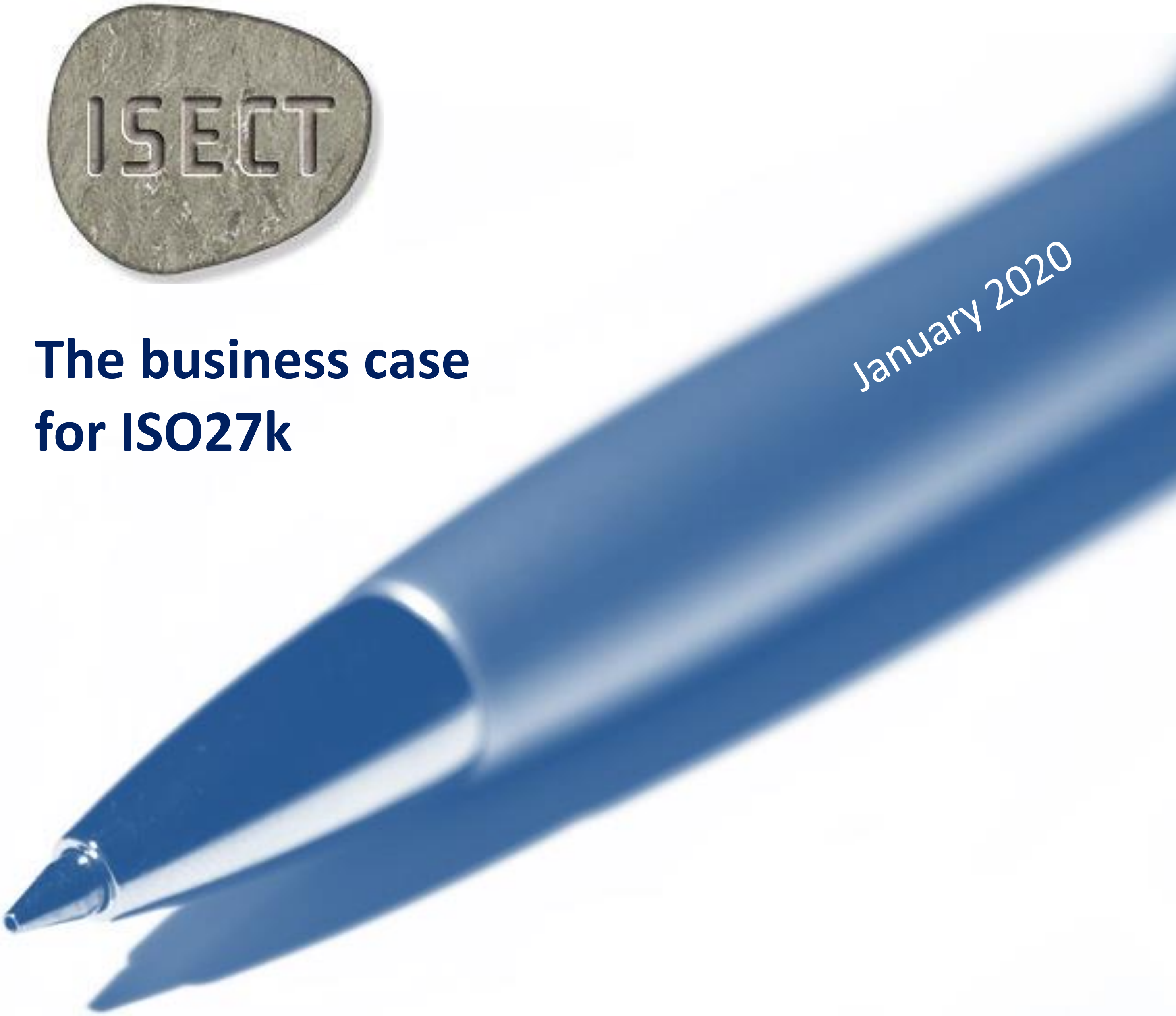
The business case for ISO27k



January 2020

Summary

This paper elaborates A-to-Z on the *typical* benefits (advantages) and costs (drawbacks) of the ISO/IEC 27000 "ISO27k" information security management standards. Use it to construct *your* business case, budget request or project proposal to adopt ISO27k or, if you already have an **I**nformation **S**ecurity **M**anagement **S**ystem in operation, find ways to squeeze *even more* business value from it.

Business case for adopting the ISO/IEC 27000-series "ISO27k" standards

Dr Gary Hinson MBA, IsecT Ltd. CEO

A

Access: widespread adoption of the ISO27k standards creates a global pool of competent expertise, information and services in this area, supplementing the standards themselves.

Competent professionals with ISO27k qualifications and extensive practical experience are in high demand and don't come cheap!

> "An asset owner should be identified for each asset, to provide responsibility and accountability for the asset. The asset owner perhaps does not have property rights to the asset, but has responsibility for its production, development, maintenance, use and security as appropriate. The asset owner is often the most suitable person to determine the asset's value to the organization"
>
> *ISO/IEC 27005*

Accountability: holding asset owners accountable for adequately protecting and exploiting 'their' information assets is a powerful means of ensuring that the associated information risks are properly identified and treated. Asset owners for the most important and valuable corporate information are generally senior/executive managers with the business perspective, resources and wherewithal to get things done. The possibility of their being held *personally* to account for incidents is curiously motivating.

Alignment: ISO management systems align at conceptual and practical levels, for instance they all support the notion of continuous improvement and share key terms such as 'nonconformity' and 'corrective action'.

> "Evaluating an ISMS at planned intervals by means of internal audits provides assurance of the status of the ISMS to top management. Auditing is characterized by a number of principles: integrity; fair presentation; due professional care; confidentiality; independence; and evidence-based approach."
>
> *ISO/IEC 27003*

Assurance: certified compliance of the organization's ISMS with ISO/IEC 27001 by a competent and accredited certification body is strong form assurance, widely recognized. It is an independent endorsement of the organization's approach, a valuable confidence boost for management and other stakeholders, such as auditors, owners/investors and evaluators.

Attraction: skilled, competent professionals familiar with the ISO27k standards are more inclined to work for organizations that are certified or are seeking certification, since management supports and has committed to information risk and security. Investors are more inclined to invest in organizations that take important responsibilities seriously.

Workers who are unable or refuse to adopt the ISO27k approach may no longer justify their positions. 'Letting people go' may be the best option.

Availability of information for legitimate business purposes is one of the core objectives of information security. The ISMS information risk management approach ensures that security controls (*e.g.* access controls, backups, business continuity controls) support, enable and do not adversely impact *appropriate* access to and use of information by *authorized* workers.

B

Baseline: for organizations taking their first tentative steps, an ISO27k ISMS is a solid foundation on which to build – specifically, the governance aspects such as a set of policies and procedures define and stabilize the information risk management decisions and security activities, enabling them to be managed systematically.

> "The scope of the information security risk management process needs to be defined to ensure that all relevant assets are taken into account in the risk assessment. In addition, the boundaries need to be identified to address those risks that can arise through these boundaries."
>
> *ISO/IEC 27005*

Boundaries: through its defined scope, the ISMS 'ring fences' information assets, risks and controls, both containing and excluding things. Within the boundary, management has a better understanding of, and more control over, the information risks and security requirements. Outside the boundary, risks that could affect information within the ISMS still need to be addressed, but the boundary itself represents an additional point of control.

Brand value: the ISO/IEC 27001 compliance certificate has marketing potential, enhancing the organization's brands by reassuring customers, owners and other stakeholders that management is serious about protecting information.

If marketing is the *sole* reason for ISO27k certification, a minimalist approach may be sufficient but the organization may miss out on other business benefits.

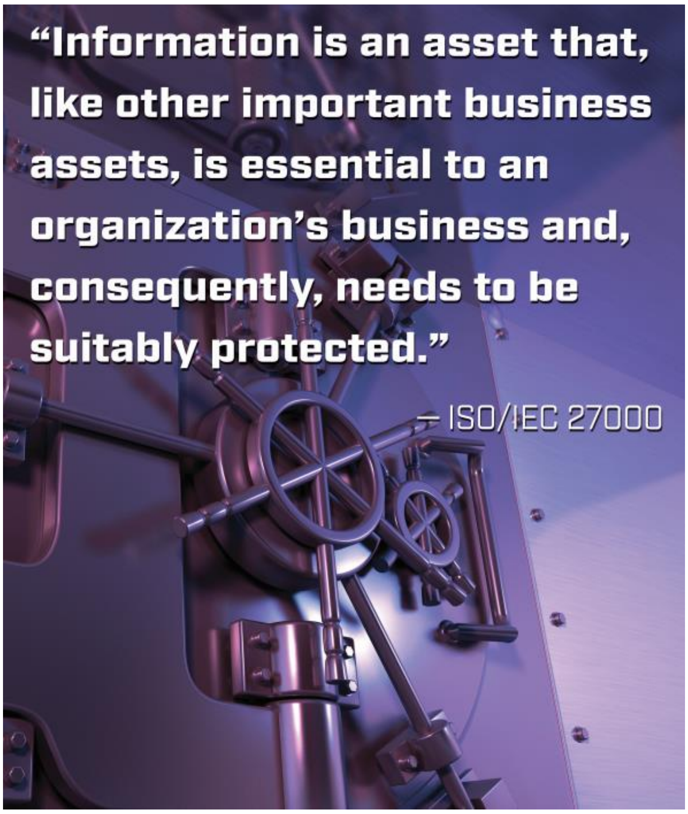
Business continuity: whereas the ISO27k standards are disappointingly weak in this area, they complement and support business continuity management such as that recommended by ISO 22301, blending resilience, recovery *and* contingency. Without adequate protection for vital information, information systems and so on, business continuity and hence the organization's survival are far from guaranteed. It's an essential foundation.

Business enablement: information security allows the organization to conduct business activities confidently, entering into relationships, markets and situations that would otherwise be too risky. An ISO27k ISMS provides the governance and assurance framework.

Business Impact Analysis: the BIA typically conducted for business continuity purposes is an excellent source of information for the ISMS. Business-critical processes are enabled and supported by business-critical information, information systems, and so on, hence it is critically important that the associated risks are under control.

> "Risk acceptance criteria should be developed and specified. Risk acceptance criteria often depend on the organization's policies, goals, objectives and the interests of stakeholders. An organization should define its own scales for levels of risk acceptance."
>
> *ISO/IEC 27005*

Business-driven: ISO27k supports the adoption of governance, management, risk and security arrangements according to the situation, in a business-like manner. Management gets top identify, evaluate and decide how best to satisfy the organization's needs, including compliance requirements imposed upon it by the authorities, business partners and society at large. For instance, privacy laws and regulations such as GDPR do not specify technical details such as the particular data encryption algorithms and key lengths required to keep personal information confidential: through its ISMS processes, the organization figures out exactly what is needed *and* makes sure the requisite controls are implemented and maintained accordingly. If privacy is vital to the business, stronger controls are justified, going beyond the compliance requirements. If not, the compliance requirements need to be satisfied. Either way, the ISMS supports management in achieving business objectives.


"Information is an asset that, like other important business assets, is essential to an organization's business and, consequently, needs to be suitably protected."
– ISO/IEC 27000

C

Clarity: ISO27k brings a clear, meaningful and sound basis for designing, implementing, managing and evaluating an organization's approach to information risk and security. ISO/IEC 27001 succinctly specifies the key elements of an ISMS, no messing.

Competence: management's concern, support for and investment in information security, privacy, compliance *etc*. is leveraged by employing ISO27k's good practices.

Competitive advantage: an organization that is stronger and more resilient than its competitors and neighbours is less likely to become a victim in the first place, and better placed to deal efficiently and effectively with any incidents that do occur. Conversely, an organization that lags the field is a sitting duck.

Compliance: aside from the obvious compliance with ISO/IEC 27001, the certificate indicates that the organization is willing and able to satisfy third party requirements rather than being purely self-centred, 'a law unto itself'.

'Surrogation' is the unhelpful tendency to focus *solely* on achieving certification regardless of what would actually be best for the organization.

Comprehensive: the ISO27k standards promote an all-encompassing approach to protecting valuable information, including personal and proprietary information, intellectual property and knowledge. If information is the modern organization's life-blood, it's not sufficient to protect the brains in IT, since any part of the body can bleed out.

> "The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed."
>
> *ISO/IEC 27001*

Confidentiality: keeping sensitive proprietary and personal information safe involves allowing access or disclosure for authorized and appropriate purposes while preventing unauthorized and inappropriate use. Although this is an important role for information security, it's not the only one: see also **availability** and **integrity**. ISO27k's broad perspective on information risk and security promotes a balanced view of the protective measures, such that *legitimate* and *appropriate* use of information is not unduly restricted.

Classification schemes tend to over-emphasize secrecy and privacy, interfering with the free-flow of information within the organization. Taking integrity, availability and utility into account complicates matters and can confuse people … but may be worth it.

> "The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system."
>
> *ISO/IEC 27001*

Continuous improvement: ISO27k facilitates and encourages ongoing refinements to the information risk and security management arrangements, constantly adapting to the changing requirements and building on experience gained (whether by the organization itself, or by third parties, shared by the wider information risk and security management community).

Control: in addition to various information security controls, ISO27k offers a coherent suite of management and process controls … which are in fact even more important. With the right information risk management process in place, the organization can systematically identify, design, implement, use, monitor, manage and maintain the particular security controls which it needs. It doesn't matter, for instance, that the current release of ISO/IEC 27002 neglects to specify the AES encryption algorithm: if the organization determines a need for strong 'military grade' encryption, AES is one of several available options. Management remains in control.

D

Demonstrable information security: certification requires the organization to *demonstrate* its capabilities, providing evidence that its processes are operating in order to convince the auditors that it is actually doing what it should be doing according to ISO/IEC 27001. A certified ISO27k ISMS is more than just a paper tiger.

> "Documented information is needed to define and communicate information security objectives, policy, guidelines, instructions, controls, processes, procedures, and what persons or groups of people are expected to do and how they are expected to behave. Documented information is also needed for audits of the ISMS and to maintain a stable ISMS when persons in key roles change. Further, documented information is needed for recording actions, decisions and outcome(s) of ISMS processes and information security controls."
>
> *ISO/IEC 27003*

Documentation: whereas some consider it 'mere red tape', documentation *or 'documented information' in the stilted language of the standards) constitutes a valuable record of what has been decided and done, guides future decisions and actions, enables reviews, assessments, audits and process improvements, and is invaluable for awareness and training purposes. The real trick, though, is to keep it reasonably succinct and on-topic, brief but not too vague.

Due care: adoption of ISO27k, especially if certified, indicates management's acceptance of and willingness to meet an externally-specified standard of information risk and security management, as opposed to doing whatever they choose – potentially nothing at all. It may constitute a credible defence against claims of incompetence or negligence in the event of serious information security incidents or privacy breaches.

> The compliance certificate alone *may* be sufficient proof of due care, although additional evidence may be required if there are specific compliance obligations or other explicit, mandatory requirements.

> "The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system."
>
> *ISO/IEC 27001*

E

Effectiveness: strong linkages between information security controls and information risks enables management to focus attention and resources on the things that matter most. For instance, rather than seeking legal and regulatory compliance purely to satisfy externally-imposed requirements, the business benefits are emphasized – as demonstrated by this very document.

> *Any* corporate initiative *can* go about things in the wrong way, have invalid or inappropriate goals, or be mismanaged. ISO27k is just the same.

Efficiency: aside from ISO27k offering a ready-made governance structure and approach to the management of information risks, *certified* compliance by accredited certification bodies increases assurance and reduces the need for evaluation, assessment and audits by third parties. True, individual organizations may seek additional assurance regarding their unique requirements or compliance obligations, but ISO27k compliance establishes a solid base level plus the documentation and other evidence typically needed for third party review.

F

Familiarity: managers and professionals familiar with any other ISO **M**anagement **S**ystems will notice similarities in the **I**nformation **S**ecurity **MS**, and *vice versa*. Although the concerns and processes being managed clearly differ between MSs, the same governance structures and overall management approaches apply.

Financial *and* non-financial benefits: aside from reducing the financial losses and costs arising from information security incidents, many of the ISMS benefits identified in this paper are not purely financial *e.g.* the assurance and good practice aspects.

> There are financial and non-financial *costs* too *e.g.* directing corporate resources into the ISO27k implementation project can limit progress elsewhere; the standards constrain management's options.

Flexibility: whereas information security standards such as PCI-DSS rigidly demand specific controls, the ISO27k standards can be applied sensibly to all types and sizes of organization, allowing them to adapt to changing risks and security requirements over time. It's not a complete free-for-all, though, as information risks drive the ISMS in whatever directions are most appropriate for the organization.

Forward-thinking: don't wait until you experience a serious information security incident to discover just how poor your information security arrangements are. It might be too late for the organization. ISO27k helps avoid or prevent situations that could prove terminal.

G

Good practice: ISO27k promotes information risk and security management practices widely acknowledged as being good security practices. The international committee responsible for the standards is comprised of experienced, competent professionals from a wide variety of cultural and professional backgrounds.

> These are good but not necessarily the very best practices. They are also incomplete and a little behind the times due to ISO's glacially slow processes for developing and publishing the standards.

Governance: ISO27k provides a sensible means of directing, monitoring and controlling the organization's management of information risks, security controls, compliance *etc.*

Holistic: the ISO27k standards are intentionally broadly-scoped, dealing with all manner of risks to information communicated, stored and processed in various formats. In contrast, "cybersecurity" *tends* to over-emphasize deliberate attacks on IT systems, networks and digital data to the extent that human aspects (such as simple errors) and non-IT information assets *may* be neglected. ISO27k helps ensure that all substantial information risks are addressed appropriately, regardless of their nature.

Improving security: it's a rare organization that implements ISO27k *without* improving its information security status! Aside from bolstering any defensive gaps, the ISMS provides a rational basis for prioritizing and instituting security improvements according to the risks.

Security improvements aren't free, but at least the ISMS processes clarify their objectives and benefits, enabling management to decide what's best for the organization.

Independent benchmark: unlike corporate strategies, policies and procedures, the ISO27k standards were not written by or for the organization specifically, independently setting information risk and security management expectations of all organizations.

Information risk management: the ISO27k standards revolve around actively managing risks to and involving information. It is appropriate to mitigate *some* information risks using information security controls, but not all – hence there's more to ISO27k than information security management.

Cultural changes can be a significant cost in organizations that are not ready to adopt ISO27k. The approach is not driven by lists of security controls, but by information risks of concern to the business. Some people can't handle that!

Integrity: a core element of information security, integrity is relevant to IT systems, networks, data, apps, information, messages, people, organizations, processes, decisions, intentions, agreements, relationships, trustworthiness, ethics and more. It's often neglected or taken for granted until an integrity failure incident occurs (= too late!). ISO27k encourages us to pre-empt and so avoid or mitigate failures of integrity, confidentiality or availability of information through information risk management.

> "It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization."
>
> *ISO/IEC 27001*

Integration: ISO has published 14 management systems standards so far: ISO 9001 (quality); ISO 13485 (medical devices quality); ISO 14001 (environment); ISO 18788 (private security); ISO/IEC 20000-1 (IT service management); ISO 22000 (food safety); ISO 22301 (business continuity); **ISO/IEC 27001 (information security**); ISO 28000 (supply chain security); ISO 37001 (anti-bribery); ISO 39001 (road traffic safety); ISO 45001 (health and safety); ISO 50001 (energy); and ISO 55001 (assets). They are sufficiently similar in design and purpose that organizations may choose to align, perhaps even integrate them, at least in part – for instance establishing incident management function for all manner of events, incidents and disasters, or a change management function that handles all kinds of changes consistently.

International recognition: thanks to the way the standards themselves are written, plus the associated compliance assessment formalities, valid ISO/IEC 27001 compliance certificates issued by any duly accredited certification body, anywhere on the globe, are functionally equivalent.

Although costly, those accreditation and certification formalities, along with the scope and Statement of Applicability, are important for organizations that depend on other organizations' ISO27k certifications.

J

Journey: while most organizations treat ISO27k implementation as a project that ends with certification, in reality that is just the start of the management system's operation. As with systems development projects in general, implementation marks a significant milestone rather than a final destination.

K

Knowledge: the ISO27k standards comprise a body of knowledge contributed by various experts in the field, a valuable resource in the form of generally-accepted good security practices. Furthermore, the standards recommend practices designed to protect and exploit knowledge and other forms of information held by organizations.

L

Lingua Franca: with the ISO27k standards in use around the globe, the language of ISO27k, the concepts and terms, are widely understood.

There can be cultural differences, however, for instance different takes on 'risk', 'compliance' and 'management'.

M

Management: many small organizations lack the resources to address information risk and security properly. ISO27k covers the governance aspects and business drivers, leaving management to make the best of available operational resources or supplement them as appropriate (*e.g.* employing ISO27k consultants, decision support and document management systems), according to the business context. Although larger organizations tend to have departments or teams already (often several!), the governance and management system approach from ISO27k can prompt reviews, leading to restructuring and realignment or endorsement of the current structure.

> "The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard."
>
> *ISO/IEC 27001*

Maturity: implementing ISO27k, especially with certification, demonstrates an organization's relatively mature, systematic and deliberate approach to information risk and security management, compared to *ad hoc* or informal arrangements anyway. Furthermore, the ISMS itself achieves maturity through continuous improvement. The ISMS is designed to adapt to changing circumstances, capturing and exploiting the knowledge and experience gained in the course of operating the ISMS and dealing with risks, controls, near-misses and incidents.

> "Measurement is an activity undertaken to determine a value, status or trend in performance or effectiveness to help identify potential improvement needs. Measurement can be applied to any ISMS processes, activities, controls and groups of controls."
>
> *ISO/IEC 27004*

Measurable: appropriate security metrics both drive and demonstrate progress towards the organization's defined goals for information risk and security management. Organizations that have an *ad hoc* and generally unsatisfactory approach to security metrics should find ISO27k, and ISO/IEC 27004 in particular, beneficial.

The *next* release of ISO/IEC 27004 may incorporate leading-edge approaches such as Goal-Question-Metric and PRAGMATIC – or it may not: it all depends on the vagaries of the ISO/IEC committee.

N

Neutrality: in situations involving multiple organizations needing to collaborate and coordinate on information risk and security matters (such as vehicle manufacturing, finance and defence supply networks), the global nature of ISO standards offers a neutral, unbiased, mutually-acceptable approach, forming a common, shared baseline.

ISO27k may form the 'lowest common denominator' as it does not demand particular information security controls that others expect. It may well be necessary to build on the platform, specifying additional controls – which is the approach promoted by ISO/IEC 27011 (telecoms), ISO/IEC 27019 (energy utilities) and ISO 27799 (healthcare).

O

Optimization: ISO27k helps the organization make the best of available resources, avoiding waste, duplication and low-value activities by prioritizing what's important to the business in relation to managing its information risks. The priorities aren't fixed in concrete, however, enabling the organization to respond appropriately to risks and opportunities as they arise.

Optimization depends on the context, so ISO27k cannot specify optimal or ideal security controls.

Oversight: an ISO27k ISMS gives management the information and tools to oversee (as in monitor, direct and control) information risk management and security activities within the organization. Oversight extends to external stakeholders as well in the sense that ISO27k compliance indicates a systematic, structured approach to governance and management of information risk and security.

> "Top management should require and regularly review reporting of the performance of the ISMS."
>
> ISO/IEC 27003

P

Performance: combining the *effectiveness* and *efficiency* aspects, a high-performance ISO27k ISMS does the right things (addresses information risks of concern) and does things right (treats the risks appropriately).

Planning: several steps in the ISMS implementation project (such as identifying and evaluating information risks, selecting and implementing risk treatments, and conducting ISMS internal audits) have to be performed in sequence prior to certification. Once the ISMS is fully operational, several information risk and security management activities are regular or again follow a defined sequence when initiated (*e.g.* incident management). Such sequences simplify the planning in the sense of providing route-maps.

Sequences can also impose constraints on planning, such as dependencies, conflicts and contention for limited resources.

Premium increases: organizations that don't appear to be taking their responsibilities seriously may be charged higher premiums for cyberinsurance, business interruption or other cover, plus there is a greater chance of any claims being scaled back or completely refused, *and* cover being denied for future events (a hidden cost of incidents).

> "Organizations and their contexts are never static. In addition, the risks to information systems, and the ways in which they can be compromised, are evolving rapidly. Finally, no ISMS is perfect; there is always a way in which it can be improved, even if the organization and its context are not changing."
>
> ISO/IEC 27003

Pragmatic: in contrast to prescriptive standards, ISO27k is designed to be interpreted and employed according to the particular organizational/business context. As we said, it's a flexible approach that adapts and responds to the ever-changing situation.

Progressive: focusing on improvement naturally emphasizes *future* directions, hence the endless quest to achieve change-for-the-better. On top of that, the ever-expanding remit of ISO27k encourages organizations to up their game in emerging areas such as privacy, cloud security and IoT security, complementing and extending the core activities.

> "Risks should be identified, quantified or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization."
>
> ISO/IEC 27005

Priorities: the combined information risk focus and business drive of an ISO27k ISMS is extremely helpful in clarifying the organization's priorities.

You probably find this lengthy business case paper overwhelming since it is generic and follows a crude A-to-Z sequence rather than reflecting your organization's situation. Feel free to sift out the issues that matter most into a shortlist you can handle.

Privacy: significant overlaps mean that improving information security naturally tends to improve privacy at the same time, a valuable side-effect. Privacy is one of the few compliance areas called out in Annex A to ISO/IEC 27001 as an aspect of concern to any organization that holds personal information on employees, customers and other business contacts. Many other legal, regulatory, contractual and ethical compliance obligations also have information security implications *e.g*. tax and accounting laws impose data integrity requirements on the financial systems and processes.

While other information security-related compliance requirements may be managed outside the ISMS, they should at least be coordinated/aligned in order to avoid conflicts, gaps and inefficiencies.

Proactive: a purely reactive approach to information security – essentially clearing-up after incidents – falls *well* short of generally accepted good security practices. Identifying, evaluating and treating information risks is far more proactive and business-like, particularly if incidents are completely avoided or substantially mitigated by effective security controls. Being certified compliant with ISO/IEC 27001 demonstrates management's proactivity: they could have chosen to 'adopt', 'use' or 'implement' the ISO27k standards *without* being certified, but no they bravely decided to go the extra mile and prove it.

> "Not every objective can be measurable, but making objectives measurable supports achievement and improvement. It is highly desirable to be able to describe, qualitatively or quantitatively, the degree to which an objective has been met."
>
> *ISO/IEC 27003*

Proportional: linking security controls to the nature and severity of information risks gives management the power to decide what security is necessary in the specific context of the organization. The risks and hence security requirements will vary markedly between, say, a corner shop, a tax advisor, a bank and a government department, yet ISO27k guides them all.

Management's role is clearly crucial in this. A naïve, careless, negligent or unethical management has the latitude to make inappropriate decisions.

Protection: ISO27k protects and enhances the value of information assets by facilitating the legitimate exploitation of information while managing the associated risks.

Q

Quality assurance: ISO's management systems stem from the ISO 9001 QA standards, and the cyclical **P**lan-**D**o-**C**heck-**A**ct approach to continuous improvement championed by Deming in Japan in the 20th Century. Although PDCA no longer features explicitly in the ISO27k standards, continuous review, refinement and improvement remains an integral and valuable part of the ISO approach.

ISO27k doesn't formally *demand* even the most basic of security controls be implemented. Instead, the ISMS enables management to implement *whichever security controls they deem necessary to address the organization's information risks*. A certified organization may not be 'secure' in an objective sense … but it is heading the right way, a leap of faith.

R

Raising-the-bar: although the requirements of ISO27k are not particularly arduous, the standards do at least define a workable set of processes to manage and systematically improve information risk and security, leading to incremental improvements across the ever-expanding cadre of organizations adopting the standards.

> "Risk assessment is often conducted in two (or more) iterations. First, a high level assessment is carried out to identify potentially high risks that warrant further assessment. The next iteration can involve further in-depth consideration of potentially high risks revealed in the initial iteration."
>
> *ISO/IEC 27005*

Rationalization: bringing information risk and security management practices into alignment with ISO27k presents opportunities to review what is going on and reconsider the way things are done. This benefit extends to related areas such as privacy, compliance and business continuity management.

ISO27k brings challenges and risks as well as opportunities. Mature processes in, say, business continuity or compliance management *may* prove tricky to align or integrate with the ISMS in practice.

Reducing direct and indirect incident costs: ISO27k assists the organization's management of information risks by reducing the number and/or consequences of incidents, hence reducing costs and penalties arising from incidents (*e.g.* GDPR fines, business disruption). More subtly, a systematic approach to managing information security helps management optimise the organization's security investments by aligning them with information risks and business requirements. Rather than collecting shiny new toys, the information security professionals are required to justify investments on business grounds – this paper being an example. Clarifying the expected returns helps monitor, drive and achieve them.

> "Overall, management review is a process carried out at various levels in the organization. These activities could vary from daily, weekly, or monthly organizational unit meetings to simple discussions of reports. Top management is ultimately responsible for management review, with inputs from all levels in the organization."
>
> *ISO/IEC 27003*

Reduction in audits, reviews and assessments: the interminable 'vendor security questionnaires' are somewhat reduced by a certified organization's ability to demonstrate its capabilities in this area with a valid ISO/IEC 27001 compliance certificate.

ISO/IEC 27001 requires management reviews, internal audits and external (certification) audits.

Reputation: generally speaking, certified compliance to international standards indicates an organization's willingness both to adopt generally-accepted standards of good practice, and to invest in raising its game in the respective area. That implies brand-enhancing business value.

If that's not a convincing argument, consider the alternative: are you happy for the organization to be considered a laggard, unwilling to take information security and related matters (such as compliance, privacy and business continuity) seriously?

Resilience and strength: ISO27k promotes *proactive* information risk management, reducing the probability and/or impact of possible *future* incidents. In the same way that an Olympic athlete makes strenuous efforts to become fitter and hence more capable of succeeding in competitions, organizations who 'swallow the ISO27k pill' deliberately position and prepare themselves for future success, whatever occurs. They aren't entirely immune to trouble but are more prepared to cope with it.

Retention of custom: if existing customers, suppliers and partners lose confidence in the organization's ability to protect their interests (*e.g*. following a significant privacy breach or malware infection), that may be sufficient cause for them not to renew their contracts, or at least to *threaten* to do so, pressuring the organization into making concessions. Implementing ISO27k can pre-empt such situations, preparing the organization to demonstrate that it is dealing professionally with whatever transpires.

> "Information security risk treatment is the overall process of selecting risk treatment options, determining appropriate controls to implement such options, formulating a risk treatment plan and obtaining approval of the risk treatment plan by the risk owner(s)."
>
> *ISO/IEC 27003*

Risk-alignment: 'risk' can be a difficult concept to grasp, but essentially it involves considering the possibility of things going wrong. In the ISO27k context, that may involve hackers, ransomware, equipment failure, fraud, accidents, power cuts, errors and omissions, physical disasters, lies and deceit, disclosure of proprietary or personal information, bugs, floods … and *much* more. Evaluating the possibilities helps management determine what must, should, could or might to be done to protect information, setting priorities.

> "Risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level."
>
> *ISO/IEC 27005*

"Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization."

— ISO/IEC 27000

Risk-based: in contrast to prescriptive approaches such as PCI-DSS, with ISO27k organizations adopt whatever information security controls and other risks treatments best address their information risks. Significant risks imply the need for strong, reliable and effective controls, focusing attention on the things matter most. This is a dynamic approach that reflects *current* risks, rather than addressing whatever risks were important when the standards were written … which may have been several years earlier.

Route-map: the ISO27k standards lay out a route from wherever the organization starts today, through a defined series of steps leading to certification, and then onwards toward maturity thanks to the ISO27k governance arrangements and management processes.

Safety and security: the incessant spread of automation inevitably leads us to become more dependent on machines and devices controlled by computers processing information. The availability and integrity of the information and the processing therefore have implications for the safety of people, passengers in driverless elevators, trains and cars for instance, but this is a far bigger issue. Modern society depends on 'critical infrastructure', ranging from safe, potable water, reliable communications and energy supplies to financial and commercial systems, manufacturing industry, and public services provided by governments funded by our taxes. We *must* invest in the secure platforms to protect our systems, networks, data, information and social structures against an uncertain but potentially devastating future. There's no time to waste: act now, before it's too late!

> "The scope defines where and for what exactly the ISMS is applicable and where and for what not ... The organization should also consider activities with impact on the ISMS or activities that are outsourced, either to other parts within the organization or to independent suppliers. For such activities, interfaces (physical, technical and organizational) and their influence on the scope should be identified."
>
> *ISO/IEC 27003*

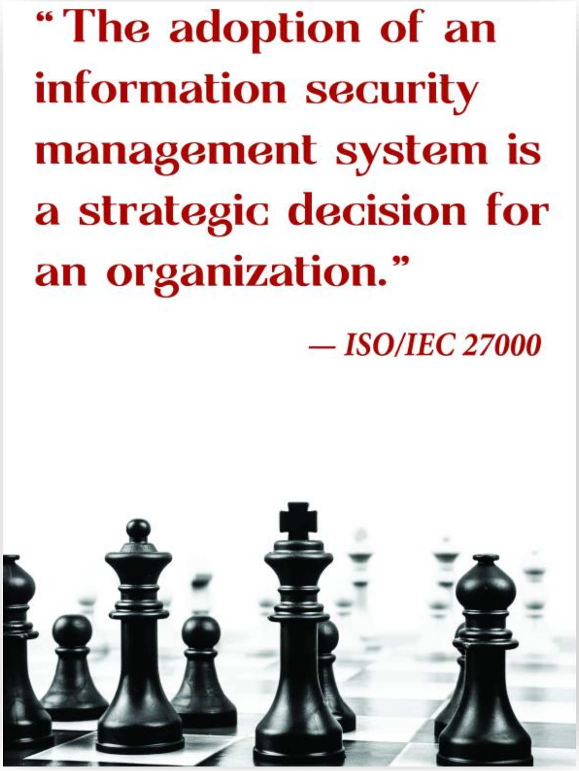
Scope: within the defined scope of an ISMS, information security is managed systematically and competently to high standards, reflecting the information risks. Beyond the boundary (potentially including other parts of the same organization), information security management is inherently less trustworthy since it *may* not be managed to the same high standards.

Secure-by-design: the idea of 'building security in' to the organization's products (goods and services) is not new, but is easier said than done. The rational risk-driven ISO27k approach makes it easier and more likely to happen in practice. Simply recognising that information security may be one of the factors of concern to customers is a good start, while the policies and procedures enable information risk and security objectives to be met.

> "The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time."
>
> *ISO/IEC 27001*

Strategic, tactical *and* operational benefits: uncertainties about whether and when incidents may occur are part of the risk, in addition to who or what may cause them and what the consequences may be. Risks of incidents in the near term tend to be easier to identify and evaluate than those in the mid to long-term, but we can't afford to just ignore uncertain situations. ISO27k supports a risk-based strategy, enabling us to foresee and forestall or at least minimize the frequency and impacts of incidents involving information.

Structured, rational, systematic and rigorous approach: rather than implementing controls on a whim or simply because they are popular or suggested, ISO27k helps organizations identify, evaluate and treat information risks sensibly.


" The adoption of an information security management system is a strategic decision for an organization."
— ISO/IEC 27000

T

Traceability: an organization's information risk and security management processes and decisions are traceable to its policies and procedures, which in turn are traceable to both the organization's business objectives in this area, plus relevant ISO27k standards and other compliance obligations. If the ISMS is certified, there is greater assurance since the key elements have been independently and competently assessed for compliance.

Transparency: certified organizations are open about their compliance with and hence acceptance of the ISO27k standards. Their management has committed to ensuring that the ISMS is sufficiently well resourced for certification, indicating their support for the principles of information risk and security management.

Commitment relies on management understanding the implications and having the integrity to 'make it so', not just for the initial ISMS implementation up to certification but thereafter … re-emphasizing the business case, hence this awareness briefing.

Trustworthiness: we touched on this earlier. Trustworthiness and trust are strongly associated with commitment, integrity and assurance. ISO27k bolsters them all.

U

Universal applicability: the ISO27k standards are widely-scoped, generic and flexible, enabling them to be applied sensibly in all manner of organizations regardless of their size, industry, structure, profit/social orientation *etc*.

Generality means a lack of specificity: ISO27k standards are not simple, prescriptive checklists of *things to do*.

V

Validation: the organization's approach to information security is validated by reference to the ISO27k standards, and by its compliant risk management processes that prioritize the identification and appropriate treatment of significant information risks.

W

Widely recognised: according to the latest ISO Survey, more than 30,000 ISO/IEC 27001 certificates were issued to organizations in 168 countries by the end of 2018, well short of ISO 9001's 878,000 certified quality management systems but clearly popular. We can only guess how many other organizations are using ISO27k informally or are in the process of becoming certified.

X

eXemplifies a modern, proactive approach to information risk and security management. Rather than reacting retrospectively to information security incidents, ISO27k encourages organizations to get ahead of the game by identifying and treating risks, ideally *before* incidents occur.

Y

Yardstick: an ISO/IEC 27001 compliance certificate confirms that an organization has adopted ISO27k to manage its information risks systematically. Certification *proves* that it has cleared the compliance hurdle (the yardstick), and takes information security seriously enough to invest in a compliant ISMS. A compliant ISMS, in turn, provides the governance framework and structures to manage, measure, direct, control and improve its information security, addressing changes and challenges as they arise.

Year-round effort: the ISO/IEC 27001 certification and re-certification audits roll around every 3 years, with "surveillance audits" every 6 to 12 months to check that nothing has substantially changed the organization's compliance status. Management reviews and ISMS internal audits further reinforce the need to maintain the ISMS as intended. In practice, therefore, the ISMS operates continuously, all year long.

Z

Zero trust: distrusting insiders as much as outsiders is information security's response to increasing threats from *within* the corporate network, including fraudsters, hackers and malware (such as ransomware). A comprehensive, all-encompassing approach to security is infeasible without being systematic and thorough about it … which is where ISO27k comes into its own.

Conclusion

I'll be honest: this *is* a biased document. I am, after all, an information risk and security management professional with a deep passion for the subject and extensive experience with the standards since the 1990's. Nevertheless, would you agree that the benefits of ISO27k eclipse the costs? Either way, I hope this has prompted you to maximise the net worth of your ISMS, optimising the business value.

Further information

For help to construct or refine your business case and plan your ISO27k implementation, please contact the author. I'm also interested to hear about *other* benefits and costs. What have I missed or misstated? Let's talk!

IsecT is an independent consultancy. We can help you with ISO27k (naturally!), information risk management, infosec strategies, infosec metrics, infosec awareness & training, ISO27k gap & pre-certification readiness assessments, SWOT analysis, post-incident & project reviews, business continuity management, ISMS internal audit, IT auditing, infosec policies & procedures, benchmarking, interim infosec management, restructuring, mentoring, CISO & executive coaching, board-level presentations & proposals, business case development & review …

Visit isect.com and ISO27001security.com for more.