****

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

Executive summary

#### Benefits

The ISMS will bring information security under firm management control, allowing direction and improvement where needed. Better information security will reduce the risk (probability of occurrence and/or adverse impacts) of incidents, cutting incident-related losses and costs.

Other benefits of the ISMS include:

* A structured, coherent and professional approach
* to the management of information security, aligned with other ISO management systems
* Comprehensive information security risk assessment and treatment according to business *and* security priorities
* Focuses information security investment to greatest advantage
* Demonstrable governance using internationally-recognized good security practices

#### Costs

Most of the costs associated with information security would be incurred anyway since information security is a business and compliance imperative. The *additional* costs specifically relating to the ISMS are mainly:

* Resources needed to design, implement and operate the ISMS
* Changes needed to bring various business processes and activities in line with the ISO standards
* Third party compliance audits (optional – only required if we decide to go for certification, a decision that can be made once the ISMS is working)

# Introduction, scope and purpose

Inspired eLearning is seeking to be compliant with the globally recognized information security standard known as ISO 27001, which is an information security management system (ISMS). This compliance will ensure that we are able to proactively work toward managing our security risks and create a comprehensive security program for all our information technology systems, people, and processes.

The scope of the ISMS will include any environment where information technology meets people and where we store customer data. This means that our offices, contractors (such as our Taiwan and/or Mexico teams) and our data center environments shall be subject to risk assessment and management based upon the principles set forth by the International Organization for Standardization (commonly known as ISO). Once operational, the ISMS will operate indefinitely, managing information security using the governance and management processes which comprise the management system.

Adopting the ISO 27001 ISMS will allow us to ensure that we are compliant with other security laws (such as the European Union’s Global Data Protection Regulation). Within the context of the ISMS, our customers and partners will know that we are not relying upon an interpretation of “best security practices” but instead have evaluated risk and taken steps to mitigate those risks wherever possible.

# ISMS benefits

These are the ways in which an ISO 27001 ISMS will benefit us.

## Information security risk reduction

* Strengthens existing information security control environment by emphasizing business information security control requirements, upgrading current information security policies, adding security controls and providing stimulus to review and where necessary improve existing 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 our 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 **– adding brand value**
* The ISO 27001 standards suite is being actively developed and maintained by the standards bodies, reflecting new security challenges (such as BYOD and cloud computing) **– adding 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**
* Allows unnecessary, inappropriate or excessive controls to be relaxed or removed without unduly compromising 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**

## 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[[1]](#footnote-1)

* 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 **– 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

* ISO 27001 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 ISO 27000 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**

# ISMS costs

These are the main costs associated with the management system elements of an ISMS:

## ISMS implementation project management costs

* Assign 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 ISO 27001
* 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, and/or business partners

## Other ISMS implementation costs

* Assess security risks to information assets, and prioritize them
* Determine how to treat information risks (*i.e.*mitigate them using suitable security controls, avoid them, transfer them or accept them)
* Design the security architecture and create a security baseline
* Review/update/re-issue existing and prepare/issue new information security policies, standards, procedures, guidelines, and contractual terms.
* Rationalize, implement additional, upgrade, supplement or retire existing security controls and other risk treatments as appropriate
* Conduct awareness/training regarding the ISMS, such as introducing new security policies and procedures
* May need to ‘let people go’ or apply other sanctions for non-compliance

## Certification costs (optional, up to $20,000 for third party audit)

* 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 all be minimized if we achieve high quality implementation through our own efforts

## Ongoing ISMS operation and maintenance costs

* Periodic ISMS internal audits to check that ISMS procedures are being followed correctly
* Complete preventive and corrective actions to address potential and actual issues
* Periodic review and maintenance of information security policies, standards, procedures, guidelines, contractual terms *etc*.
* Minor costs to maintain registration ($10,000-12,000 per year)

# Conclusion

## The benefit of achieving compliance with the ISO 27001 ISMS allows us to bring added value to our customers and an assurance that we are fully protecting their information. It will also allow us to avoid penalties and financial losses due to data breaches. We will reduce efforts and confusion in our information security and information technology programs and cause less disruption to the business by ensuring that audits and reviews are completed in an orderly fashion.

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)