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

Version 5 2023

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, including project management for the implementation project
- Changes needed to bring various business processes and activities in line with the ISO standards
- Third party audits (optional – only required if we decide to go for certification, a decision that can be delayed until the ISMS is working)

Introduction, scope and purpose

Adopting the ISO/IEC 27000 family of information security standards (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], 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 with PRAGMATIC metrics).

ISMS benefits

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

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**

[1] If the business case is overwhelmingly positive, there may no need to elaborate much further on the details in order to persuade management to approve the project … but nevertheless it pays to explore and understand those fine details just in case objections are raised, and for subsequent project planning.

- 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, cloud computing, IoT and AI/ML) – **brand value**
- Formally defines specialist terms, enabling information security issues to be discussed, analysed 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[2]

- Formal confirmation by an independent, competent assessor that the organization's ISMS fulfils 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**

[2] The ISMS may optionally be formally audited against and certified compliant with ISO/IEC 27001 by an accredited certification body. Normally management decides whether to go ahead with certification once the implementation project is finished and the ISMS is fully operational.

- Demonstrates management's clear commitment to information security for corporate governance, compliance or due diligence purposes – **cost saving** and **risk reduction**

Benefits of conformity

- 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 and conforming with it on our own terms and timescales demonstrates a proactive approach and 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 and disruption) – **brand value** and **cost saving**
- Adopting generally-acknowledged good practices provides a valid defence 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[3].

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.*

[3] 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!).

Other ISMS implementation costs

- Compile an inventory of information assets in scope of the ISMS
- 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, share them or accept them)
- (Re-)design the security architecture and security baseline
- Review/update/re-issue existing and prepare/issue new information security policies, standards, procedures, guidelines, contractual terms *etc*.
- 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[4]
- May need to 'let people go' or apply other sanctions for non-compliance

Certification costs

- Assess and select a suitable certification body
- Stage 1 (pre-certification) audit and stage 2 (certification audit) 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 and management reviews
- Preventive and corrective actions to address potential and actual issues
- Continual improvement by identifying and seizing opportunities that arise
- Periodic review and maintenance of information security policies, standards, procedures, guidelines, contractual terms *etc*.
- Minor costs to maintain certification (a few $k for annual surveillance audits) – certification-related costs may be shared across other ISO management systems

[4] This is typically handled as part of an ongoing information security awareness program.

Conclusion

You are very welcome to use this generic paper as a basis for your own business case, using hard data and realistic estimates from your organization to firm-up the numbers. By all means contact the author Gary@isect.com or visit www.ISO27001security.com for more information and advice from other ISO/IEC 27001/2 implementers, or to identify further costs and benefits that don't presently feature in the template. We welcome your involvement.

Document history

2023: minor but important correction re accreditation. Change to UK/NZ English.

2022: revised again for ISO/IEC 27001:2022 and ISO/IEC 27002:2022. Red/green colouring.

2017: updated.

2012: extensively revised.

2008: first public release of the generic business case as part of the free ISO27k Toolkit.

1995-2008: underlying concept gradually developed and refined through a number of project proposals, security strategies *etc*. with various organizations.

Copyright