Cost-benefit analysis for an Information **S**ecurity **M**anagement **S**ystem **(ISMS)** based on the **ISO/IEC 27000 standards**

Version 2025

Executive summary

ISMS business benefits

The primary benefit of the ISMS is to bring information risk and security under firm management control, allowing systematic security improvement where appropriate. Better information security, in turn, will reduce the risk (probability of occurrence and/or adverse impacts) of incidents, cutting incident-related losses and costs.

ISMS implementation and operational 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 mainly relate to the implementation project, changes to governance and security management arrangements, and certification (optional).

Introduction, scope and purpose

Adopting the ISO/IEC 27000 information security standards (commonly known as "ISO27k") generally starts with a discrete implementation project to specify, design, develop and launch the **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS). The ISMS systematically determines and aligns the organisation's information security practices with its information risks. Once up to speed, the ISMS operates indefinitely, directing and controlling information security using the its governance arrangements, management processes, strategies and policies.

This paper identifies the business implications of an ISO27k ISMS as a set of typical or commonplace benefits and costs. It is generic since we have no knowledge of your specific information assets, risks or security controls.

We have provided checkboxes for you to select items that you feel are or are not relevant. This is not a totally comprehensive list however, so you may well think of others to add.

Feel free to use this template both as a source of inspiration for your own ISMS business case, budget request or project proposal to management, and as a framework for measuring and optimising the net value of your ISMS over the long term (*e.g.* combining ISACA's Val IT approach with PRAGMATIC metrics).

ISMS business benefits

These are the ways in which an ISO27k ISMS typically benefits the organisation.

Information security risk reduction

- ☐ Strengthens existing information security control environment by (re-)emphasising 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**
- ☐ Systematic, comprehensive, well-structured approach increases the likelihood that all relevant information security threats, vulnerabilities and impacts are identified, assessed and treated rationally – **risk reduction**
- ☐ Professional, standardised and rational risk management approach gives consistency across multiple IT systems and business processes over time, and addresses information risks according to their relative priorities or significance – **risk reduction**
- ☐ A proactive, forward-thinking approach increases the organisation's resilience and adaptability in the face of significant uncertainties regarding cyber threats, the effectiveness and coverage of information security, competitive pressures *etc.* – **risk reduction**
- ☐ Increases our ability to share certain information risks selectively with 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, more risk-aware, more competent and willing to respond appropriately – **risk reduction**

Benefits of standardisation

- Consistency of approach both internally (throughout the organisation, over time) and externally (the ISO27k standards are popular internationally) – **risk reduction**
- Provides a security baseline *i.e*. a solid platform of commonplace good practice information security controls on which to build or layer additional controls as appropriate – **cost saving**, **risk reduction** and **maturity**
- Generally applicable and hence re-usable across multiple departments, functions, business units and organisations without significant changes, avoids having to specify and justify the same basic controls repeatedly in every situation – **cost saving**
- Allows management to prioritise, concentrating efforts and focusing resources on adequately securing particularly valuable, vulnerable or vital information assets – **cost saving**
- Based on globally recognised and well-respected security standards – **brand value**
- ISO27k standards are being actively developed and maintained by experts, reflecting new security challenges (such as cloud computing, IoT and AI) – **risk reduction** and **brand value**
- Formally defines specialist terms and important concepts, facilitating the discussion, analysis and consistent evaluation of information risk, security *etc*. by various people at different times – **cost saving, maturity** and **risk reduction**
- 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* organisation, as opposed to more rigid and prescriptive standards such as PCI-DSS – **cost saving** and **risk reduction**

Benefits of a structured approach

- A logically consistent and reasonably comprehensive framework/structure for disparate information risks and security controls – **cost saving** and **risk reduction**
- 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**
- A mechanism for measuring performance and incrementally raising the information security status over the long term, growing/adapting the ISMS in line with the evolving business and its information risks *e.g*. new technologies, new products and markets, new partners – **cost saving**, **risk reduction** and **maturity**
- A coherent set of information security policies, procedures and guidelines, tailored to the organisation, formally approved by management, consistently implemented and proactively maintained – **maturity** and **risk reduction**

Benefits of certification

- Formal confirmation by an independent, competent assessor that the organisation's ISMS fulfils the requirements of ISO/IEC 27001 – **risk reduction, maturity** and **brand value**
- Provides assurance regarding an organisation'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, risk reduction** and **brand value**
- Positions the organisation as a secure, trustworthy and well-managed business partner, employer and investment opportunity – **brand value**
- Establishes management's explicit commitment to information security for corporate governance, compliance, safety, privacy, due diligence, business and ethical purposes – **cost saving**, **risk reduction** and **brand value**

Benefits of conformity and compliance

- Facilitates, supports, enables and encourages compliance with information security, privacy, safety, governance and other applicable, mandatory laws and regulations, plus conformity with discretionary requirements in strategies, policies, contracts and agreements – **maturity, risk reduction** and **brand value**
- Provides an overarching framework for information risk and security management addressing a broad range of both external and internal requirements, leveraging the common elements – **cost saving** and **risk reduction**
- Involves compiling, evaluating and maintaining pertinent information (inventories) concerning information assets, vulnerabilities, threats, security controls *etc*. – **maturity**
- Stakeholders or authorities may at some point *insist* that the organisation complies with ISO27k as a condition of business or to satisfy privacy and other laws, whereas implementing and conforming with it on management's own terms and timescales is a proactive, cost-effective approach *e.g*. prioritising aspects that offer the greatest business value; taking advantage of planned IT system or facility upgrades to improve security at minimal extra cost and disruption – **brand value, maturity** and **cost saving**
- Demonstrably adopting and investing in globally-recognised good practices provides management with a valid, legitimate defence in case of legal/regulatory enforcement or stakeholder claims following information security or privacy incidents – **cost saving, brand value** and **risk reduction**

ISMS implementation and operational costs

These are the main costs associated with the **management system** elements of an ISO27k ISMS[1].

ISMS implementation project management costs

- ☐ Prepare an overall information risk and 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 necessary resources
- ☐ Identify, recruit, direct and support a suitable project manager (usually the person who will ultimately become the CISO or Information Security Manager) and team members – whether full or part-time, consultants, contractors, temps or permanent employees
- ☐ Hold regular project management meetings involving key stakeholders, and liaise as necessary with various other interested parties, parallel projects, managers, business partners *etc*.
- ☐ Track actual progress against the plans and circulate regular status reports/progress updates
- ☐ Identify and deal with project risks and changes

Other ISMS implementation costs

- ☐ Acquire (buy or license) the standards
- ☐ Compile and validate an inventory of information assets in scope of the ISMS
- ☐ Identify and assess risks to information assets, evaluate and prioritise them
- ☐ Determine how to treat information risks (*i.e.* mitigate them using suitable security controls, avoid them, share them and/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*.
- ☐ Rationalise, implement additional, upgrade, supplement or retire existing security controls and other risk treatments as appropriate
- ☐ Conduct security awareness and training, such as introducing new security policies and procedures and fostering the corporate security culture
- ☐ Investigate and apply sanctions for serious non-conformities

[1] Note that the ISO27k standards *recommend* but do not *require* any specific information security controls – it is up to management to evaluate and treat the organisation'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, whether within the ISMS proposal or separate as risk reduction/security improvement project proposals.

Certification costs

- Select a suitable accredited certification body, negotiating and contracting for stage 1 (pre-certification) and stage 2 (certification) audits, and potentially annual surveillance audits and 3-yearly full audits to maintain the certification indefinitely
- Risk of failing to achieve certification at first attempt[2]
- Staff/management time expended during annual surveillance visits

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*.
- Costs to maintain certification (annual surveillance audits, 3-yearly recertification audits)[3]

Conclusion

Although we admit a strong bias, we honestly believe the business benefits of an ISO27k ISMS *far* outweigh the costs for most organisations. By all means contact the author Gary@isect.com or visit www.SecAware.com and www.ISO27001security.com for more.

An **ISMS business case template** building on this paper is provided in the SecAware ISMS Take-off package, along with other materials for the management audience – briefings, advisories, policies, procedures, job descriptions, audit checklists *etc.*

Document history

2025: revised several items. Added "maturity" as a benefit class.

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

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

2012 and **2017:** revisions.

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

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

Copyright

[2] Since any show-stoppers raised by the auditors probably represent unacceptable information risks, this item could equally be a risk-reduction benefit!

[3] Certification-related costs may be shared across other ISO management systems