



# The financial implications of implementing ISO/IEC 27001 & 27002: a generic cost-benefit model

Gary Hinson, IsecT Ltd., 15<sup>th</sup> January 2008

## Executive summary

### Benefits

- Reduces information security risks
- Reduces probability and impacts of infosec incidents
- Certification to an international standard
- Marketing advantages *etc.*
- Structured, coherent approach
- Comprehensive risk assessment
- Focuses infosec spend to greatest advantage
- Demonstrable governance

### Costs

- Project management, project resources
- Organizational change requires organizational resources
- Design, development, testing, implementation
- Certification & surveillance visits
- Ongoing operation & maintenance

## Introduction

Organizations intending to adopt ISO/IEC 27002 (the international standard code of practice for information security management) and ISO/IEC 27001 (the information security management system certification standard) usually organize the associated work as an implementation project. This generic financial model outlined in this paper explains the financial implications of implementing ISO/IEC 27001 & 27002 as a set of typical benefit and cost categories. The model may be used both as the basis for a business case to justify the project to senior management, and as a framework for measuring and optimising the net value of the investment over the long term.

## Benefits

### Reduces information security risks

- Strengthens existing information security control environment by (re-)emphasizing business information security control requirements, upgrading current information security policies, controls *etc.* & providing stimulus to review & update information security controls periodically – **risk reduction**
- Comprehensiveness reduces probability of unrecognized information security threats or vulnerabilities – **risk reduction**
- Professional, standardized & rational risk management approach gives consistency across multiple (all!) systems over time, & addresses information security risks consistently (risk based approach focuses on highest risk areas) – **risk reduction**
- Increases ability to transfer risks selectively to insurer, and enables negotiation to reduce insurance premiums as controls are implemented – **cost saving**
- Managers & staff will become increasingly familiar with information security terms & controls – **risk reduction**

### Benefits of standardization

- Provides a 'common denominator': a strong basis on which to build system-specific additional controls as appropriate without having to constantly revisit the basic controls – **cost saving**
- Avoids need to separately-specify, implement & review common baseline control requirements & controls on each system – **cost saving**
- Is generally applicable & therefore directly re-usable across multiple departments, functions & organizations without change – **cost saving**
- Allows organization to concentrate its effort & resources on identifying & satisfying supra-baseline control requirements – **cost saving**
- Generally accepted & well established (BS 7799 → ISO/IEC 17799 → ISO/IEC 27002) with increasing awareness & uptake world-wide
- Recognized embodiment of accepted good information security practice – why re-invent? – **cost saving**
- Saves time & money by directly adopting good practice – **cost saving**
- Provides common terminology to discuss, specify, develop & assess information security requirements & controls
- May even allow some controls to be relaxed – **cost saving**

### Benefits of having a structured approach

- ISO/IEC 27002 is a logical framework for disparate information security controls, and forms a rational basis for assessing risks & implementing appropriate controls. It is internally consistent and reasonably comprehensive, without being overly prescriptive (especially if users focus on the broader control objectives). It is customizable and forms a good basis on which to build organization/industry-specific extensions as required – **general benefits**

- Provides the impetus to review systems, data and information flows with potential to reduce overhead of duplicated & 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 baseline – **long term benefits**
- Having implemented ISO/IEC 27001 and 27002, the organization will have a comprehensive set of formally-approved information security policies & procedures which are easier for staff & managers to follow consistently – **long term benefits**

#### Benefits of certification

- Will satisfy requests to partners/suppliers to substantiate information security controls without having to service individual enquiries or provide confidential information - **cost saving & risk reduction**
- Provides a rational & independent information security standard against which to assess quality of controls at partners/suppliers - **cost saving & risk reduction**
- Potentially offers a marketing advantage for early-adopters ('badge of honor' similar to ISO 9000 quality standard) – **marketing/sales benefit**
- Reluctance to demonstrate ISO/IEC 27001/2 compliance may be taken as a sign of vulnerability. Certified compliance can promote the company image as a secure business partner – **competitive advantage**
- Helps assure stakeholders, auditors, industry regulators *etc.* that organization is actively minimizing information security risks by demonstrating organizational commitment to information security (corporate governance or due diligence issue given the potential for information security exposures) - **cost saving & risk reduction**

#### Cost avoidance

- Organization may be forced down this route eventually in any event by market pressures, especially if third parties start demanding ISO/IEC 27002 compliance or ISO/IEC 27001 certificates as a prerequisite to eCommerce links *etc.* By implementing it to their own timescales, organizations can choose the most cost-effective sequence of actions – **cost avoidance**
- Governments & industry regulators may insist on ISO/IEC 27002 compliance as a rule. It may be required to demonstrate compliance with data protection/privacy and similar legislation – **legal/regulatory requirement to avoid penalties**
- Potentially reduces or narrows 3<sup>rd</sup> party claims in case of information security failures - **cost saving & risk reduction**

#### Costs

##### Costs relating to organizational change

- Need to raise organizational (staff & management) awareness
- Adaptation/rationalization of existing information security standards, procedures, practices *etc.*
- May need to 'let certain staff go' for not complying with policies *etc.*

##### Design & development costs

- Review/update of existing information security standards, guidelines, procedures *etc.*
- Preparation of (some) new information security standards, guidelines, procedures *etc.*
- (Re-)design of controls architecture

## Implementation costs

- One-off costs to upgrade and/or supplement various existing controls to meet the standard
- Awareness & training costs

## Certification costs

- Initial pre-certification & certification visits by accredited ISO/IEC 27001 certification body (a few \$k)
- 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 & 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 maintenance costs

- Annual review/maintenance of information security policies, guidelines, procedures *etc.* to maintain compliance with standard
- Minor costs to maintain registration (a few \$k) – may perhaps be reduced by combining ISO/IEC 27001 with ISO 9000 certification

## 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](mailto:Gary@isect.com)) or visit [www.ISO27001security.com](http://www.ISO27001security.com) for more information and advice from other ISO/IEC 27001/2 implementers. Good luck!

## Copyright



This work is copyright © 2008, [IsecT Ltd.](#), some rights reserved. It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](#). 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.](#), and (c) derivative works are shared under the same terms as this.

