Business Case for an  
Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k)

For

**Access Engineering PLC**

**(**http://www.accessengsl.com/**)**

By Sugathapala M.R.C.L.V

(IT13006044)

**Executive Summary**

ISMS is a system that helps to prevent and counteract interruptions to business activities. It protects critical business processes from the effects of information security incidents, disasters and major failures of information systems and ensures the timely resumption of normal operations.

**Benefits**

Nowadays Information has become a truly business critical asset. Management of Information Security covering all information assets deployed for providing Business Process Services including Healthcare Services the ISO 27001 certification is particularly useful to Access Engineering Company by helping develop a stringent [Information](http://searchnetworking.techtarget.com/tip/Developing-consistent-information-security-policy-management) security management system. Most important, it will demonstrate to employees, customers and business partners that when it comes to security, to Access Engineering Company is prepared. The benefits of implementing an ISMS will primarily result from a reduction in information security risks. Specifically, benefits realized from the adoption of the ISMS family of standards include:

* Prevention of confidentiality breaches
* Manages and minimizes risk exposure.
* Prevention of unauthorized alteration of critical information
* Credibility, trust and confidence of your customer
* Securing confidentiality, integrity and availability
* Builds a culture of security.
* Protects the company, assets, shareholders and directors.
* Prompt detection of data leakage and fast reaction
* Competitive advantage - deciding differentiator in contract negotiations
* Meeting international benchmarks of security
* Higher awareness of security
* Compliance with legislation

**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

**Introduction, Scope and Purpose**

Adopting the [ISO/IEC 27000-series information security standards](http://www.iso27001security.com/) (commonly known as “ISO27k”) generally starts with a discrete implementation project to specify, design, develop and launch the Information Security Management System (ISMS). Once operational, the ISMS operates indefinitely, managing information security using the governance and management processes comprising the management system. This paper identifies and categorizes the financial implications of implementing an ISO27k ISMS as a set of typical or commonplace benefits and costs. It is of course generic since we have no knowledge of your specific information security situation or risks. Feel free to use this paper both as a source of inspiration for your own business case, budget request or project proposal to management[[1]](#footnote-1), and as a framework for measuring and optimizing the net value of your ISMS over the long term (*e.g*. using ISACA’s [Val IT approach](http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx) with [PRAGMATIC metrics](http://www.securitymetametrics.com)).

1. [↑](#footnote-ref-1)