**Sri Lanka Institute of Information Technology**



**Enterprise Standards and Best Practices for IT Infrastructure**

**4th Year 2nd Semester**

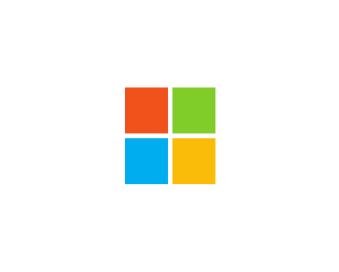
**ISO 27001 Business Case**

Name: **S.U.K. Hingalagoda**

Registration No: **IT 13 0568 58**

**Business Case for Information Security Management System (ISMS)**

**based on the ISO/IEC 27000 series standards**

****

Company: Microsoft

**Introduction**

**Microsoft Corporation** is an American [multinational](https://en.wikipedia.org/wiki/Multinational_corporation) [technology company](https://en.wikipedia.org/wiki/Technology_company) which is located in Washington. The company develops, manufactures, licenses, supports and sells computer software, consumer electronics and personal computers and services. Its best known software products are the Microsoft Windows line of operating systems, Microsoft Office and Internet Explorer and Edge web browsers. Its flagship hardware products are the Xbox video game consoles and the Microsoft Surface tablet lineup. As of 2011, it was the world's largest software maker by revenue and one of the world's most valuable companies.

Founded to develop and sell basic interpreters for the Altair 8800, Microsoft rose to dominate the personal computer operating system market with MS-DOS in the mid-1980s, followed by Microsoft Windows. The company's 1986 initial public offering (IPO), and subsequent rise in its share price, created three billionaires and an estimated 12,000 millionaires among Microsoft employees.

Throughout its history the company has been the target of criticism for various reasons, including monopoly status and anti-competitive business practices including refusal to deal and tying. The U.S. Justice Department and the European Commission, among others, have ruled against Microsoft for various antitrust violations.

**ISO 27001 Information Security Management Standards**

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world’s largest developer of voluntary international standards. The International Electrotechnical Commission (IEC) is the world’s leading organization for the preparation and publication of international standards for electrical, electronic, and related technologies.

Published under the joint ISO/IEC subcommittee, the ISO/IEC 27000 family of standards outlines hundreds of controls and control mechanisms to help organizations of all types and sizes keep information assets secure. These global standards provide a framework for policies and procedures that include all legal, physical, and technical controls involved in an organization’s information risk management processes.

ISO/IEC 27001 is a security standard that formally specifies an Information Security Management System (ISMS) that is intended to bring information security under explicit management control. As a formal specification, it mandates requirements that define how to implement, monitor, maintain, and continually improve the ISMS. It also prescribes a set of best practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures. Certification to ISO/IEC 27001 helps organizations comply with numerous regulatory and legal requirements that relate to the security of information.

**ISO/IEC 27001 implementation in Microsoft company**

The international acceptance and applicability of ISO/IEC 27001 is a key reason why certification to this standard is a foundation of Microsoft’s approach to information security. In 2009, the company received its first ISO/IEC 27001 certification for Microsoft Cloud Infrastructure and Operations (formerly Global Foundation Services), which provides datacenters and networking for Microsoft cloud services. Currently, Microsoft’s cloud infrastructure and services are audited once a year for ISO/IEC 27001 compliance by the British Standards Institution (BSI), an accredited certification body, providing independent validation that Microsoft has implemented security controls end to end.

Compliance with these standards, confirmed by an accredited auditor, demonstrates that Microsoft uses internationally recognized processes and best practices to manage the infrastructure and organization that support and deliver its services. The certificate validates that Microsoft has implemented the guidelines and general principles for initiating, implementing, maintaining, and improving the management of information security.

**Benefits of implementing ISO 27001**

## Information security risk reduction

* Strengthens existing information security control environment by (re-)emphasizing business information security control requirements, upgrading current information security policies, controls *etc*. and providing stimulus to review and where necessary improve information security controls periodically **– risk reduction**
* Comprehensive, well-structured approach increases the likelihood that all relevant information security threats, vulnerabilities and impacts will be identified, assessed and treated rationally **– risk reduction**
* Professional, standardized and rational risk management approach gives consistency across multiple information/communications systems (ICT) and business processes over time, and addresses information security risks according to their relative priorities **– risk reduction**
* Increases our ability to transfer certain risks selectively to insurers or other third parties, and may facilitate negotiating reduced insurance premiums as key controls are implemented and managed **– cost saving**
* Managers and staff become increasingly familiar with information security terms, risks and controls **– risk reduction**

## Benefits of standardization

* Provides a security baseline *i.e*. a solid platform of basic, almost universally required information security controls on which to implement specific additional controls as appropriate **– cost saving**
* An embodiment of good practices, avoids ‘re-inventing the wheel’ **– cost saving**
* Avoids having to specify the same basic controls repeatedly in every situation **– cost saving**
* Is generally applicable and hence re-usable across multiple departments, functions, business units and organizations without significant changes **– cost saving**
* Allows the organization to concentrate effort and resources on specific additional security requirements necessary to protect particular information assets **– cost saving**
* Based on globally recognized and well respected security standards **– brand value**
* ISO27k standards suite is being actively developed and maintained by the standards bodies, reflecting new security challenges (such as BYOD and cloud computing) **– brand value**

## Benefits of a structured approach

* Provides a logically consistent and reasonably comprehensive framework/structure for disparate information security controls **– cost saving**
* Provides the impetus to review systems, data and information flows with potential to reduce overhead of duplicated and other unnecessary systems/data/processes and improve the quality of information (business process re-engineering) **– cost saving**
* Provides a mechanism for measuring performance and incrementally raising the information security status over the long term **– cost saving and risk reduction**
* Builds a coherent set of information security policies, procedures and guidelines, tailored to the organization and formally approved by management **– long term benefits**

## Benefits of certification

* Formal confirmation by an independent, competent assessor that the organization’s ISMS fulfills the requirements of ISO/IEC 27001 **–** **risk reduction**
* Provides assurance regarding an organization’s information security management capabilities (and, by implication, its information security status) for employees, owners, business partners, suppliers, regulators, auditors and other stakeholders, without requiring numerous individual evaluations, assessments or audits, or having to rely purely on management assertions and assumptions **- cost saving and risk reduction**
* Positions the organization as a secure, trustworthy and well-managed business partner (similar to the ISO 9000 stamp for quality assurance) **– brand value**
* Demonstrates management’s clear commitment to information security for corporate governance, compliance or due diligence purposes **– cost saving and risk reduction**

## Benefits of compliance

* ISO27k provides an overarching framework for information security management that encompasses a broad range of both external and internal requirements, leveraging the common elements **– cost saving and risk reduction**
* Stakeholders or authorities may at some point *insist* that the organization complies with ISO27k as a condition of business or to satisfy privacy and other laws, whereas implementing it on our own terms and timescales is likely to be more cost-effective (*e.g*. we can prioritize aspects that offer the greatest business value, and take advantage of planned IT system or facility upgrades to improve security at minimal extra cost) **– cost saving**
* Adopting generally-acknowledged good practices provide a valid defense in case of legal/regulatory enforcement actions following information security incidents **– cost saving and risk reduction**

**Services covered by ISO 27001 certification in Microsoft company**

* **Microsoft Azure:** API Management, App Service: Mobile Apps, App Service: Web Apps, Automation, Azure Active Directory, Backup, Batch, BizTalk Services, Cloud Services, Document DB, Event Hubs, ExpressRoute, HDInsight, Key Vault, Load Balancer, Log Analytics, Machine Learning, Media Services, Multi-Factor Authentication, Notification Hubs, Portal, Redis Cache, RemoteApp, Rights Management, Scheduler, Service Bus, Site Recovery, SQL Database, Storage, Storage Premium, StorSimple, Stream Analytics, Traffic Manager, Virtual Machines, Virtual Network, and Visual Studio Team Services.
* **Microsoft Commercial Support:** Premier and On Premises for Azure, Dynamics CRM Online, Intune, and for Medium Business and Enterprise customers of Office 365.
* **Microsoft Dynamics CRM Online,** Microsoft Dynamics CRM Online Government, and Microsoft Dynamics Marketing.
* **Microsoft Intune.**
* **Microsoft Office 365** and **Microsoft Office 365 Government**
* **Microsoft Power BI** cloud service either as a standalone service or as included in an Office 365 branded plan or suite, but excluding data catalog functionality.
* **Visual Studio Team Services.**

**Cost of ISMS**

## ISMS implementation project management costs

* Find a suitable project manager (usually but not necessarily the person who will ultimately become the CISO or Information Security Manager)
* Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27k
* Plan the implementation project
* Obtain management approval to allocate the resources necessary to establish the implementation project team
* Employ/assign, manage, direct and track various project resources
* Hold regular project management meetings involving key stakeholders
* Track actual progress against the plans and circulate regular status reports/progress updates
* Identify and deal with project risks, preferably in advance
* Liaise as necessary with various other interested parties, parallel projects, managers, business partners *etc*.

**The cost of ISO 27001**

The foundation for ISO 27001 is your risk assessment and then your statement of applicability (SoA) and risk treatment plan. This is where you decide what controls you need to put in place. Depending on this there might be controls that are already in place (zero cost) and there might be controls that needs to be designed and implemented. There is a cost associated with this but until you have decided on the control and how to mitigate the risk you are not able to budget for the cost. For example it might be that all of your 25 employees need to receive awareness training on your information security policy at a cost of say £6000 in internal employee time or it might be that you want to buy a software solution that will help you manage and deploy security patches to your 1500 servers in your data centre at the cost of say £45000. You get the picture. This also hints at the quite natural cost variable that has to do with the size of the organization, the complexity of the organization, the geographical scope, the scope of the ISMS, the technology already used, etc.

To be successful with ISO 27001 design and implementation ISO 27001 should be treated as a project and hence there will be cost associated with this such as a project manager. Perhaps you have someone in the organization that has ISO 27001 experience as well as project management experience or perhaps you are looking at getting external assistance. In whatever case there is a cost, either internal employee time or external consulting assistance (or both in many cases). ISO 27001 is however not just done by having a project manager and a consultant. Involvement of employees is also a must so this means cost in employee time doing training, risk assessment, writing documentation, reviewing documentation, etc.