-up

  Back-ups are to maintain the integrity and availability of information and information processing facilities. Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

Benefits of Standardization

- Services

  Here it is simplifies the production of legal text and establishes quality, environmental as well as the safety policies. So this leads the organization to a massive economic development and helps to facilitate the business.

- Manufactures

  Using ISO 27001 allows Maliban to rationalize different varieties of products and protect those details from outsiders. Those products have to highlight that which products have more demand and which have less. According to that the production team can manage the amounts of production and according to the consumers’ needs they can go for variety of products. So those item must handle by authorized set of people only other than that information reveal to the all.

- Basic Control

  This avoids having to specify the same basic control repeatedly in every situation. ISO 27001 is a good practice which avoids re-inventing of activities in the organization. It is generally applicable and hence re-usable across the multiple departments, functions, business units and organizations without significance changes.

- Brand Value

ISO 27001 is based on globally recognized and well respected security standards. These standards suite is being actively developed and maintained by the slandered bodies, reflecting new security challengers.

Benefits of structured approach

- ISO 27001 provides00 logically consistence and reasonably comprehensive framework/ structure for disparate information security controls. The basic structure of the Maliban is stick into that and so the task can complete efficiently.
- It helps to improve the quality of the product. Avoid uncertainty of the product.
- This should provide a mechanism for measuring performance and incrementally raising the information security status over the long term.
- Within the organization the standards builds a coherent set of information security policies, procedures and guidelines which will manage the Maliban security status that formally approved by the management.

Benefits of Certification

- Having ISO 27001 is a formal confirmation for Maliban to prove that their independent and competent assessor that the organization have.
- It provides assurance regarding Maliban’s information security management capability. When the organization use ISO standard the customers believe the organization is secure, trustworthy and well managed. So Maliban’s brand value gets demanded.

ISMS Costs

- Find a suitable manager for give the correct guidance and handle the ISMS system.
- Plan the implementation of ISMS inside the company.
- Redesign the security architecture and the security baseline of the company.
- Prepare an overall product information security management strategy for Maliban including all the assets in the company.

- If Maliban wants to establish ISO 27001 there should be relevant equipment for them. So to buy those there is a company has to bear some cost.
- Compile an inventory or information assets.
- Conduct awareness/ training regarding the ISMS and how it works inside the company.
- Have to establish new security policies to the company.
- Hold regular project management meetings involving key stakeholders.
- Make plan for avoid risks that can be happen in the future when the company rely with ISO 27001 slandered.