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

The business case for an  
Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k) for Optimized Solutions.

Executive summary

**Benefits**

An ISMS can improve resilience to cyber assaults by raising awareness of potential threats, establishing controls to lower the chance of attacks, and having a plan in place to respond swiftly and effectively if an attack occurs. Information security this subject to strict management oversight through the ISMS allowing for guidelines and improved performance where necessary.

Moreover,

* lower security basis expenses
* Makes the workplace culture better
* Protect data availability integrity and confidentiality
* Use production for the entire organization

**Costs**

Since information security is a necessity for business and compliance, most of the associated costs would be incurred anyway.

The extra expenses which are especially associated with the ISMS include the following:

* Resources necessary for the design, implementation, and maintenance of the ISMS, including project management for the project.
* Different business activities and procedures we need to change to comply with ISO standards
* audits of third-party compliance is optional

# **Introduction, scope, and purpose**

* Optimized Solutions is a software company that is engaged in developing businesses with experience in building customized enterprise-scale software applications from the newest technology. They have been aiding businesses in achieving their objectives for business growth by offering cutting-edge and useful software solutions,
* The company is also taking part in financial services and manufacturing businesses through software skills.
* The organization's goal is to defend against external threats to sensitive and secret data through

organizational information security management systems.

* To make sure they are adhering to information security rules and regulations, (ISMS) will be useful.

# **ISMS benefits**

These are how an ISO27k ISMS will typically benefit the organization.

## Information security risk reduction

## All relevant and important information security risks, vulnerabilities, and consequences are more likely to be found, evaluated, and dealt with effectively using a thorough, well-structured process.

* This method addresses information security risks in order of importance while ensuring consistency across different information communication systems (ICT) and corporate processes.
* They gain a deeper comprehension of the concepts, dangers, and controls related to information security.

Benefits of standardization

* Without significant change, it can be applied across numerous departments, roles, and organizations, eliminating the need to repeatedly specify the same fundamental principles.
* Standardized technology reduces complexity and has advantages like easier integration, increased efficiency, lower costs due to economies of scale, and better IT support.
* Information assets can be better protected if the company concentrates its efforts and resources on

extra security requirements.

* The ISO 27K standard suites are modified and kept regularly by standards bodies, considering new security, by internationally recognized and accepted security standards.
* Limitations that are unnecessary or excessive can be relaxed or eliminated without compromising the integrity of crucial data.

## Benefits of a structured approach

* It assembles various information security controls into a comprehensive and logically sound framework.
* It also enables the evaluation of performance and the long-term development of information security and assembles a uniform set of guidelines and practices for information security.
* We must construct an organized collection of information security rules, processes, and guidelines that are customized for the firm and formally authorized by management.

## **Benefits of Certification[[1]](#footnote-1)**

* A company's ability to handle data security is guaranteed by the certification that the organization's ISMS complies with ISO/IEC 27001 requirements from an independent, experienced assessor.

## **Benefits of compliance**

* The ISO27k standard offers a framework for information security management that considers a wide range of needs, both internal and external, by employing common characteristics.
* Although stakeholders or agencies may require ISO27k compliance at some point to conduct business or to meet privacy and other standards, implementing ISO27k according to our schedules and terms is probably more cost-effective.

# **ISMS costs**

There are several costs in ISMS.

## ISMS implementation project management costs

* Create a thorough information security management policy that is connected to additional corporate goals and requirements in addition to ISO27k
* Before assembling a development team, you must first receive management's approval.
* Hold regular project management meeting sessions with important stakeholders while recruiting, allocating, supervising, and tracking a variety of project resources.
* Find a suitable project manager (usually but not necessarily the person who will ultimately become the CISO or Information Security Manager)
* Hire, assign, oversee, and monitor different project resources
* Invite key stakeholders to frequent project management meetings.
* Monitor actual progress in comparison to the plans and disseminate periodic status reports and progress updates.
* Recognize and address project risks, ideally in advance

## Other ISMS implementation costs

* List every information asset you possess.
* Give top focus to reducing cyber threats to data assets.
* Choose a course of action for handling information threats.
* Establish a security baseline and a security architecture for the organization.
* Information security management policies and regulations may need to be reviewed, updated, or reissued. Additionally, new information security processes, guidelines, and contractual requirements may need to be developed and/or issued.
* Established security measures and risk treatments may also need to be legitimized, upgraded, augmented, or retired, as appropriate.

## Certification costs

* Identify a competent certifying body after studying the problem.
* The system is inspected and audited by an ISO/IEC 27001 certification body.
* Assess and select a suitable certification body
* Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body
* Risk of failing to achieve certification at first application (any items that caused failure would themselves represent unacceptable information security risks – delayed certification more likely than complete failure)
* Staff/management time expended during annual surveillance visits
* Tri-annual re-certification (more thorough review and hence wider impact, but still relatively minor)
* All these costs will be minimized if we achieve high-quality implementation through our efforts

## **Ongoing ISMS operation and maintenance costs**

* Regular internal audits of the ISMS are conducted to ensure that the policies are being followed, and corrective and preventative measures are taken to address future and existing problems.
* Maintaining recurrent small expenditures to registration.
* Provide employees with information about ISO 27001 and ISMS.
* Make sure that every new worker is familiar with ISO 27001.

# **Conclusion**

* The organization can modify the paper to reflect their understanding and add the necessary conclusion.

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)