[](http://www.iso27001security.com/)

Business case for an  
Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k) for Sri Lanka Institute of Information Technology (SLIIT)

by **Eranda H.P.D**

**IT19029146**

Executive summary

#### Benefits

Information Security Management System ***(ISMS)*** is a framework that consists with various kind of policies & procedures to manage a particular organization’s privacy and security over its sensitive data. The main purpose of implementing ISMS is to minimize the damage from potential threats while preserving the business continuity. In order to achieve this ultimate goal, ISO IEC 27001 is the international standard certification that an organization needs to be certified with.

By implementing an ISMS, an organization gets the opportunity to experience lot of benefits out of it.

* Secures the information in all forms while preserving the CIA triad.
* Helps in improving the attack resilience of the organization.
* Provides a one central framework for keeping the organization’s information safe.
* Improves the organization’s work culture.

#### Costs

According to the current cyber security & economic standards in the world, it has become mandatory to reserve a much bigger budget for implementing an ISMS to an organization. However, there are several additional costs that are involved when implementing ISMS:

* Project planning and implementation costs.
* Certification costs.
* Costs that are spent for implementing mitigation mechanisms / countermeasures.
* Scaling up the existing security implementations to the next level.
* Costs that are spent for reviewing & supervision of the progress.

# Introduction, scope and purpose

For this particular business case assignment, I have selected **“SLIIT University”** as my organization. SLIIT is a class-leading non-state degree awarding institute approved by the University Grants Commission (UGC) under the Universities Act. When a particular organization is considered, Quality Assurance (QA) is an essential element that needs to be maintained and preserved. During the past several years, SLIIT has gained a serious attention amongst the other global Higher Educational Institutions **(HEI)**. So, when it comes to the Information Security, ISO 27001:2013 can be considered as one of the most popular information security standards in the world. For an organization like SLIIT, it is mandatory to achieve ISO 27001 international standard as it deals with the very sensitive & private information most of the time. Currently, there are huge number of stakeholders who have partnered with SLIIT. So, it has become a massive responsibility of SLIIT, to establish the necessary information security in their organization.

However, when it comes to a higher educational institute like SLIIT, there is always a particular scope that the organization needs to follow & agree with. Defining the scope can be considered as a very important stage in developing a business case since it defines what information assets need to be protected. There is no value in achieving ISO 27001 standard without a proper formal scope definition. It’s very much essential to understand the organization’s goals & boundaries first, before moving on directly towards defining the scope. So, let’s study about the scope in implementing ISO/IEC 27000 series information security standards in SLIIT.

|  |  |
| --- | --- |
| **Inside the Scope** | **Outside of Scope** |
| 1. Securing Student Information System 2. Securing Employee Information System 3. Securing the assets inside labs (PC’s) 4. Securing Server rooms 5. Implementing new security policies 6. Making implementation costs according to the budget 7. Access controlling for certain assets in the organization 8. Information Security incident management 9. Manage information security aspects of business continuity management 10. Compliance | 1. Implementing physical security (CCTV cameras, placing security guards) 2. Human Resource Security 3. Environmental Security 4. Communications Security 5. Manage supplier relationships 6. System development & maintenance 7. Organization’s future goals |

Now, let’s move on to the purpose of this particular business case. The main purpose of having this business case is to give insights to out target organization. Our main goal is to provide the stakeholders with a correct guidance & a understanding about the importance of implementing ISO 27001 Standard. Additionally, creating a proper business case for the organization greatly contributes specially when meeting with the stakeholder expectations about Information Security. This step can be considered as a very valuable & a very vital step since it ensures the confidence within stakeholders.

# ISMS benefits

These are the ways in which an ISO27k ISMS will typically benefit the organization.

## Information security risk reduction

* By developing an Information Security Management System ***(ISMS)*** in SLIIT, we can easily reduce the risk level for out particular organization. It will reinforce the existing security implementations to the next level. Scaling up the information security policies, access control mechanisms, authentication procedures can be considered as some examples of risk reduction mechanisms. **– risk reduction**
* Monitoring the organization’s systems at all the time is surely going to be helpful in reducing the risk for our target organization. **– risk reduction**
* Implementing a proper well-organized risk management approach creates the consistency over the sensitive information in our target organization. **– risk reduction**
* Providing the managers & employees with a proper security training will surely going to reduce the risk towards our target organization. **– risk reduction**

## Benefits of standardization

* Standardization can be considered as one of the most valuable benefits out of implementing a ISMS. This greatly contributes in reducing the security vulnerabilities that are caused by poor response time & various errors. **– error reduction**
* Due to the solid security baseline, it greatly contributes in cutting off the excessive expenses when implementing appropriate control mechanisms. **– cost saving**
* By implementing a proper standardized ISMS, it will reduce the cost that is spent for redundancy. **– cost saving**
* Another major benefit of standardization is the reusability. For example, a particular security implementation can be used for various departments, business units, lab rooms etc. **– cost saving**
* Rather than spending more money on implementing new security controls, the existing security controls can be improved furthermore. **– cost saving**
* 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**
* Formally defines specialist terms, enabling information security issues to be discussed, analyzed and addressed consistently by various people at different times **– cost saving**
* It helps in removing unnecessary, inappropriate or excessive controls without unduly compromising or damaging the valuable information assets **– cost saving**
* Being risk-based, the ISO27k approach is flexible enough to suit *any* organization, as opposed to more rigid and prescriptive standards such as PCI-DSS **– cost saving**
* Additionally, you will be getting a good & positive reputation throughout the world by following an appropriate standard. **– brand value**

## Benefits of a structured approach

* By having a well-organized, comprehensive structure is surely going to be helpful specially in reducing the cost. **– cost saving**
* By having a proper structured framework, it saves a great amount of money specially by reducing overhead of duplicated and other unnecessary systems/data/processes **– cost saving**
* When a particular system is created in a well-structured manner, implementing the monitoring & scalability functions becomes much more easier. **– cost saving and risk reduction**
* Having a well-structured approach ensures the correct governance of the organization through necessary information security policies & guidelines. **– long term benefits**

## Benefits of certification[[1]](#footnote-1)

* Having a proper ISO certification like ISO/IEC 27001, ensures the necessary independency & competence of the organization. **–** **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**
* It generates confidence & trustworthiness among the stakeholders about our target organization. **– brand value**
* Having a proper ISO standard certification demonstrates the utmost commitment to information security for corporate governance. **– 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**
* When our target organization complies with ISO 27001 as a condition of business, the stakeholders & other employees will also adjust and adapt according to the standard. So, in the business perspective, this might become much more cost effective for the organization. **– cost saving**
* Being aware of good practices provide a better protection for the organization in case of legal/regulatory enforcement actions following information security incidents. **– cost saving and risk reduction**

# ISMS costs

These are the main costs associated with the management system elements of an ISO27k ISMS[[2]](#footnote-2) for Sri Lanka Institute of Information Technology.

## ISMS implementation project management costs

* Payment for the ISMS implementation project manager. Most of the time this person might be the CISO ***(Chief Information Security Officer)*** of the organization.
* Preparing a well-organized information security management strategy can be considered as one of the major costs for a higher educational institute like SLIIT.
* Furthermore, planning of the implementation project is considered to be the most important stage of any given particular business case.
* However, before allocating the necessary resources to the project, it has to be approved by the higher management of SLIIT. The final outcome of the project has to be aligned with the organization’s budget range.
* It takes considerable amount of money to assign employees for various tasks & for the supervision.
* It is necessary to host group meeting with the necessary stakeholders.
* Project progress tracking also costs a considerable amount of money in a regular basis.
* Identifying & mitigating the risks also costs some amount of money.

## Other ISMS implementation costs

* Planning & designing an inventory containing all the information assets.
* Assessing the potential threats that may affect the resources and prioritize them accordingly.
* Implementing the suitable mitigation mechanisms & countermeasures based on the risk level.
* Reinforcing the existing security framework of the organization.
* Reviewing the existing security policies, standards, guidelines, protocols and fixing any sort of security loopholes within them.
* Upgrading & scaling up the currently implemented security controls to a higher level.
* Conducting multiple security awareness programs regularly for the academic & non-academic employees within the organization.

## Certification costs

* Comparing & selecting a suitable certification also cost some sort of money.
* Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body.
* There is a possibility of application for the certification getting rejected at the very 1st time.
* Delaying of the certificate acceptance also costs certain amount of money. Due to this the confidence of the stakeholders & investors may reduce as well.
* In the worst-case scenario, the intended certification may not be granted due to the poor security policies that have been implemented.
* For some instances, the organization might have to apply for one or more certifications first, before applying the main certification.

## Ongoing ISMS operation and maintenance costs

* It is compulsory to have regular ISMS internal audits in order to check the progress of the implementation operations.
* It is necessary to be consistent on applying reliable security mitigations on potential incoming threats.
* The supervision process has to be very consistent and stable specially when maintaining security policies, protocols, procedures & guidelines.
* The additional costs that are spent for the registration process needs to be cut down much as possible.

## Copyright

[](http://www.isect.com/)[](http://creativecommons.org/licenses/by-nc-sa/)This work is copyright © 2012 [IsecT Ltd](http://www.isect.com/)., some rights reserved.  It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](http://creativecommons.org/licenses/by-nc-sa/3.0/).  You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to [IsecT Ltd.](http://www.isect.com/), and (c) derivative works, if shared with third parties, are shared under the same terms as this.

1. The ISMS may optionally be formally audited against and certified compliant with ISO/IERC 27001 by a certification body duly accredited by ISO. Normally management decides whether to go ahead with certification once the implementation project is finished and the ISMS is fully operational. [↑](#footnote-ref-1)
2. Note that the ISO27k standards *recommend* but do not *require* any specific information security controls – it is up to management to determine and treat the organization’s information security risks as appropriate. Therefore, the costs of any information security controls that are implemented through the ISMS as a result of such management decisions are *not* separately identified in this template since they would presumably have been required even without the ISMS in place. However, you may prefer to identify any significant security investments that you know will be required in your business case or project proposal (perhaps with a similar note!). [↑](#footnote-ref-2)