The ISO27k FAQ

Answers to Frequently Asked Questions about the ISO/IEC 27000-series information security standards

This is a static PDF version as of September 3rd 2012.

The online version at www.ISO27001security.com is updated most months.

This FAQ (Frequently Asked Questions) provides explanation and pragmatic guidance for those implementing the ISO/IEC 27000-series ("ISO27k") standards, including a sprinkling of **implementation tips** to get you off to a flying start.

Contents

Introduction, scope and purpose of this FAQ

This FAQ is intended to spread useful and accurate information about implementing the ISO/IEC 27000-family of information security management system standards ("ISO27k"). It is meant to help those who are implementing or planning to implement ISO27k. Like the ISO/IEC standards, the advice provided here is generic and needs to be tailored to your specific requirements. It is most certainly not legal advice. Please see the copyright and acknowledgements section at the end for information on the author and contributors.

Information security vs. IT security

Q: "The titles of the ISO27k standards mention 'Information Technology -- Security Techniques'. Does this mean they only apply to IT?"

A: No, most certainly not! The formal titles simply reflect the name of the joint ISO + IEC committee that oversees their production, namely SC27 "Information Technology -- Security Techniques", itself a subcommittee of JTC1 "Information Technology".

The scope of the ISO27k standards naturally includes many aspects of IT but does not stop there. The introduction to ISO/IEC 27002 states explicitly: "Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post of using electronic means, shown on films, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, it should always be appropriately protected."

Not all an organization's information assets belongs to or are managed within the IT function. IT typically owns and manages the shared IT infrastructure (the main corporate IT and network systems) but acts as a custodian for most corporate information content which belongs to other business units, and for other content belonging to customers and business partners. There are important implications in that information owners are accountable for ensuring that their information assets are adequately protected, just like other corporate assets. While information asset owners generally delegate key responsibilities for

information security to an information security management function and/or IT function, they remain accountable and must ensure that information security is adequately funded and supported to achieve the necessary level of protection.

Implementation tip: think of IT as custodians of the subset of all information assets which exist as computer data and systems. In most cases they are not the asset owners as such, and furthermore they have little involvement in other information assets such as paperwork and knowledge. It helps to focus first on critical business processes rather than the IT systems which often support or enable them.

Q: "When creating an ISMS, is it absolutely necessary to include members from all aspects of the business (business owners, finance, legal, HR, *etc.*)? I don't see the ISMS as being IT Security driven. I see it as being driven by the business with IT Security input. Am I correct?"

A: ISO27k is most definitely about ***information*** *security management systems*. IT security is of course a large part these days, given that so much information is communicated, stored and processed on computers, but non-computerized information assets (files, paperwork, printouts, knowledge) are still valuable corporate assets that deserve protection just as much as computer data, if not more so in the case of many forms of proprietary knowledge. What's more, the average IT department does not own and hence lacks full and total control of all the computer data, systems and/or networks in the entire organization, so limiting the scope of the ISMS to IT would not necessarily protect all the data to the same degree.

ISO/IEC 27001 is a deceptively simple and elegant standard. Designing and implementing a compliant and worthwhile ISMS is not trivial for several reasons:

- Information security is inherently complex and difficult to do well, while perfect security is practically unattainable. Whereas hackers, fraudsters and information thieves need only find a small chink in our defences, we must defend all points simultaneously, both around the perimeter and within. Most organizations have a plethora of technical platforms, applications and network connections, plus a raft of non-IT information assets to protect. We all face a range of internal and external threats, including the mundane but ubiquitous errors, accidents, equipment failures, bugs *etc*.
- The need for information security mirrors the use of and dependence on information, and therefore extends across the enterprise and beyond. It is not only necessary to involve representatives of the entire organization but also

business partners, particularly where the organization outsources critical information processes or relies on IT and telecomms services from third parties and hence has a direct interest in their security arrangements. Customers, owners, regulators and other stakeholders share similar concerns, leading to substantial governance and compliance obligations.

- Information security threats and vulnerabilities are constantly changing. As with the capital markets, this dynamism creates both risks and opportunities for the organization, especially in competitive environments (which includes national security and government departments by the way!). Agile, security-aware organizations respond to both, but positioning information security as a business enabler is a hard sell to old-fashioned managers with outdated views.

It is possible to restrict the scope and apply the ISMS narrowly, perhaps to just IT Department or the data centre. Although this probably loses a significant proportion of the benefits of an enterprise-wide ISMS, it also reduces the costs and typically speeds implementation. Just be careful that you will need to clarify security issues and probably apply additional controls at the scope boundary, meaning additional hidden costs (*e.g.* explicit security clauses in SLAs and contracts between IT and The Rest). It's sub-optimal overall but can be a useful tactic to get your ISMS started and build some experience.

Implementation tip: the organization's senior management should focus on identifying suitable "information owners" - generally quite senior managers throughout the business - who they will hold personally accountable for adequately protecting 'their' assets on behalf of the organization and its stakeholders. The owners, in turn, will call on IT, information security, HR, risk, compliance, legal and/or third parties to provide the protection they require, and to help them clarify and specify their security requirements in the first place through some process of information security risk assessment. The responsibility for security cascades naturally through the organization but accountability rests firmly at the top ("the buck stops here"). This is a useful concept because those at the top generally have the budgets and influence to make security happen.

Learning more about the ISO27k standards

Q: "Where can I obtain [insert name of ISO27k standard here]?"

A: ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27006 and other published standards may be purchased directly from ISO or from the various national standards bodies and commercial organizations. Shop around for the best deals, for example using this Google search.

If money is tight, it is worth checking the prices for localized/national versions of the standards. ISO sells the standards directly *e.g.* ISO/IEC 27002 costs ~200 Swiss dollars as a PDF or hardcopy. Several national standards bodies release translated versions of the standards in their local languages but all of them go to great lengths to ensure that the translations remain true to the original.

By the way, it is normally worth searching on the full formal names of the standards including the "/IEC" bit, but perhaps not the date since country-specific translations of the standards are often issued later than the original versions (avoid superseded versions though!).

Most if not all of the issued ISO27k standards can be purchased in electronic softcopy and printed hardcopy formats. Hardcopies are easier to read on the train or discuss in meetings. Softcopies are ideal for online searching for specific controls and for cutting and pasting into your own policy documents *etc*. (subject to the copyright restrictions). In addition to the usual PDF downloads, standards bodies may license online (intranet) access to the standards, limited by the number of concurrent users - this may be suitable for organizations who implement the standards and want to give their employees instant access to the standards for reference.

Implementation tip: ANSI sells downloadable PDFs of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27006 for just US$30 each (bargain!).

Q: "I want to become an ISO27k consultant. I'm looking for books or courses that teach ISO27k. Is there an exam? ... "

A: The best books on the ISO27k standards are the standards themselves - in other words, you should buy and read the standards. Being standards, they are quite formal in style but readable and useful. If you are going to implement them, write policies based upon them, consult around them *etc*. you will inevitably have to become very familiar with them so buy your copies and start reading!

The following ISO27k standards well worth studying:

- ISO/IEC 27000 introduces and gives an overview of the whole set of ISO27k standards, and provides a glossary defining various information security terms specifically as they are used in the context of the standards.
- ISO/IEC 27001 formally specifies the system for managing information security. Along with ISO/IEC 27006, it is essential if you intend to become an ISMS certification auditor by taking a "ISO/IEC 27001 Lead Auditor" training course offered by various training, consultancy and certification companies, and completing the requisite number of compliance audits under the wing of a fully-qualified ISMS certification auditor. If you are looking to implement rather than certify compliance with the standard, you should also study ISO/IEC 27002 (see below) and perhaps ISO/IEC 27003.
- ISO/IEC 27002 is the 'Code of Practice', a practical standard offering oodles of advice for those choosing/designing and implementing information security controls. The best way to learn ISO/IEC 27002 inside-out is to use it for real, which means going all the way through one or more ISMS implementations from planning to operations, auditing and maintenance. If you have no prior experience in information security, you should try to find an experienced mentor or guide, or take an "ISO/IEC 27001 Lead Implementer" course. Professional organizations such as ISSA, ISF and ISACA can help, along with the ISO27k Forum.
- ISO/IEC 27005 concerns the analysis and treatment of information security risks and as such underpins all the ISO27k standards.

You should also be aware of the remaining ISO27k standards and have some familiarity with other similar/related standards, methods, laws *etc*. (such as PCI DSS, COBIT and various privacy laws).

As to becoming a consultant, you are well advised to start by building a solid technical understanding of IT, risk and control concepts, and establishing your own expertise, experience, competence and hence credibility. Advice for those who want to become IT auditors in the IT Audit FAQ is also relevant to becoming an information security management specialist since the two fields are very

closely related. Another highly recommended resource is www.CCcure.org, especially if you are considering becoming CISSP, SSCP or CISM qualified in information security management.

Implementation tip: further resources are outlined on the books and links pages at ISO27001security.com and don't forget to join the ISO27k Forum. If you are struggling with particular ISMS-related issues, it's worth searching the Forum's archive or raising a query on the Forum.

Q: "Are there any qualifications for ISO27k professionals?"

A: Kind of. Other than the ISO and national standards bodies' processes for checking and accrediting organizations who wish to offer 'official' compliance certification services, there is currently no equivalent of, say, ISACA or $(ISC)^2$ overseeing the ISO27k courses and qualifications in order to set and maintain professional standards, insist on continuous professional development and so forth. At present there is nothing to stop *anyone* offering "ISO27k Lead Implementer"-type training courses and issuing certificates like confetti. This unfortunate situation casts doubt on the validity of Lead Implementer certificates in particular, and potentially discredits both the organizations currently offering them and the candidates who obtain them, even though they may be truly excellent. *It's a question of assurance not quality*.

There are a number of ISMS-related training courses that hand out certificates of completion but I would not necessarily call them 'qualifications' on that basis alone. 'Designations' may be a better term. This is still a relatively new field so it will inevitably take time for the training and qualification practices to settle down and for the most worthwhile and meaningful certification schemes to become universally accepted. Meanwhile, read on.

The two most common types of ISMS-related designations are as follows.

ISO/IEC 27001 Lead Auditor (LA)

The term "Lead Auditor" was coined by training schemes that were initially designed and run internally by accredited ISO/IEC 27001 certification bodies in order to train up their own staff to perform certification audits. Subsequently, various public/commercial LA training courses have emerged. There are at least four possible routes to someone calling themselves an ISO/IEC 27001 LA:

1. **The highway:** spend 5 straight days on a suitable officially-recognised training course run by an officially-recognised training body, pass the end of course exam, then undertake a further 35 days of third party certification audits under the guidance of a registered ISO/IEC 27001 LA. This route is

preferred by the International Register of Certification Auditors and, in Japan, JRCA. The highway naturally suits students who are employed by the accredited certification bodies, since they can get both the classroom training and on-site experience from their employers.

2. **The country route**: complete some other form of ISMS/audit related training (for example modular courses comprising a day or two's training on ISMS plus 3 days on auditing), then undertake further ISMS assignments such as internal ISMS audits, ISMS-related consultancy gigs or third party certification audits, and finally pass some form of "on-site skills examination". The country route may be the best option for students not working for accredited certification bodies, but may not deliver as much assurance.
3. **The cross-country 4x4 route**: become a qualified and experienced information security professional *and* a qualified and experienced IT audit professional *and* gain lots of real-world experience of designing, building, implementing, managing, maintaining and advising on ISO27k ISMSs. Most professionals with more than, say, a decade or two's work experience crossing these three areas have amassed valuable expertise, knowledge and battle scars, having faced many situations in the field. Some of them go on to take the highway or the country route, while others are too busy working for their clients or sharing their expertise with their employers to worry about certificates *per se*.
4. **The back alleys**: a few students and consultants evidently don't bother with the hardship of actual training, exams and/or on-the-job experience, simply adding "ISO/IEC 27001 LA" (or similar) to their CVs and email signatures and carrying on regardless ...

ISO/IEC 27001 or ISO/IEC 27002 Lead Implementer (LI)

In response to market demand for help with implementing the ISO27k standards rather than just auditing ISMSs against '27001, a number of IT training companies are now offering commercial ISO27k LI courses. These aim to give students some familiarity with the ISO27k standards, and then presumably provide pragmatic guidance on how to apply them to the design and implementation of an ISMS.

As with ISO27k LAs, do not rely on a candidate's claimed ISO27k LI qualification alone if information security is important to you - and why else would you be employing them? Skills (both technical and social), expertise, competencies and experience all vary from person to person, as does trustworthiness.

Caveat emptor! If you are employing information security professionals on the basis of their competence and integrity, it pays to check carefully into their backgrounds. Verify their claims. See ISO/IEC 27002 section 8.1.2 for sage advice on this very point.

Implementation tip: in our opinion, demonstrable hands-on ISO27k ISMS implementation and audit experience, ideally with more than one organization, is by far the best "qualification" in the field today. Next best would be demonstrable consultancy experience, helping a number of clients design, install and run their ISMSs, preferably again with a considerable amount of hands-on work and not merely advising at a distance. The LA and particularly the LI certifications vary in credibility but nevertheless the courses are a valuable introduction for beginners, although students who already have a reasonable understanding of information security management concepts are more likely to benefit from ISO27k-specific training.

Advice for people who want to become IT auditors in our IT audit FAQ is useful for those planning to become LAs or LIs and is also pretty relevant to becoming an information security management specialist since the two fields are very closely related. Another excellent resource is www.CCcure.org, especially if you are considering becoming CISSP, SSCP or CISM qualified in information security management - these are not specific to ISO27k but give you a sound basis for ISO27k work, particularly the management and implementation of appropriate/good practice information security controls.

Q: "Where else can I find answers on ISO27k and information security?"

A: Besides this FAQ and the ISO27k standards themselves, there are several professional/special interest groups and forums (fora?) worth considering, most of which are free or cheap to join:

- **ACM SIGSAC** (Association for Computing Machinery - Special Interest Group - Security, Audit and Control). Mission: "to develop the information security profession by sponsoring high-quality research conferences and workshops. SIGSAC conferences address all aspects of information and system security, encompassing security technologies, secure systems, security applications, and security policies. Security technologies include access control, assurance, authentication, cryptography, intrusion detection, penetration techniques, risk analysis, and secure protocols. Security systems include security in operating systems, database systems, networks and distributed systems, and middleware. Representative security applications areas are information systems, workflow systems, electronic commerce, electronic cash, copyright and intellectual property protection,

telecommunications systems, and healthcare. Security polices encompass confidentiality, integrity, availability, privacy, and survivability policies, including tradeoff and conflicts amongst these."

- **InfraGard.** "InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters."
- **ISACA** (originally the Information Systems Audit and Control Association). "As a nonprofit, global membership association for IT and information systems professionals, ISACA is committed to providing its diverse constituency of more than 95,000 worldwide with the tools they need to achieve individual and organizational success. The benefits offered through our globally accepted research, certifications and community collaboration result in greater trust in, and value from, information systems. Through the more than 190 chapters established in over 75 countries worldwide, ISACA provides its members with education, resource sharing, advocacy, professional networking, and a host of other benefits on a local level."
- **(ISC)²** (International Information Systems Security Certification Consortium). "... the global, not-for-profit leader in educating and certifying information security professionals throughout their careers. We are recognized for Gold Standard certifications (CISSP, SSCP, *etc*.) and world class education programs. We provide vendor-neutral education products, career services, and Gold Standard credentials to professionals in more than 135 countries. We take pride in our reputation built on trust, integrity, and professionalism. And we're proud of our membership – an elite network of nearly 75,000 certified industry professionals worldwide. Mission: we make society safer by improving productivity, efficiency and resilience of information-dependent economies through information security education and certification." [The CISSP Forumis particularly recommended.]
- **ISO27k Forum** (ISO/IEC 27000-series standards discussion forum). "This is a practitioner's group with a pragmatic rather than theoretical focus, where every contribution is treasured and every member valued. We mostly discuss practical matters of interest to those interpreting and applying the standards in real world situations. Forum members are encouraged both to ask questions and to offer answers, tips, suggestions, case studies, example materials and so forth. This is a self-help user community that thrives on proactive involvement in a supportive atmosphere."

- **ISSA** (Information Security Systems Association). "... a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members. The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government."
- **OISSG** (Open Information Systems Security Group). "OISSG is an independent and non-profit organization with vision to spread information security awareness by hosting an environment where security enthusiasts from all over globe share and build knowledge. OISSG has identified followings to achieve its vision: writing assurance/testing standards; organizing conferences; finding software bugs; organizing challenges; building computer security incident response teams; developing multiple channels of communications; setting up research labs."
- **OWASP** (Open Web Application Security Project). "The OWASP Foundation came online on December 1st 2001. It was established as a not-for-profit charitable organization in the United States on April 21, 2004 to ensure the ongoing availability and support for our work at OWASP. OWASP is an international organization and the OWASP Foundation supports OWASP efforts around the world. OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas."

Implementation tip: questions are good. I learn a lot from questions. I also learn a lot from answering questions and from considering other people's answers, further responses, corrections, clarifications, retrenchments and counterpoints. Despite the popular mantra, there *are* dumb questions, but there are also deceptively simple questions that turn out to be extremely eloquent once we peel back the layers and try to respond. Whatever your initial state of knowledge, expertise and experience, actively engaging in the debate puts you on the fast track to further personal and professional development. Do join in. Remember: *life is not a spectator sport.*

ISO/IEC acronyms and committees

Q: "What does 'ISO' mean? And what about 'ISO/IEC'?"

A: ISO is the short or common name of the global standards body known in English as the International Organization for Standardization. "ISO" is not strictly an abbreviation since the long name varies in different languages - it is in fact derived from the Greek word *isos* meaning equal. At least, that's what we're told.

IEC is the International Electrotechnical Commission, another international standards body that cooperates closely with ISO on electrical, electronic and related technical standards. Standards developed jointly with ISO are prefixed "ISO/IEC" although in practice most users [incorrectly] shorten it to "ISO".

ISO/IEC also collaborate on some standards with other international organisations (both governmental and private sector) such as the ITU, the International Telecommunication Union. The ITU is primarily a trade body coordinating telecomms organizations to enable worldwide communications. It allocates radio frequencies, for example, to minimize co-channel interference and encourage the manufacture of radio equipment that can be used internationally.

Q: "What do 'WD', 'CD', 'FDIS' and those other acronyms prepended to draft ISO standards really mean?"

A: The acronyms indicate the stages reached by International Standards as they progress sequentially through the various committees and approvals:

1. **PWI** = Preliminary Work Item - initial feasibility and scoping activities
2. **NP** = New Proposal (or study period) - formal scoping phase *
3. **WD** = Working Draft (1st WD, 2nd WD *etc.*) - development phase
4. **CD** = Committee Draft (1st CD, 2nd CD *etc.*)- quality control phase *
5. **FCD** = Final Committee Draft - ready for final approval *
6. **DIS** = Draft International Standard - nearly there *
7. **FDIS** = Final Draft or Distribution International Standard - just about ready to publish *

8. **IS** = International Standard - published!

* At several stages during the standards development process, national standards bodies that belong fully to ISO/IEC JTC1/SC27 are invited to vote formally on the standards and submit comments, particularly if they disapprove of anything.

A similar sequence applies to Technical Reports.

The process from PWI to IS normally takes *between 2 and 4 years (average 2.8 years)*, given the attention to detail at every stage and the need for collaboration and consensus on a global scale *e.g.* when a WD is issued for comments, representatives of the national standards bodies that belong to ISO or IEC (known as "Member Bodies" MBs within ISO but "National Committees" NCs in IEC) typically have ~3 months to review the document, discuss it amongst themselves and submit formal votes and comments. If the comments are unfavourable or complex, an updated WD is normally released for a further round of comments. When documents have stabilised, they are circulated for voting. Any of you with experience of getting formal documents such as security policies prepared, reviewed and approved by your management will surely appreciate the 'fun' involved in doing this in an international arena!

A fast-track process is sometimes used to adopt an existing national standard as an ISO standard. Some 6 months is allowed for comments and no more than a quarter of the votes may be negative if the standard is to be approved. Don't forget that "fast" is a relative term.

Published standards are reviewed every five years, or earlier if defect reports are submitted.

Q: "What is meant by 'JTC/1 SC27' and what are 'WG's'?"

A: As you might expect, an international body developing and coordinating a vast range of technical standards on a global basis has evolved a correspondingly vast bureaucracy to manage and share the work. Member Bodies normally participate in the development of standards through Technical Committees established by the respective organisation to deal with particular fields of technical activity. The ISO and IEC Technical Committees often collaborate in fields of mutual interest. IT standardisation presents unique requirements and challenges given the pace of innovation therefore, in 1987, ISO and IEC established a Joint Technical Committee **ISO / IEC JTC 1** with responsibility for IT standards.

JTC1's purpose is "Standardization in the field of Information Technology" which "includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of

information." While there is general agreement that information security is a superset of IT security, the fact that the ISO/IEC committee is IT specific means that the ISO27k information security standards are in fact labelled IT standards.

In ISO-speak, "SC" is a "Sub-Committee". **SC27** is the main (but not the only!) ISO Sub-Committee responsible for numerous IT security standards. SC27 is a Sub-Committee of ISO/JTC1. SC27 runs around 90 projects of which around half are actively progressing. SC27, in turn, has carved-up its workload across five WGs (Working Groups):

- **SC27/WG1 - Information Security Management Systems**: responsible for developing and maintaining the ISO27k family, in particular the core ISMS specification ISO/IEC 27001 and the code of practice ISO/IEC 27002. Convenor: Professor Ted Humphreys;
- **SC27/WG2 - Security Techniques and Mechanisms**: cryptography, algorithms, authentication, key management, digital signatures and all that. Convenor: Mr K Naemura;
- **SC27/WG3 - Security Evaluation Criteria**: Common Criteria, evaluation methods, protection profiles, security capability maturity models *etc*. Convenor: Mr M Ohlin;
- **SC27/WG4 - Security Control Objectives and Controls**: responsible for a variety of existing standards covering intrusion detection, IT network security, incident management, ICT disaster recovery, use of trusted third parties *etc*. and new areas such as business continuity, application security, cybersecurity and outsourcing. Some of these also fall into ISO27k. Convenor: Dr Meng-Chow Kang;
- **SC27/WG5 - Identity Management and Privacy Technologies** : does pretty much exactly 'what it says on the tin' (the title is self-explanatory). Includes biometrics. Convenor: Professor Kai Rannenberg.

As if that wasn't complicated enough, there are also "Other Working Groups" (OWGs), "Special Working Groups" (SWGs), "Rapporteur Groups" (RGs, advisors), "Joint Working Groups" (JWGs), Workshops and the IT Task Force (ITTF). [There is presumably also a secret CRfA (Committee Responsible for Acronyms) somewhere in ISO/IEC land!].

Aside from SC27, other subcommittees that consider security-related matters include:

- **SC 6** - Telecommunications and information exchange between systems
- **SC 7** - Software and systems engineering
- **SC 17** - Cards and personal identification
- **SC 25** - Interconnection of information technology equipment
- **SC 29** - Coding of audio, picture, multimedia and hypermedia information
- **SC 31** - Automatic identification and data capture techniques
- **SC 32** - Data management and interchange
- **SC 36** - Information technology for learning, education and training
- **SC 37** - Biometrics

Implementation tip: once you have gained ISMS implementation experience, consider helping the continued development of the ISO27k standards by contacting your national standards body and volunteering your assistance (more advice follows ...).

Please note: the ISO27001security.com website is independent of and does not belong to, nor is it endorsed by or affiliated with, ISO/IEC. Please read the online disclaimer for more.

Keeping up with security standards developments

Q: "How can I keep up with developments to the ISO 27000-series standards?"

A: If you are actively using the ISO27k standards, the best way to keep up with developments is to join the ISO27k Forum. Don't forget to bookmark the ISO27001security website and call back every so often to check what's new.

You might like to check out the ISMS newsletters out there and sign-up to any that provide useful and reliable information about the standards as opposed to merely promoting specific products. Good luck in your quest!

Another option is to Google ISO/IEC 27000 or related terms. Google knows about helpful resources such as this article from the UK's National Computing Centre.

Professional information security-related organizations such as ISSA and ISACA, and journals such as EDPACS, are increasingly publishing articles on ISO/IEC 27001/2 *etc*. The CISSPs over at CISSPforum discuss ISO27k related matters quite often.

Finally, if you discover some ISO27k news before it is published here, please tell us so we can share it with the user community via the website and/or via the ISO27k Forum.

Q: "Can I see draft ISO/IEC standards? Can I contribute to them?"

A: If you would like to get involved in contributing to, reviewing and commenting on the ISO/IEC 27000-series standards, contact your national standards body and get in touch with the person, team or committee working with JTC1/SC27 on the information security standards. There is a genuine chance for experienced professionals to influence the future directions of ISO27k if they are prepared to put in the effort and collaborate with colleagues around the world. Don't wait for the published standard to raise your criticisms and improvement suggestions! Offer to get involved in the drafting and review!

Q: "How can I get involved in the development of security standards?"

A: Contact your local national standards body (*e.g*. BSI, NIST) to find out about any special interest groups and committees working in the information security arena. If you can spare the time to get involved with standards specification, development and/or review, contact your local ISO/IEC JTC1/SC27 representative/s to volunteer your services.

Implementation tip: the ISO/IEC security Sub-Committees and Working Groups are extremely busy and produce *lots* of paperwork. Committee work drafting and reviewing standards plus responding to queries from other interested parties has to be slotted-in with other duties including the day-job. If you get involved, be prepared to lose a substantial chunk of your free time reading, reviewing and contributing to draft standards. It's fun though, and good to have the opportunity to influence the development of ISO27k standards!

Getting started on ISO27k implementation

Q: "How do we *engage* our management, persuading them that the ISMS program *has* to be established?"

A: A good place to start is to work on raising awareness at the management levels, as high as you can go. There are several ways of actually doing that, such as:

- Directly working with your senior security contacts/friends, including colleagues in risk, compliance, legal, IT, facilities, Internal Audit *etc*. (particularly any business units that have a clear and pressing need for information security *e.g*. R&D functions with pre-patent information; S&M functions with customer credit card info; HR with personal data on personnel ...): they (should!) already have some awareness of information security but may be unfamiliar with ISO27k and ISMS concepts, and may have the rather narrow IT security perspective;
- Drawing up strategies and plans for the ISMS, linked as explicitly as you can to corporate strategies and plans. The closer and more obvious those linkages, the harder it will be for management to resist the need for security in support of the business. Work hard at this - it will pay off big time in the end, trust me;
- Work with Finance on business plans, cost-benefit analysis, budget proposals or whatever it takes to get sufficient resources for the ISMS, both initially at design/development/implementation and long-term for ongoing security operations and maintenance of the ISMS. Without sufficient resources, the ISMS is doomed. This is largely a matter of prioritization relative to other business activities and initiatives, so you will have to negotiate timing and funding in the business context - which means *you* need an appreciation of what else is going on;
- Mapping communications and power relationships in your management levels i.e. the informal structure chart for management (not [just] the formal organogram that HR puts out, but the one showing who really wears the trousers, who they consult/rely on - possibly even a RACI-type chart and psychometrics if you have the knowledge, energy and access). This can help you understand your audience/customers better, communicate more effectively, and develop an uncanny ability to get your way. It can also help you identify and deal with any blockers. Validate your findings and assumptions with one or more friendly managers;
- Working with your team *i.e.* the information security people, help-deskers, security architects and others to formulate plans and approaches, and exploit

their business contacts where possible. Implementing a formal ISMS is a change management activity for the team as a whole - not something for the lone ranger!;

- Launching some basic strategic/management-level metrics, such as maturity scores against the recommendations in ISO/IEC 27002, section by section in only as much detail as you need to make the numbers meaningful to management;
- Finding and exploiting opportunities to tackle security pinch-points, longstanding security issues that have caused problems for the business. If you can resolve some of these in the business's favour, you will make friends. Make sure to take notes and use these situations as examples illustrating the new approach you are taking;
- Setting up regular briefing sessions with relevant managers, leading in to and supplemented by ad-hoc security briefings and workshops for management meetings, committees, teams or groups on security and risk-related matters (*e.g.* BCM/BIA workshops). Engagement is the underlying aim, which means both informing them and drawing them along, motivating them to support your efforts and helping them with whatever they need from security ("you scratch my back and I'll scratch yours");
- Tackling any outstanding audit issues of relevance to information security, and starting to build up your 'stock' of security anecdotes, incidents, policies, procedures, briefings *etc*., leading in to a full-on security awareness program when the time is ripe;
- Working with independent security consultants/contacts, perhaps starting by using external (and internal?) experts as invited speakers for management events. Help them find and speak on topics of current interest to management, and so set managers thinking about security stuff. If appropriate, keep the speakers on for a few hours or days to do some actual work as well! They can often help you find and exploit good relationships within the management hierarchy, and often have access to higher levels purely by dint of being independent experts. Just be careful to manage their expectations *i.e*. you may not be keen to have managers employ them independently of your initiatives.

Implementation tip: a bit of creative/lateral thinking should come up with a bunch of ideas of your own along these lines, from which to select the few that you are actually going to pursue *this* month. Don't try to do too much at once or nothing will get the attention it requires. It takes planning, prioritization and focus on your part to exploit the opportunities and techniques that work best in your organization.

Q: "Should we aim for ISO27k conformance, alignment, compliance or certification?"

A: Yes.

Well OK, I guess you want some advice on which way to go? Here are some of the pros and cons:

- **Conformance** (here meaning a general intent to apply the ISO27k standards) is a basic starting point, achievable at little cost for any organization that takes information security seriously. However, the 'general intent' bit implies a fair amount of management discretion about which specific parts of the ISO27k set are going to be used, and more importantly to what extent they are to be adopted. Conformance gives little if any assurance to third parties about the organization's information security status. It's practically meaningless without further information (for example which ISO27k standards have been implemented, and to what extent? Is the organization merely planning to adopt the ISO27k standards at some future point, or has it already done so? Does it actually have a working ISMS??). However, some people confuse "conformance" with "compliance": just remember that conformance starts with a con...
- **Alignment** is about as worthless as conformance. It could mean practically anything. Putting all your ISO27k standards in a neat row on the bookshelf is one form of alignment ...
- **Compliance** (meaning a more rigorous, comprehensive and systematic adoption of the ISO27k standards) is the next level which typically involves the organization implementing an ISMS of some form (ideally using ISO/IEC 27001) along with a suite of information security controls (ideally using ISO/IEC 27002). The organization *asserts* that it is compliant with standards but may or not offer any proof. The value of the assertion by itself depends largely on whether the organization is both competent at information security management and trustworthy.
- **Certification** *normally* means formal certification of the organization's ISMS against ISO/IEC 27001 by an accredited certification body. This in turn means that the organization's ISMS has been independently audited by competent ISMS certification auditors to confirm that the management system fulfills all the mandatory requirements of ISO/IEC 27001, and is operating correctly. *It is a moot point as to whether this means the organization is actually secure in any real sense* since certification auditors need not necessarily probe too deeply into the presence, design and/or operation of the information security controls: their primary interest is in to check the management system not the information security. That said, it is commonly assumed that an effective ISMS which complies fully with ISO/IEC 27001 will in fact be supported by a

reasonably comprehensive and effective suite of information security controls, and that the organization is proactively managing and continually improving them.

Certification of your ISMS is a laudable objective but even that is not much of a goal in itself. The real value of an ISMS is in the **realization of business benefits**, primarily the reduction in number and/or severity of information security incidents, provided the cost savings outweigh the cost of the ISMS and the controls (both elements being difficult to measure accurately). Additional business benefits stem from the reduction in information security risks and increased management control over them, leading to greater confidence. The value of assuring third parties about the organization's information security status depends on the specific commercial situation: increasingly, organizations are being forced to become ISO27k compliant if not certified by business partners, regulators or legal obligations. This then raises the question about whether management feels it is worth the organization becoming compliant/certified under its own terms and timescale, or under pressure from a third party.

Implementation tip: if you are genuinely compliant, the incremental cost of certification is relatively low whereas the benefits of independent assurance are significant. Why would you *not* go the whole hog? If a third party claims but cannot demonstrate compliance (ideally by accredited certification), it's worth asking why they don't have the certificate to prove it.

Q: "How many man-years (or man-months) are needed to implement an ISMS?"

A: Well, that depends. Here are just some of the relevant factors:

1. **Level of senior management support**. Definitely *the #1 factor* in my book, as just noted above. Affects most of the rest of this list. Itself depends on management's understanding of what will be or is involved in the implementation, and what are the business drivers and anticipated positive outcomes for the organization when the ISMS is in place and certified. Can be overcome to some extent by information security awareness activities, business cases, and general schmoozing, focusing specifically on these issues for the Execs and dealing positively with their concerns. Hint: it pays to work one-on-one with individual managers, not address just some faceless "management".
2. **Level of middle/junior management understanding and support**, particularly in areas such as IT, HR, Risk Management and Legal/Compliance. Tends to follow #1 but not necessarily in dysfunctional organizations. Can also be mitigated/improved through security awareness,

schmoozing *etc.* Make friends and influence these people by showing them how the ISMS will make their jobs easier and more effective.

3. **Experience, capabilities and diligence of ISMS implementation team** comprising the team leader (probably but not necessarily the Information Security Manager) plus assorted team members. Can be boosted by reading and training, plus of course this website and the ISO27k Forum. It is also worth considering targeted consultancy assistance to benefit from others' experiences (both good and bad!). Includes expertise in project and change management, and political astuteness: remember this is *NOT* repeat *NOT* a purely technical project within IT!
4. **Organization's information security maturity level** when starting the project, and their desired goal level when the implementation phase can be considered "finished". Usually unstated and difficult to pin down. Worse than that, it's a moveable feast that will shift as the project proceeds, typically because improved information security risk assessment processes identify 'risks and opportunities' [for improvement] that weren't even appreciated in the beginning (ah, ignorance is bliss) ...
5. **The organization's actual/true level of information security risk.** This factor rather self-evidently affects the amount and quality of security controls necessary, and hence the nature of the ISMS required. A military or high-profile organization in an intensely competitive market or highly regulated industry will *probably* end up with a rather different ISMS than, say, a bicycle shop.
6. **Existing compliance load and experience** *e.g.* PCI DSS, DPA, FISMA and particularly ISO 9000 or similar *ISO management systems* expertise within the organization. The need for compliance with externally-imposed information security-related laws, regulations, contractual terms *etc*. may be driving the ISMS implementation project forwards, but equally this pressure tends to divert many of the self same resources from their ISMS implementation activities.
7. **Level of understanding and support for the ISMS project in related functions** such as IT, risk management, finance, HR, legal/compliance, physical security, audit, plus key business functions (*i.e*. the political and commercial powerhouses of the organization). Make no mistake: if your ISMS does not have - or at least if the implementation project cannot generate - sufficient genuine friends in such functions, you are stuffed. Ignore this factor at your peril.
8. **Strategic fit** between the putative ISMS claimed/actual benefits and the organization's stated/actual business goals. Finding, creating and/or making explicit the points of alignment (such as obviously shared objectives

etc.) can be the key *both* to surmounting any speed bumps on the road to ISMS nirvana *and* generating ISMS success metrics that management simply cannot ignore.

9. **Number and power of blockers or barriers** - generally this refers to powerful people within the organization (not necessarily managers!) but sometimes technical and/or commercial barriers can threaten to derail a project. See #1 and #8.
10. **Resourcing levels** (**not just the core ISMS implementation project team!**), plus the level of other competing initiatives and activities. This includes $$$, skilled people, consultants *etc*., and I mean the actual level of effort expended on the project-related activities, not just the supposedly budgeted or committed levels.
11. **Scope** of the ISMS *e.g*. business units to be included, supplier relations included or excluded. Counterintuitively, perhaps, this is not necessarily a prime factor since there will always need to be a basic level of effort required to design and implement the management system, regardless of how widely it is applied throughout the organization. A too-narrowly-scoped ISMS can actually create more work for the implementation team, *and* may damage the realizable business value!
12. **String length** :-)

Implementation tip: as a very rough guide to perhaps set management's initial expectations and indicate broad parameters for the project planning, I would estimate needing somewhere between one and five years from scratch to certificate. Some organizations claim to have done it more quickly, but I guess they started with a relatively mature ISMS already in place (did they really start from scratch?) and probably set themselves quite specific objectives with a narrow scope. Some clearly take much longer (to infinity - and beyond!) because their implementation projects flounder, people get burnt out, other stuff happens, key people move on, support wanes, that sort of thing. Don't forget, as well, that **an ISMS is for life, not just for Christmas** - in other words, it is a project with only an arbitrary end point, since eventually the delivered ISMS becomes just a routine part of normal business activities.

Q: "Is it necessary to appoint an Information Security Manager to implement and run an ISMS? If so, what qualifications should the ISM possess?"

A: Yes, in practice an ISMS needs a nominated Information Security Manager (ISM), Chief Information Security Officer (CISO) or similar leader to plan,

implement, run and maintain it, although the ISO27k standards don't exactly say it that clearly. A *very rough* rule-of-thumb suggests around 1% of an organization's total employees should work in information security (a greater proportion in any organization for which information security is a critical business issue). Small organizations may not have a dedicated ISM but may assign the corresponding responsibilities to the IT Manager or someone else as a part-time duty. Organizations of all sizes are encouraged to utilize independent experts (consultants, contractors, auditors *etc*.) as necessary, both for the additional pairs of hands and more importantly their brains and experience.

Here are some generic suggestions of suitable qualities, qualifications and experience levels for an ISM/CISO (based on a list initially submitted to the ISO27k Forum by Wawet):

Must haves:

- Personal integrity (#1 requirement), high ethical standards, basically beyond reproach and entirely trustworthy
- Passion for information security and IT risk management, with a professional track record in the field typically evidenced by certifications such as **CISSP** or **CISM** plus hands-on experience running an ISMS of some form (ideally compliant to ISO27k)
- Can competently and confidently explain what CIA really means and why this is so important to the organization

Highly recommended:

- Professional IT or similar technical background (*e.g*. former IT system/network administrator, analyst, developer, project manager, operations, IT disaster recovery/contingency planner/manager)
- Project and personnel management experience, good at scheduling and managing time, people, budgets, tasks *etc*. and working to dynamic priorities
- Excellent communication skills, both written and oral, able to demonstrate the ability to write well and present confidently, evangelically even (check in the interview process)
- Business management experience & expertise, ideally **MBA** material, with knowledge of the organization's business situation, strategies and goals
- IT audit skills (*e.g*. able to assess risks, ask the right questions and get to the bottom of things, plus write and present formal management reports), ideally qualified to **CISA** or equivalent
- Hands-on experience of ISMS design and implementation (*e.g*. actively contributing member of the ISO27k Forum!)
- Process- and quality-oriented (demonstrated ability to identify and deliver continuous process improvements, knowledge/experience of ISO 9000 and

ITIL/ISO 20000) plus people skills (*e.g*. generally gets along with all types of person yet self-confident and assertive enough to lay down the law when required without being aggressive)

- Highly organized, structured and self-motivated, "driven" even
- Negotiation skills
- Pragmatic rather than overtly academic, theoretical or idealistic outlook
- Works well under stress induced by conflicting priorities, frequent "interrupts", limited resources, unreasonable/unrealistic expectations and often negative perceptions about the value and role of information security
- Knowledge of, and ideally familiarity with, the ISO27k standards
- Can competently and confidently explain the differences between threats, vulnerabilities and impacts, giving relevant examples

Nice to haves:

- Experience of ISMS implementation and/or certification to ISO27k or similar standards
- Knowledge of COBIT, FISMA, GAISP, SOX, PCI-DSS and other information security, governance, risk management or related standard, methods, laws, regulations *etc*.
- Able to understand and discuss the pros and cons of quantitative *versus* qualitative risk analysis methods as applied to information security
- Experience of designing and delivering successful education, training and/or awareness activities (*e.g*. trainers, teachers, help desk workers *etc*.)
- Experience of security administration, security architecture, physical security, risk management, compliance etc.
- Information security and/or IT audit consultancy experience with a variety of organizations, and the accumulated wisdom that is 'experience'

Implementation tip: good ISMs are hard to find. If you have a potential ISM already on the payroll but he/she lacks sufficient experience or qualifications to carry the whole job right now, consider employing a consultant to assist with the ISMS implementation project but give them the specific brief to mentor/train the proto-ISM and gradually hand over the reins. A significant ISMS implementation is a fabulous learning and career development opportunity in its own right!

Q: "Is it possible to restrict the scope of the ISMS to just one department or business unit, at least initially? If so, how do we treat risks that require controls outside the scope of our ISMS?"

A: Restricting the scope of the ISMS *may* reduce some of the effort and costs involved in the implementation but also reduces the realisable benefits, hence the net business value of the ISMS may well be lower. It is not necessarily such an easy option as it might at first appear, as your supplementary question implies.

The scope boundary can be a problem since, by definition, everything outside the scope is inherently less trustworthy than that within. Information security risks within scope of the ISMS (*i.e.* risks directly affecting the in-scope area) are assessed and treated, and this includes risks affecting the information flows going into or out of the scoped area. The treatments that you select to deal with these boundary risks may include:

- **Controlling** the risks through Service Level Agreements (typically with other business units or departments of the same organization) or contracts (with third parties) that specify certain security requirements, and perhaps technical and/or procedural controls for example a defined process for identifying and dealing with information security incidents affecting the trans-border information flows;
- Knowingly **accepting** the risks, albeit preferably with suitable contingency arrangements in place in case they materialise;
- **Transferring** the risks through some form of insurance, agreed liabilities *etc.*;
- **Avoiding** the risks [by not restricting the scope!].

Furthermore, while the incremental costs to extend the scope of an operating ISMS will normally be lower, there will inevitably be initial costs to plan and establish the ISMS of any size (*e.g.* to create a decent set of information security policies, standards, procedures and guidelines), all of which would have to be borne up-front by the in-scope area and may be impossible to recover from other business units/departments later.

In other words, this is a strategic investment decision for management.

That said, there are some advantages to starting small: it focuses the project and makes planning simpler. The project manager should have an easier time running the project with a smaller team (probably) and fewer stakeholders to satisfy. It may be a worthwhile learning opportunity, a chance to build skills and gain experience before proceeding with the remainder of the organization.

Implementation tip: rather than deliberately and consciously restricting the scope of the ISMS as you suggest, it may instead be worth talking in terms of a "pilot implementation" in whichever area/s you choose. This minor wording

change implies that, provided it is successful, the pilot *will* be expanded to become a full-scope implementation ...

Q: "What are the differences between the Statement of Applicability (SOA), Risk Treatment Plan (RTP) and Action Plan (AP)?"

A: The SOA is your formal definition of the controls listed in ISO/IEC 27002 that are relevant to your ISMS. There needs to be some rationale to explain your reasoning and persuade the auditors that important decisions were not made arbitrarily. Be ready for some robust discussions if you decide not to implement common controls, or to accept significant risks.

The AP and RTP seem similar at first glance but the AP is normally a development/contraction of the RTP. The RTP systematically identifies the controls that are needed to address each of the identified risks from your risk assessment, whereas the AP (or program plan or project plans) says what you are actually going to do - who will do it, by when, and how. A single control, especially a baseline control such as physically securing the organization's perimeter, may address numerous risks and so may appear multiple times in the RTP but hopefully only once in the AP when it is designed, implemented, verified and 'operationalized' (horrid word!).

ISO/IEC 27000 should help resolve any remaining confusion.

Implementation tip: don't get too hung up on the acronyms and titles of the documents. It is conceivable that one or more of them may be dropped when ISO/IEC 27001 and 27002 are revised. Concentrate on their primary purpose, which is to document the links between information security risks, control objectives and controls.

Q: "I would like to see an RTP example, with one or two risks managed, please ... I would give anything to see a little part of one... I don't know how to start... I recently finished my risk analysis and I'm really stuck here....."

A: the idea of the RTP is essentially to document how your organization intends to "treat" identified risks, where "treatment" means reduce, avoid, accept or transfer. Here's a fictitious RTP extract:

> 21. Risk: network infection by worms and similar malware, causing network outages, data damage, unauthorized access to systems and various consequential damages/losses including incident investigation and cleanup costs.
>
> Risk treatments: mitigate the risk primarily through antivirus controls, plus network, system and data logical access controls, plus incident management, backups, contingency plans, plus policies, procedures and guidelines.
>
> 22. Risk: serious fire in the data centre, causing loss of datacentre IT services for an extended period.
>
> Risk treatments: avoid risks by taking care over the location and construction of the data centre, including any post-build modifications. Also avoid excessive storage of flammable materials including magnetic media (e.g. locate the media archive elsewhere on site). Physical security controls including fire alarms, extinguishers etc., coupled with fire evacuation procedures and training. Also insurance cover against fire damage. Also avoiding excessive reliance on the data centre through dual-siting of critical network devices and servers.
>
> 23. Risk: corporate prosecution for copyright abuse.
>
> Risk treatments: avoid copyright abuse through using a centralised software and license inventory, regularly audited and reconciled both internally (e.g. actual number of installations <= licensed number) and against installed software on corporate IT systems (e.g. searching for additional software not listed in the inventory), coupled with various compliance measures, policies and procedures. Also restrict physical site access to authorized persons, limiting the potential for license snoopers ...
>
> 24. Risk: unreliable commercial software causing Blue Screen Of Death at the worst possible moment.
>
> Risk treatments: specify and test security aspects in software procurement process. Maintain software. Accept the residual risk for Windows.

Implementation tip: you could set this up as a table or matrix, since many risks will require some combination of treatments and, in virtually all cases, "accept residual risk" is a necessary evil:

Risk	Treatment			
	Reduce	**Avoid**	**Accept**	**Transfer**
1. Name or describe an information security risk here (with reference to the output of your risk analysis and prioritization process)	Say how you plan to reduce or mitigate the risk through the implementation of suitable information security controls selected from ISO/IEC 27002 or elsewhere	Can you avoid the situation that creates the risk in some way e.g. by good design and pre-planning, or by not doing risky business processes?	If it is not cost effective to completely mitigate a risk, management should openly acknowledge the residual risk	Can you transfer some or all of the risk to a third party, for example an insurer or business partner?
2. Next risk				

Q: "In order to conduct a risk assessment, we need a list of all of our 'information assets'. What kinds of things should be included in the list?"

A: You need to start with a reasonably comprehensive inventory of your information assets. Information assets may for example be categorized under the following generic headings:

- Pure/intangible information assets (content, data, knowledge, expertise);
- Software assets (commercial, bespoke or internal/proprietary applications, middleware, operating systems *etc*.);
- Physical IT assets (computers, routers, disks *etc*.);
- IT service assets - see ITIL or ISO 20000;
- Human information assets ("people are our greatest assets" is actually true when considering their skills, expertise and unwritten knowledge).

The classification is based on a list originally submitted to the ISO27k Forum. **A much more comprehensive version of this list is now available in the free ISO27k Toolkit.**

Don't worry about needing a complete inventory before you kick off: you can make a start on risk assessment almost as soon as you have identified the first few items, provided you are prepared to revisit them later on in the light of additional knowledge from assessing other assets. You will be revising

assessments periodically in any case once the ISMS and its PDCA cycles are running smoothly.

Another approach involves starting with the organization's key information resources - the things that are *clearly* crucial to the organization's ongoing business and survival. Disney's brand and intellectual property, for example, or the Treasury's taxpayers' database. Obviously enough, security incidents involving such vital information assets are likely to have massive impacts on the organization, hence the risks are likely to be highly significant. However, the devil may be in the details: maybe the CEO's laptop containing all the company's strategic plans is highly vulnerable to being stolen by a competitor. The capital value/replacement cost of the PC may be negligible, but the information it contains may be (to coin a phrase) "priceless".

Implementation tip: if you have a reasonable contingency planning process in operation, its list or inventory of critical information assets is probably a decent starting point for the ISMS. It's a fair bet that systems and functions supporting processes that have been designated business-critical are themselves business-critical and therefore deserve adequate security. Remember that it is better to avoid or avert disaster than recover from it!

Q: "Should the risk assessment process cover *all* our information assets?"

A: It's probably too much work to risk-analyze everything in depth so consider instead a two-phase process:

1. A broad but shallow/high-level risk assessment to categorize all your information assets and distinguish those that deserve more in-depth risk analysis from those that will be covered by baseline information security controls;
2. A detailed risk analysis on individual higher-risk assets or groups of related assets to tease out the specific supra-baseline control requirements.

Document "everything important" including management decisions about the categorization process. There's more advice on inventories above.

Implementation tip: to avoid analysis paralysis (*i.e.* seeking to inventory and risk assess absolutely every information asset and becoming grid-locked in that part of the process), remember that information is a fluid asset that changes all the time. Even if you were theoretically able to cover absolutely everything today, the position would be slightly different tomorrow and substantially different within a few weeks, months or years. Therefore it is perfectly acceptable to move ahead with an inventory that is "good enough for now" provided that the ISMS incorporates review and update processes as part of the continuous improvement.

Q: "What are the most challenging aspects of ISO/IEC 27002 implementation and ISO/IEC 27001 compliance?"

A: The following typical issues are summarised from a paper published in the ISSA Journal by Bil Bragg, a senior consultant with Dionach Ltd., who drew up the list by examining the gap analyses conducted for 20 client organisations. The first two concern mandatory requirements for ISO/IEC 27001 certification:

> **4.2 Establishing and managing the ISMS:** few organizations had formally stated the scope of their ISMS or documented their risk assessment method and risk acceptance criteria in accordance with the standard.
>
> **6.0 Internal ISMS audits:** only one organization had an internal ISMS audit program, and none had undertaken a management review of the ISMS.

The information security controls succinctly listed in Annex A of ISO/IEC 27001 and explained in more detail in ISO/IEC 27002 are not strictly mandatory for certification but are widely implemented and generally accepted as good security practices.

> **A.6.1 Internal organization:** few organizations (especially SMEs) had an information security committee or forum, and had nominated a manager for the ISMS.
>
> **A.6.2 External parties:** identification and treatment of risks relating to suppliers (including IT outsourcers) and customers was sporadic or missing.
>
> **A.7.1 Responsibility for assets:** few organizations maintained inventories of intangible information assets.
>
> **A.9.1 Secure areas:** while physical security gaps varied, they should have been identified through the ISMS risk assessment.
>
> **A.10.7 Media handling:** most lacked formal security policies and/or procedures for handling and disposing of media such as USB flash memory sticks.
>
> **A.10.8 Exchange of information:** many organizations have neither an information exchange policy nor agreements with customers and suppliers on transferring confidential information securely (*e.g.* emailing confidential information).
>
> **A.10.10 Monitoring:** few system clocks were time-synchronised, other than on MS Windows systems. This is obviously important on security systems such as CCTV.

A.11.1 Business requirement for access control: few organizations had systematically documented user and system admin roles for their business applications.

A.11.2 User access management: few organizations regularly and systematically reviewed access rights across all IT systems.

A.11.3 User responsibilities: very weak or default passwords were common on subsidiary and older systems, including network devices, databases and physical access control systems. Compliance with clear desk and clear screen policies was very weak in practice.

A.11.7 Mobile computing and teleworking: few organizations had formal policies and procedures for mobile computing and teleworking.

A.12.3 Cryptographic controls: there was seldom a consistent approach to managing encryption methods and keys.

A12.5.5 Outsourced software development: contracts did not stipulate intellectual property rights, escrow, quality and security requirements nor a right to audit the supplier.

A12.6 Technical vulnerability management: configuration management and security patching processes often neglected utility software such as Acrobat Reader.

A.13.1 Reporting information security events and weaknesses: many organizations lacked formal procedures for reporting security events, and mechanisms to quantify and monitor incidents. [Cumulative security incident costs are an important strategic metric that helps management justify continued investment in the ISMS, while the detailed cost breakdown focuses attention on aspects requiring improvement.]

A.14.1 Information security aspects of business continuity management: business continuity plans were often either absent or outdated, while continuity exercises were irregular and unrealistic (*e.g.* limited scope).

A.15.1 Compliance: no organizations had identified all the information security-relevant laws and regulations, and established mechanisms to stay up-to-date on changes.

[Many thanks to Bil for permission to share this list. Bil's original article in ISSA Journal, available online to ISSA members, is well worth reading for additional details and guidance on this.]

Implementation tip: without neglecting the other requirements, double-check that your ISMS implementation project plans do in fact allocate sufficient resources and time to tackle all the issues identified here.

ISMS documentation

Q: "What documents are normally part of an ISMS?"

A: Please visit our ISO27k Toolkit page for a checklist of typical ISMS documents and examples/samples and a paper describing the documents mandated by ISO/IEC 27001. We, the members of the ISO27k Forum, are working to produce a more comprehensive suite of samples/examples of each type of document. If *you* own materials that you are willing to donate to the cause, please get in touch. Thank you.

Q: "What format and style is appropriate for ISMS documentation?"

A: I would suggest putting your ISMS documentation online, on the corporate intranet. There are several advantages to using the intranet:

1. The intranet and hence the ISMS documentation will be readily available throughout the organization to anyone with access to a PC on the corporate LAN. Other departments can not only read and refer to your materials but hyperlink directly to them in their own policies, procedures *etc*. (and *vice versa* of course!).
2. The content can be structured and presented neatly (*e.g*. short, easy-to-read summary/intro pages hyperlinked to more detailed supporting pages containing the nitty gritty; embedded graphics such as process flow charts, mind maps ... oh and security awareness stuff).
3. It is easier to control the ISMS website than printed/hardcopy ISMS documents, provided someone has control over what gets posted to the intranet ISMS area (implying some sort of change management process to review and publish stuff). Everyone should be clear that the ISMS materials on the intranet are the current, live, versions. [You may like to have a separate 'trial' or 'draft' area to expose proposed changes for feedback, but make sure that area is easily identified as such *e.g*. with a different colored page background.]

There are some drawbacks though:

1. You need the skills and tools to design, prepare, publish and maintain the website, or at least easy access to someone who does that.

2. Web pages (like this one!) don't usually print out very well, so for things that people want to print and refer to, comment on, or whatever, you may need to supply printable versions (*e.g.* PDFs) to download and print from the same web pages.

That covers the format and type of communication. As to the writing style, that's something you will have to develop. Parts of the ISMS are inevitably formalized (*e.g.* policies), others can usefully be more user-friendly (*e.g.* guidelines). It's OK to have fun too, using more creative security awareness materials such as quizzes, crosswords, seminar/workshops and prize draws.

Implementation tip: it definitely helps to have a consistent style/format for each type of material, and even better some consistent elements on all of them to bind them into a coherent suite. Do you have an ISMS logo, perhaps, with which to 'brand' the documentation and security awareness materials?

Q: "What should we cover in our [information] security policy?"

A: It's up to you - well, strictly speaking, it's up to your management. See section 5 of ISO/IEC 27002 for a decent outline of what the policy should cover, as a minimum. However, the current versions of both '27001 and '27002 are somewhat cryptic, talking about both an "ISMS policy" and an "information security policy" without actually explaining exactly what they really mean by those terms, what the differences might be *etc*. [It is *conceivable* that the original authors were actually thinking about the same thing but accidentally used different words, and that difference has subsequently taken on a life of its own! It's something that several SC27 members noted as an issue and is being addressed during the current revision of the standards. Sorry we can't be more specific right at this moment: we are literally trying to figure it out for ourselves! The revision process will take time so meanwhile everyone just has to make the best of it and hope that your certification auditors are reasonable about it (we've not yet heard of any that aren't!).]

Although your approach may well differ, my *personal* preference is for a comprehensive security policy manual following the structure of ISO/IEC 27002 and supported by technical standards (*e.g.* "Baseline security standard for Windows 7"), procedures, guidelines and other security awareness materials at a lower level, with higher level security

principles and axioms laying out management's key control objectives.

The policy manual forms an important link between the higher and lower level documents in the hierarchy, and between the organization's approach to information security and the ISO/IEC recommendations.

I find the 39 control objectives ISO/IEC 27002 make an excellent comprehensive yet succinct set of policy axioms, albeit with the wording adapted to reflect what management actually wants to achieve in relation to the organization's business objectives. Taken together, perhaps with the addition of even higher-level principles (*e.g*. the principles of least privilege and defense-in-depth - there are just a handful) and maybe a senior management statement of support for the ISMS, the 39 axioms comprise a useful Corporate Information Security Policy, an 'overarching security policy statement' that summarizes and forms a solid basis for the entire policy suite.

Two styles of information security policies are common:

1. Individual policies covering specific security topics or issues such as "Email security policy" and "Network access control policy". Typically these are quite formally worded and define security responsibilities of key groups, functions, teams or people. They may include introductions and explanations to aide reader comprehension, and should reference relevant documents at higher and lower levels of the policy hierarchy. They should be technology-neutral and succinct - ideally no more than a few pages.
2. A comprehensive policy manual containing succinct policy statements reflecting the whole of ISO/IEC 27002, with numerous embedded cross-references between related policy statements and references to the related axioms, standards, procedures and guidelines. The manual functions as a master index for the entire policy suite, which helps avoid overlaps, g a p s and (worst of all) conflicts.

Many organizations use *both* styles of policy. This is not an either-or situation.

The axioms, if not the principles and detailed policies, should be formally reviewed and mandated by senior management to endorse the entire security programme. Don't neglect the value of senior management support, right from the start. The programme will most likely lead to changes to working practices and systems throughout the organization so management must be aware of the overall objectives and support the changes when it comes to the crunch. Consider starting with security awareness activities targeting the CIO and her peers: build your cohort of supporters by talking in strategic business terms as much as possible (*e.g*. do you have a documented business case for the security work?).

Finally, the whole policy suite should be put online on the corporate intranet, ideally through a dedicated security policy management system or wiki, for two good reasons:

1. The online set becomes the definitive reference - no more wondering about whether printed policies are still current or have been superseded. Other online/offline security policies should be ruthlessly hunted down and vigorously eliminated like vermin;
2. Everyone with access to the intranet can read and refer to the policies *etc*. easily, for example cross-referencing between them or to/from other policies *etc*. using hyperlinks to the respective URLs.

The next level down from policies usually involves security standards for specific technical platforms and situations. The Security Technical Implementation Guides (STIGs) from NIST, NSA and DISA/DoD form an excellent basis for corporate standards, along with technical security guides available directly from operating system and other software vendors. A compilation of STIGs plus the associated checklists and scripts is normally available as a downloadable ISO CD image (261 Mb!) covering: Active Directory, application security, biometrics, database security, desktop applications, DNS, DSN (Defense Switched Network), enclave security, network infrastructure, Secure Remote Computing (SRC), Sharing Peripherals Across the Network (SPAN), UNIX & Linux & various flavours of Windows, VoIP, Web server and wireless networking.

Bob Ralph expressed this issue very eloquently on the ISO27k Forum: "Sooner or later, whatever it is, it needs to be documented - worded to suit top middle or bottom (*e.g.* policies, procedures or work instructions). If its properly hierarchical then the system is like a completed jigsaw, each part a perfect fit with its partner, no more no less, and if that is achieved hey presto you get the big picture. The number of parts will depend on the size of the organisation and the number of processes."

Implementation tip: as with the information asset inventory issue noted above, information security policies, standards, procedures and guidelines are never truly "finished" as they need to be updated from time to time to reflect changes both within and without the organization (*e.g*. the emergence of new information security threats may justify the modification of existing policies *etc*., or at least the generation of additional security awareness materials about the changing threats). It helps to have a reasonably complete policy suite but it need not be totally comprehensive provided that you establish the ISMS processes necessary to identify and make updates on an ongoing basis in normal operation.

Q: "ISO 27002 provides general rules, but I cannot translate that to match what I have at work, in real life. Any guidance or advice?"

A: There is no definitive answer for your question: 'it all depends' is the classic consulting recommendation. The diagram and outline above should give you a reasonable idea of the overall process and the key documents that will be required or produced. However, the details vary in each organization. Take a look at the ISO27k Toolkit for more free advice.

If you already have a security policy manual, for instance, the specified controls may well address most of the risks in scope of ISO/IEC 27002, in which case you need to work more on the implementation and compliance side, having reviewed the manual for currency and suitability.

If your organization is just setting out on the path towards having an ISMS, you will probably need to start working on management understanding in order to justify the financial expense and changes associated with the program of work ahead - *i.e*. prepare your plan, business case and/or strategy. Think about it, document it, circulate it for comment and build executive support. Deal with the inevitable objections as best you can, don't just ignore them. You will not regret later time spent now making friends in senior management.

How will you obtain sufficient dedicated budget to achieve what needs to be done and how will you deal with the probable shortfall between ideal and actual funding? If you define your strategy as an investment proposal or business case, you will need to track projected and actual costs and benefits to demonstrate the net value of the program. This implies designing and implementing a comprehensive suite of information security metrics, either up-front or behind the scenes as the program continues. Don't underestimate the difficulties of generating helpful and informative metrics, nor the practical problems of estimating the Return On Investment for information security or indeed other risk management activities.

Implementation tip: get some professional help with the program management, project planning *etc*. unless you are a wizard with these things. Take suggestions from sources within the organization: most people are flattered simply to be asked their professional opinion and it pays to re-use existing processes, forms *etc*. where possible if information security is to become truly embedded in the corporate culture.

Q: "I am trying to put together a document for *working in secure areas (9.1.5)*. How much information should it contain *i.e.* is this just a one pager or a full manual?"

A: Regarding corporate policies, procedures and the like, shorter and more succinct is almost always better as it means less to:

- Write;
- Review, consider, check out;
- Approve;
- Implement i.e. mandate, circulate, put into practice;
- Read and understand;
- Train people about/make them aware of;
- Police i.e. check/ensure compliance with, and audit against; and
- Maintain ...

... but there are practical limits to this. It needs to be sufficiently comprehensive to meet your organization's particular risk mitigation needs, expansive and clear enough not to be totally cryptic, and needs a certain *gravitas* to be considered by management and staff as an actual policy (a single policy of "Keep all our information assets secure" scores very high on the succinctness scale but very low on the "What on Earth am I meant to do to comply with this policy?" scale!).

Section 9.1.5 of ISO/IEC 27002 guides you on the sorts of controls you ought to consider in the specific area you are working on. It makes sense to use the standard as a basis, a starting point. See how well it fits your organization's needs (considering your particular risks, circumstances and other supporting controls), modify it as necessary, then implement your policy ... and finally drop into 'maintenance mode' where subsequent practice, incidents, near misses and any changes in the security threats and vulnerabilities or business impacts in that part of your ISMS imply the need to change your controls.

Your policy development process will, in time if not now, come up against the challenge that many potential subject areas *could* be covered by multiple policies, looking at similar issues from different angles. "Working in secure areas", for instance, begs obvious questions about what constitutes "working" (do you mean just employees, for instance, or does it apply to contractors, cleaners, maintenance people, even security guards on patrol?), and how you have identified and defined "secure areas" (is there a physical risk assessment process? Does it take into account the security risks associated with information assets in each area? Does it adequately cover information that is in use, in storage or in transit? Are you dealing with classified information, whether internally classified or national security classified). You can carve up all your

controls in numerous ways, and (trust me!) it is very easy to end up with a totally unworkable mess of overlapping, conflicting and yet gappy policies if the overall policy development process is not itself well managed. Again, my advice is to think and plan comprehensively from the outset, using ISO/IEC 27001 and especially the more detailed ISO/IEC 27002 as a basis for your policy set, since:

1. The ISO27k standards' authors (members of committee ISO/IEC JTC1/SC27) have put a lot of work into figuring where each potential subject area is 'best' covered. ISO27k is reasonably comprehensive in coverage but the option remains to extend it if you need more. ISO/IEC 27002, in particular, incorporates numerous cross-references between applicable areas where appropriate rather than duplicating controls;
2. ISO27k constitutes good practice, in other words it is a sound basis for information security risk management, accepted worldwide;
3. Even where an arbitrary decision has been made about which heading suits some topic, it is specified thus in an international standard which makes it OK to copy that;
4. ISO27k provides a generally understood common vocabulary and structure, meaning your '27001 certification auditors, ISMS consultants and any new ISMS-aware employees will be instantly familiar with the layout and general content of your policy suite.

Implementation tip: keep it short if you can. You don't necessarily need to write a complete policy manual, the entire edifice, right now. You can work on it piecemeal, one policy, standard, procedure or guideline at a time but, using ISO27k as 'the picture on the box', all the pieces should gradually fall into place like a nice 2D jigsaw, not some fantastic but weird piece of modern art.

Maturing your ISMS

Q: "What Content Management System should we use for our ISMS?"

A: We cannot recommend a specific CMS for you without knowing your specific requirements, and yes they do vary from organization to organization. You really ought to consider a structured specification and evaluation process such as that recommended for choosing risk analysis/management methods.

Implementation tip: start by clearly defining your functional requirements before evaluating potential CMS candidates. If you don't know what you're looking for, how can you tell when you've found it? See Wikipedia's Content Management Systems entry for pointers to the different types of CMS including document management systems and web content management systems.

Q: "Should we roll our own Policy Management System or buy one?"

A: *[This excellent advice was kindly contributed by Michael Rasmussen. Thanks Michael!]*

The mismanagement of policies has grown exponentially within organizations with the proliferation of collaboration and document sharing software such as Microsoft SharePoint. These solutions to their credit as well as downfall enable anyone to post a policy. Organizations end up with policies scattered on dozens of different internal websites and file shares, with no defined audit trails or accountability for them. This produces policies that are written poorly, out of sync, out of date, and with no evidence of how the policy was communicated, read and understood.

Collaboration and content software is a great tool for managing and sharing content in a general way — such as wikis, blogs, Web content and documents usually shared among a specific group. While collaboration and document-sharing software appears easy and cheap to implement, the reality is that the cost to the organization is significant in the liability and exposure of ineffective policy management if not done properly. Many organizations have decided to take that path only to find that it is cumbersome for policy management.

There are strict compliance and legal requirements that must be instituted when managing policies — requirements that a build-your-own policy management system makes difficult to achieve and come at a significant cost to the organization. Some organizations feel that they could accomplish at least some of the necessary features, requiring significant internal IT development effort to achieve an appropriate and effective policy management environment. The cost actually exceeds the cost of purchasing a policy and procedure management (PPM) software platform. Add ongoing maintenance and support of a build-your-own policy management system, and the costs grow higher.

Consider that an organization will have to dedicate IT development resources to this project for several months and ongoing years. Is the organization willing to maintain the policy portal project as the priority for that long — and will it continue to test it and support it with updates as needed? Can it continually verify an audit trail that can hold up in court and with critical regulators? Can the organization demonstrate a strong policy management program that maintains and keeps policies current while showing who accessed them and when?

Another point of consideration is whether the organization wants to live with a home-grown system that will most likely have a fraction of the features contained in a purchased system. Companies can spend as much as 10,000 man hours to build a policy portal on collaboration technologies — and increase that development time every year thereafter trying to enhance it and provide the features an organization learns it needs to manage policies correctly. What are the opportunity costs an organization is losing by focusing on this a custom approach to policy management?

Some specific features to consider when building your own policy management solution:

- The desirability of a consistent platform for the entire enterprise instead of each department implementing their own policy portal;
- The ability for the platform to manage the lifecycle of policies through creation, communication, assessment/monitoring, tracking, maintenance/revising, to archiving and record keeping;
- The ability to restrict who can read what documents and determine who has the permission to edit, review and approve;
- The training requirements needed to show that individuals understand what is required of them through linkage to learning systems/modules, quizzing and attestation;
- The accessibility of the system, with the ability to communicate policies in the language of the reader as well as provide mechanisms of policy communication for those with disabilities;
- The requirement to be able to gather and track edits and comments to policies as they are developed or revised;
- The mapping of policies to obligations (*e.g.* regulatory or contractual requirements), risks, controls and investigations so there is a holistic view of policies as they relate to other areas of governance, risk management, and compliance (GRC);
- The ability to provide a robust system of record to track who accessed a policy as well as dates of attestation, certification, and read-and-understood acknowledgments;
- The ability to provide a user-friendly portal for all policies in the environment that has workflow, content management, and integration requirements necessary for policy management;
- The capability to provide a calendar view to see which policies are being communicated to areas of the business, so that policy communications do not burden the business with too much in any given month of the year;
- The need to provide links to hotlines for reporting policy violations;

- The ability to publish access to additional resources such as helplines and FAQs to get questions answered on policies;
- The cross-referencing and linking of related and supporting policies and procedures so the user can quickly navigate to what they need to understand;
- The ability to create categories of metadata to store within policies and to display documents by category so that policies are easily catalogued and accessed;
- The requirement to restrict access and rights to policy documents so that readers cannot edit/change them and sensitive policy documents are not accessible to those who do not need to see them;
- The necessity that the organization keep a system of record of the versions and histories of policies to be able to refer back to when there is an incident or issue that arises from the past and the organization must defend itself or provide evidence;
- The capacity to enforce templates and style on all policies with the ability to guide policy authors and prompt them to maintain the corporate brand as well as associate specific properties, categories, or regulatory obligations with the document;
- The need for accountable workflow so certain people can approve policy documents and then tasks can be moved to others with full audit trails on who did what to the policy;
- Deliver comprehensive reporting — consider the time it takes in a build-your-own approach, and organization could spend months or years trying to create the depth and breadth of reports included in commercial policy and procedure management software.

Implementation tip: although you may be able to implement a few of these features using a build-your own approach, the cost in training, maintenance and management time, let alone the legal ramifications due to lack of proof of reader signoff and comprehension, makes it a risky venture for policy and procedure management.

Q: "Is control X mandatory *[for various values of X]*?"

A: This kind of question comes up all the time on the ISO27k Forum, hence the reason it qualifies for this FAQ. To save further bandwidth on the Forum, please select one of the following answers:

1. Yes, you need X because it is a basic security control that everyone needs. You'd be silly/negligent/risking the farm not to have it.

2. No, X is not needed because *we* don't have it, therefore we consider it neither good practice nor best practice nor recommended.
3. That depends - I'm a consultant with lots of letters after my name but you'd have to pay me $$$$ to answer your question.
4. No, X is unnecessary because it is more costly than the incidents it prevents. Unless we are really unlucky anyway. Do ya feel lucky, punk?
5. You tell me: have you assessed the information security risks and identified a troubling risk that control X might mitigate? Have you decided that it would be better to implement X than some other risk treatment (avoid the risk, transfer the risk, accept the risk)? Is X the most cost-effective control in this situation? Does X adequately mitigate the risk and, ideally, others too yet without making the situation worse through additional complexity, procurement/management costs or whatever? Is X feasible?
6. Yes because NIST/COBIT/SOX/a little bird says so.
7. Yes.
8. No.
9. Yes because it is “mandatory”, according to [insert favorite authority figure here].
10. No because it is “optional” and/or was not explicitly listed in black and white as absolutely mandatory by [insert favorite authority figure here too].
11. Yes because it's the law [in country Y].
12. Only if your policies, plans, strategies, technical architecture, or internal standards say so.
13. Yes if there is a positive ROSI [Return On Security Investment], no if the ROSI is negative or if someone has seeded “reasonable doubt” or if there is something sexier on management's agenda this afternoon.
14. Yes, absolutely - I am a vendor selling X. X is all you need. X is better than sliced bread. I'd sell both my kidneys to buy X ...
15. Yes because we will get a bad audit report and/or grief from HQ if we do not have X.
16. Not necessarily now but it will definitely be required in the future. Trust me.
17. No because we cannot afford it at the moment.
18. No because if you have it, then we have to have it too, else we will appear behind the times and that is BAD.

19. Yes because we have it and you are Behind The Times.
20. Do you even have to ask? Doh!

OK OK enough already. While there may be an element of truth in all of them, the most correct answer is (arguably) #5. You will no doubt have spotted that it is the longest answer and consists of a load more questions. If they are too hard for you, simply choose between answers #7 and #8, or consider the following advice.

The ISMS specified in ISO/IEC 27001 allows management to decide which information security controls are necessary for the organization, based on their assessment of the information security risks. If they have done the analysis, understood the risks and made a management decision, it is their right.

However, any competent ISMS auditor would probably be concerned at the nature of the risk analysis that led to the decision to exclude commonplace controls, and would want to explore the documentation around it for a start. This is the classic auditor's "show me" situation!

The basic rationale, from an audit point of view, is that yes, management can decide not to apply any of the recommended information security controls in Annex A of 27001 or the whole of 27002 that most other organizations consider essential *provided* they can justify that decision on a rational basis. If the risk analysis and/or their reasoning and decision making processes were fundamentally flawed, the auditor would have grounds to complain and (in the case of a certification audit) perhaps refuse to certify, although even this outcome is not absolutely certain.

This is a tricky issue for ISO27k that extends well beyond such obvious examples as excluding incident management or continuity planning controls. The key aim of ISO27k is to ensure that management designs and implements a solid and reliable management system in order to manage *and improve* information security on an ongoing basis (including the periods between audits!) and over time get as close as reasonably possible to a state of security. That target security state, however, cannot reasonably be defined prescriptively in an international standard that is meant to apply to all types and sizes of organization. Controls that are entirely appropriate, if not "essential" for some organizations would be inappropriate and perhaps harmful (*i.e.* the costs would outweigh the business benefits) to others. Certain controls may be inappropriate today given the current state of maturity of the organization, but entirely appropriate n a few months or years from now. The ISO27k approach, therefore, stops short of mandating specific information security controls but does mandate a series of management controls comprising the management system. For these reasons, 27001 is the certification standard, not 27002.

Implementation tip: joking aside, this question betrays a lack of understanding of the ISO27k approach to Life, The Universe and Everything. Information security requirements are context dependent, hence the control requirements have to be determined by the organization's management examining its risks as best it can, determining its best options for dealing with whatever risks it identifies, and making investment decisions based on the phases of the moon, lucky crystals, ley lines or whatever. IF management decides some commonplace information security controls are simply not required or justified in their circumstances, they should prepare to be challenged on this decision and consider their rational very carefully. In many cases, they may decide to make a limited implementation instead, which largely avoids the issue.

Q: "Which laws and regulations do we need to comply with, according to ISO/IEC 27002 section 15?"

A: *[Important caveat: I am not a lawyer. This is not legal advice.]* Here is a far from comprehensive or accurate list of ten kinds of laws and regulations that may or may not be applicable to your organization, and may or may not fall under the remit of your ISMS:

1. **Privacy** or data protection acts if you are handling personal data (client data or employee data).
2. Computer misuse act or equivalent laws about **hacking**, unauthorized network access, malware *etc*.
3. **Telecommunications** laws about lawful/unlawful interception *etc*.
4. General **business laws** around company structure, taxation, governance (*e.g.* SOX), HR, health & safety, building codes, fire escapes *etc*.
5. Other **general laws** *e.g.* theft, fraud, misrepresentation, deception ...
6. **Consumer** laws concerning how your company represents its products, warranties, fitness for purpose, merchantability, quality (and by implication, security) *etc*.
7. **Contract** law concerning contracts with third parties (suppliers, partners, customers), liabilities, commitments *etc.*
8. **Intellectual property** protection laws including copyright, patents and trademarks, protecting both your own IP and that of third parties.
9. **Industry-specific laws and regulations** *e.g.* finance industry (banking laws, money laundering), PCI-DSS, govt & defence industry (freedom of information, official secrets, critical infrastructure, terrorism ...), medical

(more privacy requirements, sometimes regulations about data formats) *etc*.

10. **International** laws, or rather the laws of foreign jurisdictions, if your company does business with foreigners, uses overseas facilities or services *etc*.
11. **++ Others**: speak to your lawyers/corporate legal counsel about this, and/or your compliance function if you have one. Aside from the more obvious laws and regs about information security, several "non-IT" laws have an impact on IT and information security in the sense that the laws concern protecting or using or abusing information, or concern business processes and individual activities which are often computerised. Therefore there can be compliance obligations affecting the way the IT systems and information processes are designed and/or used, even from "non-IT" laws.

Note: strictly speaking, the current wording of ISO/IEC 27002:2005 section 15 *could* be interpreted to mean that it concerns compliance in general - not necessarily just in relation to information security and closely related areas such as privacy. However, that was not the intention of SC27 which is focused on information security management.

Implementation tip: compliance with externally-imposed obligations can be an important driver to implement an ISMS, not least because the ISMS can take some of the weight off management's shoulders. Managers generally either accept the need to comply, or can be persuaded to do so in order to avoid the personal adverse consequences (typically fines, prison time and career limitations). However, the formal rules tend to be minimalist, meaning that mere compliance is seldom sufficient to protect the organization's wider interests. Compliance may be important but it alone is insufficient for security.

Q: "How can we generate a 'culture of security'?"

A: Generating a security culture is certainly a challenge in several respects. Organizational cultures are easier to experience than to describe, and hard to change (influence is probably a better term in fact). Here are five Hinson Tips:

1. Culture is heavily influenced by management, especially senior management. This is one of the key reasons that genuine senior management support is considered essential when implementing an ISMS ... which implies the importance of addressing senior management, helping them understand and appreciate the value of information security from the earliest opportunity.

2. Corporate culture is also heavily influenced by powerful opinion-formers within the organization (at any level of the hierarchy), by internal communications and networks (both formal and informal), and by the wider business/industry and national cultures in which people live. These are influencable to varying degrees. An effective information security awareness program will identify and target the people, themes, messages and mechanisms across *all* these areas.
3. Culture is an emergent property or characteristic of the organization, that is it is demonstrated by people's actions and belief systems in practice, when they are behaving normally and not being watched, whatever the formal mission statements or fancy posters about corporate values may state. [Security awareness posters, for example, are unlikely to be sufficient to change culture by themselves, no matter how sexy they appear.] This includes management: it is no good management telling staff "Don't share your passwords" if they share their passwords with their PAs, for example, as this cultural dissonance is unhelpful.
4. Changing corporate culture may be viewed as a massive organization-wide long-term change management activity. Anyone who truly understands how to do massive change management reliably can make a fortune! It is a very complex and difficult topic, with many different approaches, some of which are complementary and others are conflicting. It is also highly dependent on the specific context, plus the history leading up to the decisions to change. A serious information security incident, for example, might be the trigger to "do something" about information security which could include implementing an ISMS, but that's a different starting point than, say, having a cost-benefit justified business case for information security, or legal/regulatory compliance pressures, or pressure from within (*e.g.* the CISO, ISM, CEO or Risk Manager). Experience with whatever precedes the ISMS may be positive or negative, and to some extent can be used accordingly by selectively reminding people about and reinterpreting the history.
5. Culture is dynamic: it will continue to change or evolve after it has been (somehow) pushed in a certain direction, and that future evolution is not entirely controllable. This is the main reason that we promote the idea of rolling or continuous security awareness programs, since a single event will gradually be forgotten and awareness levels will decay unless constantly refreshed. Using a sequence of security topics is a good way to make sure that the materials remain interesting and engaging, along with having excellent awareness content prepare by people who understand the audiences' needs. It's also why we like using security metrics and news of security incidents, especially how they were addressed and resolved, in

order to generate positive feedback and so continue driving the ISMS ever onward and upward. It requires management of perceptions.

Implementation tip: plan your approach to developing and establishing a security culture over the long term. If you expect overnight success, you will surely be disappointed but please don't assume that it is impossible and give up before your initiative has had a chance to get going. Investing time and effort consistently into this will pay dividends in the long run - in other words, it is worth it. Tackle it in bite-sized chunks rather than all at once, aiming for incremental, solid improvements rather than dramatic but often short-lived changes. Use suitable metrics to measure your corporation's security culture and confirm that it is moving in the right direction, adjusting your approach as you go.

Q: "What can the ISMS implementation project manager do to assure success?"

A: We can't *guarantee* your success but here are some of the trade secrets from successful ISMS PMs:

- Become familiar with the business you serve. Get to know the department heads and the challenges they face. Try to see information security risks and controls from their perspectives, and look hard for situations in which strong, reliable information security is taken for granted or presents opportunities for new business activities that would otherwise be too risky.
- Cultivate business champions for information security in key areas, for example by talking to sales people on how they win business and what would help them be more successful, asking R&D people about the importance of keeping research secrets from commercial rivals, and checking how finance department satisfies SOX and similar integrity obligations.
- Make friends with colleagues in related functions such as risk management, compliance, internal audit, site security/facilities and IT. Take time to explain to them how an ISMS will support what they do, and garner their explicit support for the implementation project. These people are often influential with senior management.
- Present ISO27k as a **practical solution** to current and future business problems rather than an academic set of controls. Solutions are more palatable than controls. Focus on the business outcomes of the ISMS rather than the ISMS itself. Continue to sell the ISMS as a solution to business needs and encourage other managers involved with security to adopt a similar business-focused attitude. Seek out and exploit strategic alignments.

- Remember that if the business is to adopt ISO27k and take on board a culture change, it should be perceived as empowering and enabling not restrictive and disabling.
- Tone down the technobabble and learn business-speak. Remember, IT is only *part* of the ISMS albeit an important one. Make a special effort to reach out to, inform and engage senior management up to board level: their understanding and support for the ISMS will facilitate the numerous changes necessary to business processes and systems as they are secured, and conversely their active or passive resistance will make your job *much* harder. Consider starting your management-level security awareness activities early in the ISMS implementation - even before your project is proposed and approved.
- Celebrate successes. Take every opportunity to write-up and share situations in which information security helps the organization mitigate risks. Case studies and direct quotations from managers or staff who appreciate the value of the ISMS all help to spread the word: security is as much about saying "Yes!" as "No!"

Got other tips? Please contact us directly or by all means share your good ideas with the ISO27k Forum.

Implementation tip: learn and adopt worthwhile approaches from other initiatives, both internal and external to your organization and whether entirely successful or not (it's better to learn from other people's mistakes than your own, given the chance!). Many experienced project managers keep 'little black books' of things that worked for them or others, things to avoid, and ideas to try out when the opportunity arises. Seek out and adopt good ideas from all quarters.

Q: "Our organisation is planning to implement metrics to measure the effectiveness of both information security and management controls. What is the starting point and process?"

A: It's tough to give simple advice on metrics: it is arguably the hardest part of what we do. But here goes.

First I recommend reading the ISO27k implementation guidance paper from the ISO27k Toolkit available elsewhere on this site. It proposes a set of 39 information security metrics aligned with the 39 key sections of ISO/IEC 27002, which will give you a basic starting point and some ideas of things perhaps worth measuring.

Other metrics-related references that you should check out include:

- You are what you measure by Hauser and Katz - warns about driving the organization the wrong way as a result of an inappropriate choice of metrics;
- Information Security Management Metrics by Krag Brotby - strong on strategic and governance aspects of metrics;
- IT Security Metrics by Lance Hayden - IT-specific, explains GQM (Goal-Question-Metric) approach;
- Security Metrics by Andrew Jaquith - good all-round text if a bit heavy on mathematical theory;
- NIST SP800-55 rev 1 - focused on measuring FISMA compliance but the principles are broadly applicable (it's also well-written and FREE!).

As you read through that lot, start thinking hard about what you and your management might really want to know about how you are doing on information security, and start defining and prioritizing the collective requirements. This is the crux of your problem. Management probably wants to know things like "Are we secure enough?" and "Are we more secure today than we were this time last month?" and "What are the most significant information security risks we are facing?" and "Why is information security so expensive?"! These are really tough questions to answer, so work hard to refine them and make them at least partly answerable.

Hint: look at those parts of the ISMS which caused you the most grief when designing and implementing it. Are there parts of the ISMS that are self-evidently painful to operate? If so, these are classic ISMS process improvement opportunities, and hopefully good places to gather metrics that will help you justify, plan and make those improvements, with the spin-off benefit that you will be making things easier for those involved.

It may seem too early but it's almost certainly worth talking to your management about what they might expect during this metrics design phase. Look at what kinds of metrics they get from other management systems. Find out what they actually use *versus* what they get, and look for clues about what kinds of things work best in your organization. Consider phoning your peers at other similar organizations for some good ideas. Find out what formats and styles of reporting they like best or hate most. Ask them what few reports they could really not do without. Think minimalist at the start.

Next, start looking at the realities of gathering information on those things you really want to know, and continue refining your requirements. Some metrics will be straightforward (great! These are probably keepers), some will be feasible but more difficult (bear these in mind - may need more work) and some will be so awkward and/or costly that the effort required to measure them will outweigh any benefit obtained (park these, at least for now: you may revisit them later as your ISMS matures).

Be careful with any existing infosec metrics: some of them may be being measured simply because they are easy to measure, such as simple counts of things ("23 malware incidents this month", "23 million spams blocked today" or whatever). Unfortunately, such simple metrics typically don't tell management, especially senior management, anything really worthwhile. While a few may have value to the Information Security Manager as operational metrics, most are at best 'nice to have' numbers rather than "Oh boy, this one is in the red, we'd better turn dial ZZY to the left 20 degrees"!

Most of all, avoid the temptation to list and discuss all the information security-related things you can measure, like a giant shopping list. Some of them may be worthwhile ingredients, but most will be distracting and unhelpful. Trust me, this is not an effective way to start designing your ISMS metrics. If you must have one, keep the shopping list to yourself but share the menu.

Finally, towards the end of your lunchtime (!), it's time to start experimenting, trialling a few metrics, getting the data gathering, analysis and presentation processes working and getting feedback from management. Give them some 'sample' reports and ask them if they know what to do about the things you are reporting. This is where all your pre-work starts to pay off, hopefully. If you have chosen well, you should by now be ready to routinely report *a few good metrics*, and more than that use management should be using them to make decisions. Management should be saying "Ah, I see, yes, nice, let's have more of these ..." and "Mmm, that's not quite what I had in mind. I really need to know about ...".

During this stage, you will inevitably find that you need to gather more detailed 'supporting' metrics to underpin the high level/strategic management stuff, and you will also figure out that there are various routine/operational issues and controls within the ISMS that deserve measuring and using for day-to-day purposes by the Information Security Manager and team.

Now is the time to work on defining targets. At what level, exactly, does metric 26 go 'into the red'? At which point on the scale can we relax?

Then, over the next several decades (!!), keep on refining your metrics, testing new ones, dropping the ones that aren't working and responding to changes in your ISMS, the risks and controls, the people, the fashions, the good ideas you pick up at conferences ... and extending the answer to this FAQ with your expertise!

--- Alternatively, see if you can make any sense of ISO/IEC 27004:2009. Good luck. ---

Implementation tip: browse SecurityMetametrics.com for eminently practical advice including a new FAQ on security metrics and security maturity metrics that align with ISO/IEC 27002.

Q: "Are there any standard metrics for ISO/IEC 27001?"

A: Unfortunately not. Metrication is one of the hardest problems in information security management, so it is not realistic to expect easy answers such as a standard set of security metrics, in just the same way that there is no universal set of security controls: there are simply too many variables. In time, a core set of common controls and metrics *may* emerge from the mire but there will probably never be total consensus. Even if there was a standard set, you would still have to extend it to suit your unique situation anyway. In short, there is no way around figuring out the information security risks, controls and metrics that matter to your particular organization.

The standard ISO/IEC 27004 offers guidance on ISMS metrics, but does not appear to be widely used. It is not a very practical standard, hence not much help to the busy Information Security Manager or Chief Information Security Officer looking for answers.

Certification could be considered a metric process: organizations are either certified or not certified, so in that sense it is a binary measure. However, the certification process involves a degree of interpretation and judgment (some organizations certify easily, others barely scrape through), the competence and interests of the certification auditors vary, and certification is a periodic snapshot of the ISMS status which may not be the same the very next day after the certificate is issued. In other words, this supposedly black-or-white metric actually has shades of grey.

Implementation tip: selecting security metrics that are appropriate for your organization starts by figuring out things such as who are the audiences for the metrics, and what do they expect to achieve with the information. If metrics are to provide the answers, what are the questions?

Information security risk analysis, assessment and management

Q: "We are just starting our ISO27k program. Which information security risk analysis method/s could we use?"

A: It is difficult to recommend particular methods or tools without knowing more about your organization in terms of its experience with risk analysis and information security management, size/complexity, industry, ISMS maturity and so on. While ISO/IEC 27005 offers general advice on choosing and using information security risk analysis or assessment methods, the ISO27k standards do not specify any specific method, giving you the flexibility to select a method, or more likely several methods and/or tools, that suit your organization's requirements.

Many different information security risk analysis methods and tools exist (see the long list below), in two main groups sharing broadly similar characteristics: the quantitative (mathematical) and qualitative (experiential) methods. None of them, not one, is explicitly required or recommended by the ISO27k standards which give some guidance but leave the choice of method/s down to users, depending on their requirements and factors such as their familiarity with certain methods. So compliance is not really a factor in the choice, except in the most general sense (methods to analyse the risk of, say, heart disease won't be much help here!).

By the way, it is perfectly acceptable, advised even, for an organization to use multiple information security risk analysis methods. Some are more suited to particular situations than others - for example, it might make sense to use a simple high-level overview method to identify areas/aspects of concern, and then to change to other more detailed in-depth method/s to examine those particular areas/aspects more fully. Furthermore, some risk analysis methods are favoured by audit, [general|commercial|financial|legal/compliance] risk management, health and safety, penetration testing, application design and testing, contingency planning, and many other groups: there is no real benefit in stopping them using their favourite methods and tools just to conform to ISO27k. In fact, the differing perspectives, experience and insight these methods/tools bring could prove very useful.

One thing to take care over, though, is how to resolve the inevitable discrepancies in the results from different methods. A crude policy such as "Pick whichever recommends the least costly controls and minimise only the obvious risks" is no better than "Pick the most comprehensive and minimise all the risks". The analyses are merely decision support tools to guide management,

who still need to make the vital decisions about how much security investment is appropriate, how much risk can be tolerated, how much certainty is really needed in the decision process, and when to make any needed information security improvements. Resolving such dilemmas requires management vision and experience, coupled with expert analysis/advice ... and gut feel. Good luck ... and don't neglect your contingency plans!

Below is a very brief introduction to a number of information security risk analysis/risk management methods, standards, guidelines and tools, plus some aimed at supporting GRC (governance, risk and compliance) and even SIEM (Security Information and Event Management). *Please note that we are not selling or endorsing any of them. We haven't even used most of them, personally. The short descriptions below are mostly drawn from supplier/vendors' websites and should not be swallowed whole. You need to determine your own risk analysis, risk management and/or governance requirements and evaluate the methods, tools, products etc. carefully - there is* ***further advice on how to select specific methods/tools in the next Q&A.*** *Caveat emptor.*

1. **AS/NZS 4360:2004** is a well-respected risk management standard published jointly by Australia Standards and New Zealand Standards. **HB 436:2004**, a handbook of risk management guidelines, is designed to accompany and expand on AS/NZS 4360. HB 436 includes and explains the text of the standard;
2. **Calabrese's Razor** is a method developed by Chris Calabrese to help the Center for Internet Security prioritize technical controls in their security configuration guides, though it has wider application. It helps to evaluate and compare the costs and benefits for each control on an even footing. An interesting approach;
3. **chaRMe** is an open source information security risk management support tool being developed by Secopan. The tool is available as a VMware appliance and has a German, English and Chinese (Mandarin) user interface;
4. **COBIT** from ISACA provides a comprehensive model guiding the implementation of sound IT governance processes/systems, including to some extent information security controls. It is widely used by SOX and IT auditors;
5. **COSO ERM** (the Committee of Sponsoring Organizations of the Treadway Commission's Enterprise Risk Management framework), published in 2004, is a widely used general structure/approach to managing all forms of organizational risk;
6. **Delphi** is essentially a forecasting technique involving successive rounds of anonymous predictions with consolidation and feedback to the participants

between each round. It can be applied to predicting information security risks with no less chance of success than the other methods shown here;

7. **DIY** (Do It Yourself) methods - see below;
8. **EBIOS** from the Central Information Systems Security Division of France is available in several European languages. There is a freeware tool supporting the method;
9. **FMEA** (Failure Modes and Effects Analysis) is a generic method commonly used in engineering design. It focuses on examining the possible ways in which a system (or process or whatever) might possibly fail and cause adverse effects on the organization (or the users or customers or managers or whomever). The actual causes of such failures are de-emphasized compared to other risk analysis methods;
10. **HMG IAS 1** (Her Majesty's Government Information Assurance Standard Number 1) is a standard on 'technical risk assessment' used by the UK government;
11. **IRAM*** (Information Risk Assessment Methodologies) is not itself an RA method or tool but rather an ISF project looking at several RA methods and tools, I think, like the ENISA project;
12. The UK's Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC) and ALARM, The National Forum for Risk Management in the Public Sector, jointly produced **A Risk Management Standard** in 2002. It encompasses all forms of organizational risk, not just information security, using terms defined in ISO Guide 73;
13. **ISO 31000** is based on AS/NZS 4360 and others such as COSO-ERM. It offers guidance on the principles and implementation of risk management in general (not IT or information security specific). ISO 31000 is intended to provide a consensus general framework for managing risks in areas such as finance, chemistry, environment, quality, information security *etc*.;
14. **ISO/IEC 27005** isn't really a risk assessment or management method as such, more of a meta-method, an approach to choosing methods that are appropriate for your organization;
15. **ISO TR 13335**: this multipartite ISO Technical Report is a precursor to ISO/IEC 27005;
16. **MAGERIT** (Metodologia de Analisis y Gestion de Riesgos de los Sistemas de Informacion) is available for free in Spanish and English;
17. **Mehari** is a free open-source risk analysis and management method in several European languages developed by CLUSIF (Club de la Sécurité de

l'Information Français). The 2010 version adopts terminology and concepts from ISO/IEC 27005 and provides a spreadsheet tool;

18. **NIST SP 800-30** "Risk Management Guide for Information Technology Systems" is a free 55-page PDF download from NIST;
19. **NIST SP 800-39** "Managing Risk from Information Systems - An Organizational Perspective" is currently still a draft, released in 2008;
20. **OCTAVE** (**O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation) is CERT's risk-based strategic assessment and planning technique for security. It takes a business rather than technology-centric view of security risks. **OCTAVE Allegro** is, as the name suggests (to musicians if not the unfortunate owners of possibly the worst British car model ever produced by Austin!), a quick version of OCTAVE;
21. **PCR** (Perceived Composite Risk) by professors Bodin, Gordon and Loeb in Communications of the ACM, volume 51 number 4 (April 2008) uses the Analytic Hierarchy Process, taking into account the expected loss (similar to ALE), the expected severe loss (worst case scenario), and the standard deviation of loss (reflects inaccuracies in the analysis) to rank alternative security investments economically.
22. **Risk Asset Professional** (RAP) and **Compliance Assessment Professional** (CAP) products from Consult2Comply support information security risk/compliance assessments and management reporting;
23. **Risk IT** from IT Governance Institute/ISACA is similar to COBIT and Val IT but focuses on the management of risk;
24. **RM Studio** is a risk management support product from Icelandic company Stiki;
25. **SOMAP** (Security Officers Management and Analysis Project) offers an open source infosec risk assessment guide and infosec risk management handbook;
26. **STAR** (Security Targeting and Analysis of Risks) is a method developed for the IT Security function at Virginia Tech - click their Next:resources link to access the explanatory files, forms and spreadsheets;
27. **Stochastic** modelling methods using Markov chains, stochastic Petri nets, Monte Carlo simulation, Bayesian or other statistical techniques and probability theory are commonly applied to estimate uncertain risk values from incomplete data in the financial industry, but have some potential for systematically examining information security risks;

28. **Verinice** is a free open source tool for a variety of platforms supporting ISMS implementation and operations using the BSI IT-Grundschutz standards, currently only available in German.

Please note: we are happy to list and link to free open source tools as well as commercial tools from vendors who advertise on ISO27001security.com, provide suitable materials for the *ISO27k Toolkit*, *white papers* etc. Vendors of other information security risk management products are very welcome to ***sponsor-a-link directly to their websites*** to help offset the costs of running this website. *Contact us* for details.

If you are confused at which way to turn, ENISA's standardized comparison of risk analysis and risk management methods and tools might help (browse the selection from the left hand menu).

We are not recommending the methods and products/tools listed above, merely providing some options for your consideration. If you know of other information security risk analysis tools, products and methods worth including (for free!) in this FAQ, please get in touch.

By the way, **DIY** (do-it-yourself) is a genuine alternative, not just a straw man. It involves using risk analysis methods with which you or your organization are already familiar, perhaps home-grown methods or even those that are not normally used to examine information security risks (*e.g.* Delphi). Most if not all organizations have to examine and respond to all sorts of risks routinely. Many use informal/unstructured techniques such as risk workshops and brainstorming, coupled with more structured and rigorous methods as necessary. Maybe your existing risk analysis methods, processes and tools are already being used or could be adapted to examine information security risks? Provided they are sufficiently documented, rational, comprehensive and stable (meaning the results are reasonably repeatable), the ISO/IEC 27001 auditors *may* be persuaded that your organization understands its information security risks well enough to design a solid management system.

That said, be wary of naive attempts to quantify and compare risks mathematically for example using simple products of risk factors such as threat, vulnerability and impact values, or worse still summing those values. This is all figurative, informal arithmetic, not mathematically let alone scientifically sound by any means. There are problems as a result of:

- The values we assign to the risk factors, which are usually ordinal values on arbitrary and often non-linear scales;
- Inherent uncertainties in our assessments of those values, not least because they can vary dramatically from day-to-day; and
- Doubts about the validity or sufficiency of the chosen factors in calculating risk - are there other factors we don't yet appreciate? Are they equally important?

Similar issues occur, by the way, with many information security metrics. People who are unfamiliar with statistics can easily get carried away by the numbers and assign great significance to minor differences that are well within the bounds of random noise. On top of that, the situations we are dealing with are inherently complex and difficult to model or analyze scientifically, so an apparent correlation between two or more factors, whether positive or negative, could simply be an anomaly, a pure coincidence, rather than a true causal relationship. This is hard.

Implementation tip: check the ISO27k Toolkit for a risk analysis spreadsheet and risk register, along with other helpful items generously contributed by members of the ISO27k Forum. Also check our growing list of Content Management Systems supporting ISMS.

Q: "How should I choose a risk analysis tool or method?"

A: Read ISO/IEC 27005 for starters! If that's not enough, here is a tried-and-trusted spreadsheet-based method to evaluate options and choose preferred tools, methods, software, cars, partners, holiday destinations, political parties, employers, employees, careers, lifestyles, widgets ....

First skim through the list of methods and tools listed above and think carefully about your requirements. What do you expect the method to achieve for you? Which factors and/or features are most important? Are there any things that your would want the method not to do (e.g. consume vast amounts of limited resources)? Consider aspects under headings such as:

- **Quantitative or qualitative**: opinions vary on the relative value of quantitative *versus* qualitative methods. Few information security or risk management professionals would recommend truly quantitative analysis of information security risks in all circumstances due to the shortage of reliable data on incidents (probabilities and impacts), although they are potentially useful in some more narrowly-defined situations. One solution to this dilemma is to use quick/simple qualitative risk assessments followed by risk analyses on selected 'high risk' areas using more detailed qualitative or quantitative methods;
- **Scope**: are you purely looking at "information security risks", or risks in a broader sense, and what do you understand by "information security risks" anyway? Which information assets are you concerned with? These questions are very much linked to the scope of your ISMS and need to be thrashed out by management in order to compile your Statement Of Applicability (SOA);
- **Scaleability**: are you looking to support a relatively simple analysis of risks for a single process or IT system, an organization-wide analysis, or all of the above? Will you be completing the analysis just once or repeatedly, and if so

how often? If you intend to gather and analyze vast amounts of data over time, you will probably prefer tools based on databases rather than spreadsheets;

- **Maintainability and support**: some methods use clever decision support software to support those undertaking the analysis, whereas others are procedural or can be supported by generic tools such as spreadsheets. Clearly, therefore, they vary in the amount of technical expertise required to install, configure and maintain them. Home-grown tools can be more easily and cheaply modified in the light of your experiences compared to commercial tools (at least until the original developer departs, unless he/she made a conscious effort to document the system!) whereas commercial tools tend to be slicker and more polished. Commercial software having flexibility as a key design goal may give the best of both worlds;
- **Usability**: some methods and tools lead the user through the risk analysis process a step at a time, whereas others are more free-form but arguably assume more knowledge and expertise of the users. Some attempt to reduce the information gathering phase to simplistic self-completion questionnaires for risk non-specialists, others require competent risk analysts to collect the data;
- **Value**: by this we mean the benefits to your organization from the tool, offset by the costs of acquiring, using and maintaining the tool. *Purchase price is just one factor.* An expensive tool may be entirely appropriate for an organization that will get loads of value from the additional features. A cheap or free tool may prove costly to learn, difficult to use and limited in the features it offers ... or it may be absolutely ideal for you. Your value judgment and final selection is the end result of the evaluation process. You may even decide to adopt more than one for different situations and purposes!

Now write down your evaluation criteria, preferably as rows in a spreadsheet. Talk to your colleagues and ideally peers in other organizations who already use risk analysis tools/methods about the criteria and incorporate good ideas. Go back and look again at the tools/methods listed above and further refine your criteria, ideally into a ranked series ranging from “absolutely vital” down to “nice-to-haves”.

Add a ‘weighting’ column to your spreadsheet and fill it with a series of percentages that reflect the relative desirability of all criteria and add up to 100% (*e.g.* something really important might be weighted at say 10%, something entirely optional might be worth less than 1%). [If you are evaluating risk analysis tools/methods for distinctly different circumstances, create separate variant spreadsheets with the corresponding criteria and weightings for each.]

Add columns in which you will enter evaluation scores for each tool/criterion combination *e.g.*:

0 = “hopeless”: tool/method does not satisfy this criterion at all;

1 = “poor”: tool/method barely satisfies this criterion;

2 = “OK”: tool/method adequately satisfies this criterion;

3 = “good”: tool/method fully satisfies this criterion;

4 = “outstanding”: tool/method exceeds expectations with additional useful/valuable functions.

If you can’t decide whether something scores 2 or 3, it’s perfectly OK to score, say, 2½!

Add columns for comments against each tool/method, and a summary row for closing comments on each tool/method - trust me, comments will come in handy later.

Finally, insert mathematical functions to multiply each score by the corresponding weight and total each column, and your spreadsheet is ready to support the next step: evaluation.

For the evaluation, start by a quick assessment and rough scoring of your list of tools/methods in order to weed-out those that are very unlikely to meet your needs (*i.e*. low scores in high-ranked requirements), leaving you with a shortlist for further analysis.

You will most likely need to obtain evaluation versions of the shortlisted tools/methods to try them out - you might even go so far as to run mini trials or pilot studies, preferably using the same or similar scenarios in each case for fairness.

Continue looking at the shortlisted methods/tools and refining the scores until you have scores under every criterion for them all.

If you have followed the process diligently, the tools/methods that score the highest are your preferred ones (remember: you may end up using more than one). You are now all set to write your investment proposal, management report or whatever, adding and referring to the completed evaluation spreadsheet as an appendix. Those evaluation comments repay the effort at this stage. Consider incorporating sample reports, screenshots *etc*. from the tools/methods.

Don’t forget to secure and classify your evaluation spreadsheet and report! The information it contains (the criteria, the weightings, the scores and the comments) is valuable and deserves protection. Consider the information security risks!

Implementation tip: don't get too hung-up on the terminology or methods. If your organization already does some form of risk analysis or assessment of its information security or indeed other risks (such as health and safety), it is generally worth adopting the same or a similar approach at least at the start. Managers and others are likely to be more comfortable with what they know, and hence it should be easier to get them to focus on the content of the analysis rather than the method being used. Within reason you can also try out useful parts of methods/processes piecemeal, rather than necessarily adopting the entire set at the outset. Remember, risk analysis is a tool, a step on the way not a destination in itself.

Q: "What is the difference between risk assessment and audit?"

A: Risk assessment is an activity to identify and characterise the inherent and/or residual risks within a given system, situation *etc*. (according to the scope of the assessment). It tends to be a somewhat theoretical hands-off exercise, for example one or more workshop sessions involving staff and managers within and familiar with the scope area plus other experts in risk and control, such as Risk Managers, Information Security Managers and (sometimes) Auditors, discussing and theorising about the risks.

While audit planning and preparation also normally involves assessing the inherent risks in a given system, situation, process, business unit *etc*. (again according to the scope), auditors go on to check and validate the controls actually within and supporting the process, system, organization unit or whatever in order to determine whether the residual risks are sufficiently mitigated or contained. Audit fieldwork is very much a practical hands-on exercise.

Risk assessments are normally performed by the users and managers of the systems and processes in scope, whereas audits are invariably conducted by independent auditors. Auditor independence is more than simply a matter of organization structure *i.e.* auditors not reporting to the business managers in charge of the areas being audited. More important is the auditors' independence of mind, the ability to "think outside the box". Whereas those closely involved in a process on a day-to-day basis tend to become somewhat blinkered to the situation around them through familiarity, auditors see things through fresh eyes. They have no problem asking dumb questions, challenging things that others take for granted or accept because they have long since given up trying to resolve them. They are also perfectly happy to identify and report contentious political issues, resourcing constraints and opportunities for improvements that, for various reasons, insiders may be reluctant even to mention to their management. Audits are arguably the best way to find and address corporate

blind spots and control weaknesses that sometimes lead to significant information security incidents.

Compliance audits are a particular type of audit that assess the extent to which the in-scope processes, systems *etc*. comply with applicable requirements or meet their obligations laid down in laws, regulations, policies and standards. In the case of ISMS certification audits, for instance, certification auditors from an accredited certification body check that the ISMS complies with and fulfils the requirements in ISO/IEC 27001. There is also an element of risk assessment in compliance audits, however, since noncompliance can vary in gravity between purely inconsequential (*e.g.* trivial spelling mistakes in information security policies) and highly material (*e.g*. a complete lack of documented information security policies). Issues at the lower end of the scale (as determined by the auditors) may not necessarily be reported while those at the higher end will definitely be reported to management and will probably result in a refusal to certify the ISMS compliant until they are adequately resolved.

The risk assessment process is potentially auditable, by the way, while auditors are also concerned about audit risks (for example the possibility that their samples and checks may fail to identify some significant concern).

Implementation tip: challenging the *status quo* can be a valuable, if cathartic experience. At the end of the day, just remember that the primary aim of audits is to improve the organization, stimulating management to make changes for the better. Effective auditing includes but goes beyond pure compliance checking and the rather negative aura associated with that. It is the ultimate change catalyst.

Q: "How should management define the organization's *risk appetite*?"

A: Apart from certain limited circumstances, most "real world" information security risks cannot be objectively, rationally and accurately calculated or measured mathematically. We're dealing with an unbounded problem space and imperfect knowledge of it. At best some "knowable" risks can be estimated and ranked, but even this process is critically dependent on how the risks are framed or scoped (including how risks or information assets are accumulated or grouped together), and on who does the assessment and how, while other "unknowable" and hence unpredicted risks are almost certainly Out There waiting to bite us on the bum. It's a matter of probabilities and complex interdependencies so simple mathematics don't help: risks aren't simply additive or accumulative.

But that is not to say that risk assessment, measurement and comparison is totally pointless, rather that the results should be treated with a great deal of caution since there are clearly significant margins for error. Large differences in calculated probabilities or impacts of certain information security risks and

incidents may be meaningful, whereas small differences may not. Where you draw the line between big and small is down to your own experience in this area, your trust in the numbers and analysis, the reasons for differentiating them, and gut feel.

There is a perspective effect too. From a senior executive's point of view, impacts that involve them personally going to prison, being demoted or sacked, or suffering big hits on their executive bonus schemes through stock price crashes, are likely to register, even when probabilities drop from "probable" to "possible". Compliance with laws and regulations tends to fall into this category. From an individual data subject's perspective, impacts involving unauthorized disclosure of their most personal details are likely to be off the scale yet they may not understand or be concerned about probabilities.

And there's still more to consider in terms of selecting appropriate risk treatments. Few information security controls absolutely reliably and comprehensively mitigate risks. Even "strong" encryption is fallible, often due to implementation or key management flaws and sometimes due to cryptanalysis or blind luck. Most risk treatments help to reduce if not eliminate specific risks, and a few (such as contingency planning and having an effective ISMS) help reduce unspecified risks.

Implementation tip: given the above, it may not be realistic for us to expect management to define their 'risk appetite' in general policy terms but, faced with individual situations, someone needs to make judgement calls about the risks and controls. Risk analysis helps frame and make those decisions but doesn't often give cut-and-dried answers.

Q: "How should we handle exceptions?"

A: You first need to understand the vital difference between **exceptions** and **exemptions:**

- **Exceptions** are ***un****authorized* noncompliances with mandatory requirements, typically identified by compliance or other audits, management reviews, during the design phase when developing software and processes, or revealed by information security incidents;
- **Exemptions** are ***authorized*** noncompliances with mandatory requirements. They are the way to formalize risk management decisions to accept identified information security risks by not implementing certain mandated controls.

For example, an IT systems audit might identify that system A is configured to accept passwords of at least 6 characters, while the corporate password standard mandates at least 8 characters. This is an **exception** that should be brought to the attention of the Information Asset Owner (IAO) for system A. The IAO then considers the situation, considers the risk to the organization and to 'his/her' information asset, takes advice from others, and decides how to treat the risk. If the IAO's decision is to accept the risk, an**exemption** to the specific requirement is granted, but - *and this is the important bit* - the IAO is held personally accountable by management for any security incidents relating to that **exemption**.

Exemptions should be formalized *e.g.*:

- The IAO should be required to sign a crystal-clear statement regarding their understanding and acceptance of the risk to their asset if the **exemption** is granted;
- The **exemption** should be granted by being countersigned on behalf of management by an authoritative figure such as the CEO or CISO;
- Optionally, the **exemption** may specify compensating controls (such as explicit guidance to users of system A to choose passwords of at least 8 characters in this case);
- All **exemptions** should be formally recorded on a controlled corporate register;
- All **exemptions** should be reviewed by IAOs and management periodically (*e.g.* every year) and, if still required and justified, renewed using the same formal process as the initial authorization. Typically **exemptions** may be renewed and continue indefinitely just so long as the IAO is prepared to continue accepting the risk and management is prepared to accept the situation, but some organizations may impose limits (*e.g.* an

exemption automatically expires after one year and cannot be renewed without a majority vote in favour by the Board of Directors).

If there are loads of **exceptions** and especially **exemptions** to certain mandatory requirements, management really ought to reconsider whether the requirements are truly mandatory. If in fact they are, any current **exemptions** should be set to expire at some future point, forcing IAOs to use risk treatments other than 'accept the risk'. Information Security should take up the challenge to help IAOs improve compliance. If the requirements are not in fact mandatory after all, the policies *etc*. should be revised accordingly.

Implementation tip: key to this approach is personal accountability of IAOs for adequately protecting/securing their information assets. If management doesn't really understand or support concepts such as exceptions, exemptions, accountability, responsibility, ownership, information assets and risk, then the organization has more important governance issues to address, and the rest is moot!

Q: "Is there a published list of information security threats?

A: Yes, in fact there are several. ISO27k Forum members have used the following:

- ISO/IEC 27005 Annex C (an updated version of ISO 13335-3 Annex C) is a basic starting point;
- BSI's IT Grundschutz Kataloge (the baseline IT protection manual) includes an extensive threat catalog [HINT: Google toolbar's translation function works very well for us unfortunates who don't understand German];
- NIST SP 800-30 table 3-1 lists a few intentional/malicious human threats but don't neglect those unintentional threats (such as human errors) and natural/non-human threats (such as storms, fires and floods);
- BITS risk assessment spreadsheet covers a wide range of threats;
- Dejan Kosutic's wiki threat catalog;
- While not a threat catalog as such, Building Secure Software by John Viega and Gary McGraw, plus many of Gary's other books, discuss the concept of threat modelling to develop security specifications for application software;
- The Security Development Lifecycle by Michael Howard and Steve Lipner outlines Microsoft's approach to threat modelling using STRIDE (Spoofing identity, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) - again it's not a complete list of threats but just a starting point.

Implementation tip: these are of course generic information security threat catalogues. They may be useful reminders of the general types of threat you should consider in your risk analyses but it is worth brainstorming with colleagues from information security, "the business", and related functions such as risk management, compliance, legal *etc.* to develop a more specific list of threats (and vulnerabilities and impacts) that are relevant to your particular context and business situation. Why not develop and maintain your own threat catalogue on the corporate intranet to remind employees of the wide range of issues of concern to Information Security and the business?

Q: Our third party penetration testers recently found 2 medium risk and 7 low risk vulnerabilities. I disagree with the ratings and want to challenge the medium risks (some old software) before they report to the Board. What do you think?

A: 'Low/medium risk vulnerability' doesn't actually make sense. Fair enough, your pen testers have identified some technical vulnerabilities, but that's not the same as risks to the organization. To be classed as risks, there would also have to be threats and impacts:

- Threats could be, for example, just the general threat of non-specific hackers or malware, or something more significant such as your organization being a high profile target, likely to be attacked specifically by more competent and resourceful hackers.
- Impacts depend on what those servers are used for, how they are connected on your network, and the projected business effects and costs that successful compromises would cause.

Finally, you need to consider the cost and perhaps additional risks of mitigating the vulnerabilities. I've no idea what the costs to upgrading or replacing the products would be, nor what effects that might have on the rest of your IT. I would at least consider compensating controls such as additional/closer monitoring and slick responses instead of upgrades. In other words, look at the full range of risk treatments.

With additional information on these wider aspects of risk, management should be able to make better informed decisions about what, if anything, needs to be done to treat these risks or whether other risks are of greater concern.

Implementation tip: third party security testers, like IT auditors, are independent of the organization and hence often see things in a new light. They bring experience and knowledge of the outside world. This is a valuable perspective that insiders lack, so don't just dismiss what they tell you out of hand

without considering it properly and ideally discussing it openly with them. However, their independence means they may not fully appreciate the business context for information security, for example competing investment priorities. It is your management's role to take decisions and allocate resources in the best interests of the organization, so give them the information to help them do their job.

Q: "I'm confused with 'residual risk'. For example, after risk assessment there are 3 risks (A, B and C): risk A is acceptable, B and C are not acceptable. After risk treatment, B becomes acceptable but C is still not acceptable. Which is the residual risk: just C? Or B and C?"

A: Residual literally means 'of the residue' or 'left over'. So, residual risk is the left over risk remaining after all risk treatments have been applied. In your example, A, B and C *all* leave some (residual) risk behind.

- **Accepted risks** are still risks: they don't cease to have the potential for causing impacts simply because management decides not to do anything about them. Acceptance means management doesn't think they are worth reducing. Management may be wrong (Shock! Horror!) - the risks may not be as they believe, or they may change (*e.g*. if novel threats appear or new vulnerabilities are being exploited).
- **Mitigated or controlled risks** are still risks: they reduced but not eliminated, usually, and the controls may fail in action (*e.g.* antivirus software that does not recognize 100% of all malware, or that someone accidentally disables one day).
- **Eliminated risks** are probably no longer risks, but even then there is still a possibility that the risk analysis may be mistaken (*e.g*. perhaps you only eliminated part of the risk), or that the controls applied may not be as perfect as they appear (again, they may fail in action).
- **Avoided risks** are *probably* no longer risks, but again there is a possibility the risk analysis was wrong, or that they not be completely avoided (*e.g*. in a large business, there may be small business units out of management's line of vision, still facing the risk, or the business may later decide to get into risky activities it previously avoided).
- **Transferred risks** are reduced but are still risks, since the transferal may not turn out well in practice (*e.g*. if an insurance company declines a claim for some reason) and may not be adequate to completely negate the impacts (*e.g*. the insurance 'excess' charge).

The overall point is that you need to keep an eye on residual risks, review them from time to time, and where appropriate improve/change the treatments if the residuals are excessive.

[Aside: before any risk treatment is applied (or ignoring all risk treatments), the risk is known as the **inherent risk**.]

Implementation tip: actually managing residual risks, systematically, is a sign of a mature ISMS since it implies that the organization already has a grip on its unacceptable risks and is taking a sensible, realistic approach towards managing information security risks.

Certification against ISO/IEC 27001

Q: "How does my organization get certified against ISO/IEC 27002?"

A: It cannot - for reasons best known to ISO/IEC, organizations can be assessed or audited or reviewed but not formally certified against ISO/IEC 27002.

One reason is that ISO/IEC 27002 is a "code of practice" (whatever that means!) containing general good practice guidance rather than prescriptive requirements. Certification auditors who are essentially compliance auditors would therefore have to apply their judgement and discretion when checking compliance with the standard, which is evidently beyond them :-) In truth, the variation that would arise in practice to reflect each organization's specific context and information security needs would detract from the value of a generic certification scheme. Context is all-important.

Your organization could be reviewed informally or even audited against ISO/IEC 27002 by competent IT auditors, consultants or indeed experienced information security professionals familiar with ISO27k, and indeed this is the "gap analysis" activity common to many ISMS implementations. Information security controls currently in operation in the organization are compared against those recommended by ISO/IEC 27001, looking for gaps that will probably have to be addressed at some point during the ISMS implementation project (if the missing controls are judged necessary to mitigate risks).

ISO/IEC 27001 lays out a formal specification for an ISMS, with the emphasis very much on 'management system' rather than 'information security'. The management system element of an ISMS is more easily specified in a generic yet

formal way than the information security controls, and therefore ISO/IEC 27001 is the standard against which organizations are formally certified (see below).

This does however leave us with a problem: how can organizations place confidence in the actual information security controls of their business partners? Their ISO/IEC 27001 certificate only tells us that they have a working and compliant management system, and we assume that therefore they have assessed their information security risks, implemented appropriate information security controls, and are proactively managing them ... well in fact that's quite a lot of assurance when you think about it. Business partners can still opt to disclose more information about their actual information security controls, for example by sharing their information security policy manuals or by permitting third parties to audit their information security controls (perhaps using ISO/IEC 27008 when it is released).

Implementation tip: read the standards!

Q: "OK then, how do we get certified against ISO/IEC 27001?"

A: DNV has a helpful overview of the process.

First obtain and read the standard. We recommend obtaining ISO/IEC 27000 (provides a glossary of terms and an outline of the whole ISO27k series, useful for explaining them to management), ISO/IEC 27001 (the 'certification standard' which summarizes the process of implementing an Information Security Management System ISMS) plus ISO/IEC 27002 (which gives more detail on the nature of the ISMS). ISO/IEC 27002 contains a reasonably comprehensive set of 39 key control objectives for information security and lists a whole load of good practice security controls that are commonly used to satisfy those control objectives. I tend to speak of ISO/IEC 27002 as a menu of information security controls from which you need to pick your meal. You make your order (select the specific controls) using a risk analysis process which is briefly mentioned in section 4 of the standard, and is covered in more detail in yet another ISO/IEC standard, ISO/IEC 27005.

Next you need to plan and conduct some form of information security risk analysis. In reality, you first need to set the scene with management and then line the relevant parts of the organization and people up to ensure they engage with the risk analysis process. They need to be reasonably open to the concept of improving their information security controls and you will probably need to engage suitable risk/security experts to make this process as painless and effective as possible (hopefully you are lucky enough to have the resources on board already, otherwise you have to choose between building the competence in this area or buying-in expertise in the form of contractors/consultants). The risk

analysis may be called a 'gap analysis' or 'ISO27k review' since it may make sense to compare your existing controls against the advice in the standard, looking for weaknesses and omissions as you go, or you may prefer to do a zero-base risk analysis, assuming that there are not controls in place. The advantage of the latter approach is that you might identify unnecessary controls that can perhaps be deinstalled later.

By the way, "the relevant parts of the organization" relates to the scope of your intended certification. You have the option to certify the whole shootin' match or only parts. This is a critical decision for management. You will need to work closely with management to clarify what is in and out of scope, with the important proviso that everything declared as out-of-scope is inherently untrusted from the perspective of the in-scope elements, therefore suitable security controls (both technical and non-technical *e.g*. contracts or SLAs) are probably needed for data flows, systems, networks, processes *etc*. that cross the scope boundary. Cutting the scope right down is not necessarily the easy option!

Having completed the risk/gap analysis, you have the challenge of persuading senior management that they really do need to invest in information security, and of explaining the issues and risks that your analysis has identified in terms they appreciate. This is a tricky step, a balancing act: over-egg your dire predictions and they may back away saying you are being sensationalist. Underplay the security issues and they may not pay much attention to the need for improvements. It really helps to lean on someone with prior experience in this area. Management's appetite for addressing the issues you identify will determine the financing and priorities for the next step. If management say "no" at this point, you might as well reconsider your career options.

With management backing, you now implement the security improvements. Easier said than done! It could be a mere formality if your setup is already very security aware and competent in this area. It could be an extremely arduous job if you are starting from a low base, such as an organization which has habitually underinvested in information security, has made strategic changes in its use of, and dependence on, IT (*e.g*. it has started using the Internet for business processes/transactions and communications, rather than simply for promotional websites), or where there are no clear accountabilities for information security. It is impossible for me - or indeed for you - to say how long or how costly this phase will be for you until you have completed the previous steps, and even then you can only estimate.

With the improvements well under way and security gradually becoming an inherent part of business-as-usual, it's time to think forward towards ISO/IEC 27001 certification. Like other management systems standards from ISO, ISO/IEC 27001 is process-focused - it helps set up a management system for information security comprising a suite of management processes loosely relating

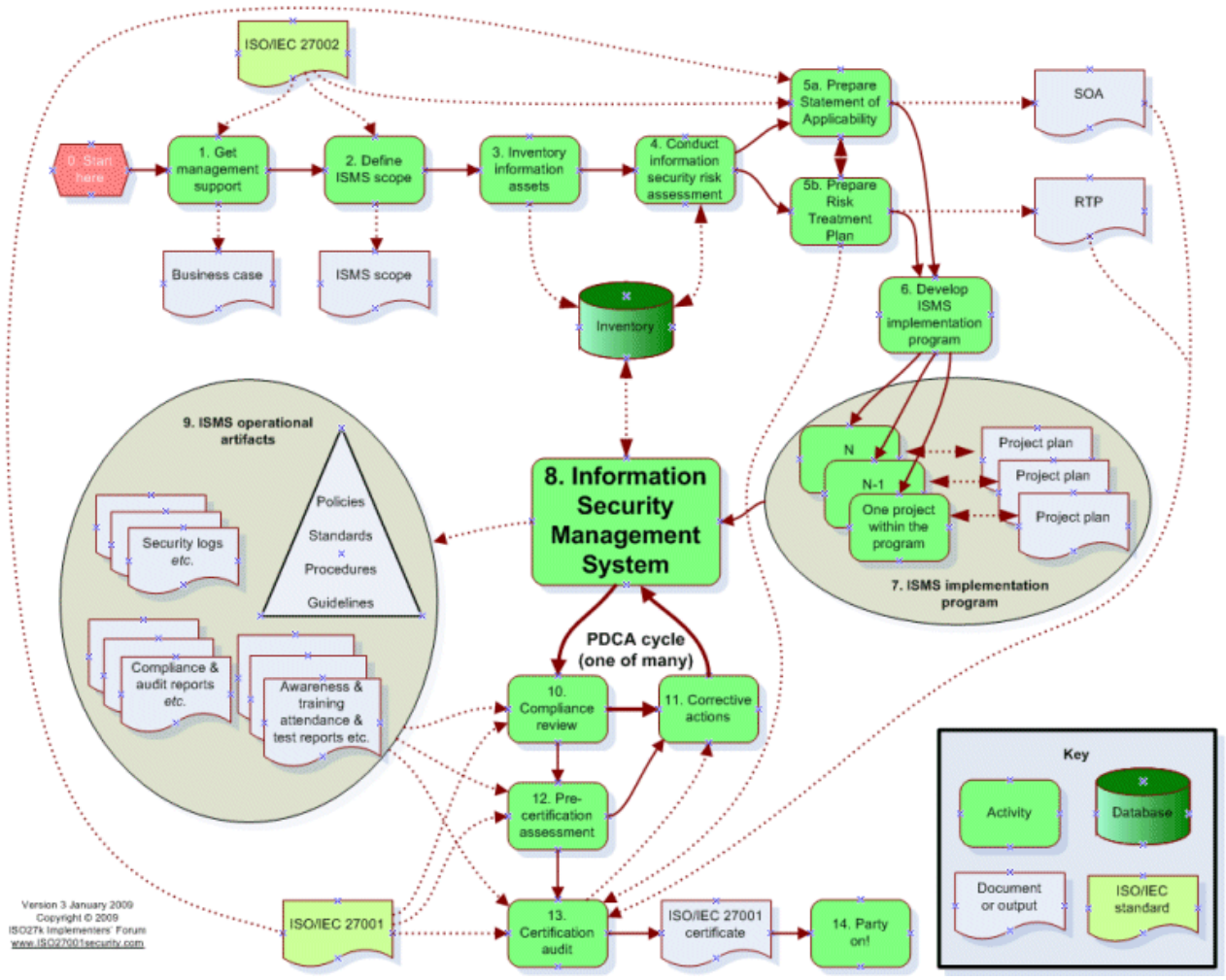
to the Plan-Do-Check-Act Deming cycle normally found in ISO 9000 quality management systems.

Certification involves contacting a suitable accredited certification body to review your Information Security Management System ... [continues below]

Implementation tip: establish contact with the certification auditors as soon as you like. They don't bite and most will happily answer basic questions about the process if it means a smoother audit for both of you in the long run.

Q: "What is *really* involved in becoming ISO/IEC 27001 certified?"

A: See the overview ISMS implementation and ISO/IEC 27001 certification process diagram:



The flow chart gives a high level view of the major steps in the process. This is a generic diagram - the details will vary from situation to situation. The main activities are as follows:

1. **Get management support** - easier said than done! This typically involves raising management's awareness of the costs and benefits of having a ISO/IEC 27001 compliant ISMS. A great way to start is to raise management's awareness of some of the key current information security risks and potential good practice controls (drawn from ISO/IEC 27002) that are not yet in place, perhaps through a "gap analysis" (outline risk assessment) followed by a business case and/or strategy for the security improvement (ISMS implementation) program.
2. **Define ISMS scope** - what businesses, business units, departments and/or systems are going to be covered by your Information Security Management System?
3. **Inventory your information assets** - the inventory of information systems, networks, databases, data items, documents *etc*. will be used in various ways *e.g*. to confirm that the ISMS scope is appropriate, identify business-critical and other especially valuable or vulnerable assets *etc*. (more below)
4. **Conduct an information security risk assessment** - ideally using a recognized formal method but a custom process may be acceptable if applied methodically. More advice below.
5. (a) **Prepare a Statement of Applicability** - according to ISO/IEC 27000, the SoA is a "documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS". Which of the control objectives from ISO/IEC 27002 are applicable to your ISMS, and which are irrelevant, not appropriate or otherwise not required? Document these management decisions in your SOA; and in parallel ...
   (b) **Prepare Risk Treatment Plan** - ISO/IEC 27000 describes the information security RTP as "a plan that identifies the appropriate management actions, resources, responsibilities, timeliness and priorities for managing information security risks".
6. **Develop ISMS implementation program** - given the scale, it is generally appropriate to think in terms of an overall program of individual projects to implement various parts of ISO/IEC 27002, for example one project for each of the main sections of the standard. Which resources can you call upon, direct, use, borrow or persuade to build or supplement your core ISMS implementation team? You will probably need experienced information security professionals (particularly to lead the team) and

support from a variety of related functions such as Internal Audit, Risk, Compliance, HR, Finance and Marketing, not just IT. You are advised to plan the work in risk-priority-order where possible *i.e.* tackle the biggest risks early so that, whatever happens to your program of work in practice, it has had a good go at knocking down the main issues and can demonstrate real progress, even if it then falters for some reason. Also, early wins are a source of helpful positive feedback: this is an important aspect to the program which as to be seen to be effective by management, as well as actually being effective. If all the program does is interfere with business, annoy managers and cost a packet, it is hardly going to be on the shortlist of "things we really must keep doing next year"!

7. **Run the ISMS implementation program** - through the individual project plans, the implementation team sets to work to implement the controls identified in the RTP. Conventional program and project management practices are required here, meaning proper governance, planning, budgeting, progress reporting, project risk management and so forth. If the program is large, seek professional program management assistance.
8. **Operate the ISMS** - as each project in the program fills in part of the ISMS, it hands over a suite of operational security management systems and processes, accompanied by a comprehensive set of policies, standards, procedures, guidelines *etc*. *Operating the ISMS has to be an ongoing routine activity for the organization: this is not a one-shot project!* The Information Security Management function needs to be established, funded and directed, and many other changes are likely to be required throughout the organization as information security becomes part of the routine.
9. **Collect ISMS operational artefacts** - the ISMS comprises your framework of security policies, standards, procedures, guidelines *etc*., and it routinely generates and uses security logs, log review reports, firewall configuration files, risk assessment reports *etc*. ... all of which need to be retained and managed. These artefacts are crucial evidence that the ISMS is operating correctly. You need to build up sufficient artefacts to prove to the auditors that the system is operating, stable and effective.
10. **Review compliance** - are you actually doing what you said you were going to do? Section 15 of ISO/IEC 27002 covers compliance with both internal requirements (corporate policies *etc*.) and external obligations (such as laws and industry regulations). The ISMS itself needs to incorporate compliance testing activities which will generate reports and corrective actions. Internal compliance assessments, and perhaps external/independent assessments (audits, penetration tests *etc*.) are therefore routine activities in a mature ISMS. The ISMS operational

artefacts produced in step 9 are a major source of evidence for such compliance activities - they give the auditors something to test.

11. **Undertake corrective actions** - to improve the ISMS and address risks. The "Plan-Do-Check-Act" Deming cycle is central to the 'management system' part of ISMS and should result in continuous alignment/re-alignment between business requirements, risks and capabilities for information security. As with quality management systems, the idea is to give management a means of controlling information security management processes systematically such that they can be continually monitored and improved, not least because perfect security is an unattainable goal in any real world situation.
12. **Conduct a pre-certification assessment** - when the ISMS has stabilized, an accredited certification body or other trusted, competent and independent advisor is invited by management to check whether the ISMS is functioning correctly. This is largely a compliance assessment but should ideally incorporate some independent review of the scope, the SOA and RTP to make sure that nothing important has been missed out of the ISMS, especially as the business situation and information security risks have probably changed in the months or years that it will have taken to implement the ISMS. It is a golden opportunity for your organization to identify and tie up any remaining loose ends before the actual certification audit. It's also a good low-impact way to get to know the auditors.
13. **Certification audit** - when management is happy that ISMS is stable and effective, they select and invite an accredited certification body to assess and hopefully certify that the ISMS complies fully with ISO/IEC 27001. The auditors will check evidence such as the SOA, RTP, operational artifacts *etc*. and will attempt to confirm that the ISMS (a) is suitable and sufficient to meet the organization's information security requirements in theory *i.e.* it is correctly specified; and (b) actually meets the requirements in practice *i.e*. it is operating as specified.
14. **Party party** - seriously, when it's all over, celebrate your success. You've earned it! More than that, your ISO/IEC 27001 certificate is a valuable asset. The organization should be proud of what it has achieved, knowing of course that information security is never really "done". With your certified ISMS operating normally, take a good look at the information security arrangements in place at your supply chain: are your suppliers, partners and customers also certified? Are they certifiable? Do they need your encouragement? If you haven't already done so, please join the ISO27k Forum to share your experience with others who are in the process.

Implementation tip: genuine management support is the *sine qua non.* Time invested in explaining to managers what the ISMS is and more importantly how it benefits the organization is time well spent. At the same time, listen hard to find out what managers really need from information security and pick up opportunities for strategic alignment. If the ISMS *supports or enables* key business objectives, it is less likely to be seen as an impediment to progress, and is harder for reluctant managers to resist.

Q: "Will the security controls we have already implemented be sufficient for the final ISO 27001 certification?"

A: Unlikely, unless your organization already has a full suite of mature best practice security controls, supporting a comprehensive ISMS! Controls already in place won't be wasted but (in my experience) will probably need improvements, most likely documentation for a start and probably some extensions to cover the whole breadth of ISO/IEC 27001 or ISO/IEC 27002. Identifying and initiating any necessary security improvements is the first step towards a true self-sustaining ISMS. This process will eventually become a routine part of your ISMS.

Implementation tip: look for alignment between internally-driven information security requirements and those imposed by compliance obligations such as SOX, PCI DSS, privacy laws *etc*.

Q: "Are there levels of compliance with ISO/IEC 27001, or are organizations simply compliant/noncompliant?"

A: In reality, there are 'degrees of compliance' with ALL laws, rules, regulations and standards ... but not as far as the laws, rules, regs and standards themselves, and perhaps the authorities normally behind them, are concerned. ISO/IEC 27001 for instance is worded as if organizations **absolutely must without any dispute fully comply** with all its core mandatory requirements concerning the management system. The intention was to leave no wiggle-room.

When certifying an organization in practice, however, the certification auditors will accept all the management system elements or processes that are clearly fully compliant with the standard, and will consider and discuss with management any aspects that are not quite so clearly or fully compliant, before making a decision as to whether or not to issue the certificate. At the end of the day, it is a matter of judgment as to whether the standard's requirements are satisfied sufficiently to issue or renew a certificate.

Implementation tip: aspects of the standard that seem most 'challenging' are likely to be the ones that the organization needs to put most effort into getting right prior to the certification audits. The auditors may probe more deeply into those same areas if there are concerns, but occasionally organizations are tripped up by things that seem relatively straightforward or easy: this is where the auditors' independence and competence come to the fore. Experienced auditors know the standards well and see many organizations struggling with various aspects, so they can often spot issues and maybe even suggest solutions that the organizations themselves may fail to see.

Q: "Who can certify us against ISO/IEC 27001?"

A: *Anyone.* You can even do it yourself! However, the certificate only has real meaning and value if it is issued by a recognized Certification Body (CB - also known as registrars *etc*. in some countries), which in practice means they should have been accredited by a recognized accreditation organization. "Accredited" means their certification practices have been checked to ensure that the certificates issued are legitimate, trustworthy and meaningful. If compliance certificates were issued by anyone who felt like it, the certificates and potentially ISO27k as a whole would soon lose value and be discredited. The formality in the process builds and maintains confidence and trust. The accreditation process (*i.e*. checking that CBs are competent and suitable to assess clients against ISO/IEC 27001) is itself the subject of ISO/IEC 27006.

Aside from CB companies, individual auditors may be accredited by bodies such as the International Register of Certificated Auditors (IRCA). They generally work for large consultancies or system integrators, though some are self-employed or work in small companies.

Find your national accreditation body/bodies listed here. Contact an accreditation body for details of the CBs they have accredited. You can cross-check using Google or sites such as the register of ISO/IEC 27001 certificates which identifies the accredited CBs that issued the certificates, and has a separate list of them here.

Implementation tip: see the next Q&A ...

Q: "How do we choose a Certification Body?"

A: Start with ISO's advice on choosing a Certification Body (CB) and the role of accreditation.

In essence, choosing a CB is like selecting any service supplier, so you should follow your standard vendor selection, procurement and contracting practices. In

short, figure out what you want (your criteria), review available service offerings on the market against the criteria, select the best fit and then make the purchase.

These are examples of the kinds of criteria you might consider:

- Vendor quality, standing, reputation *etc*., in particular their accreditation status (see below);
- General vendor selection criteria such as their ethics, policies and practices for health and safety, equality, corporate responsibility, environment *etc*.;
- Technical competence, qualifications and experience of the ISMS auditors they will actually assign to the job;
- Their working practices, procedures *etc*. (*e.g*. will they permit your ISMS internal auditors to shadow and support their auditors?);
- The quality, breadth and utility of typical/example/sample/template reports and other outputs (aside from the formal compliance certificate, you may for example find value in the completed assessment checklists or improvement suggestions and advice from the CB auditors if they will share them with your management or ISMS internal auditors);
- Value for money (there's more to this than price!);
- Availability *e.g*. timescales within which they can complete the job;
- Past performance *e.g.* previous jobs for your organization, credible customer references, or suggestions from industry peers, local contacts or other auditors and trusted advisors;
- Their information security and privacy arrangements (see further below);
- Other factors - develop your own unique criteria.

You may prefer to prioritize or weight your criteria and prepare a scoring spreadsheet, but it's hardly worth the effort for such a simple activity with, probably, a rather limited shortlist of candidate suppliers from which to select. Check the vendors' marketing and sales collateral though, as differences in their proposed approaches to the job may help you choose between them.

The accreditation status of your chosen CB is important if you are expecting your ISO/IEC 27001 compliance certificate to be credible to, and hence trusted by, third parties such as your suppliers and business partners. *Anyone* can issue you with a compliance certificate - you can even self-certify if you like, or ask your implementation partners for one - but third parties who will rely on the certificate normally *insist* on certificates issued by CBs that are independent, competent and trustworthy. In practice, this means the CB must have been properly accredited by trustworthy bodies such as the UK Accreditation Service (UKAS). To be accredited by the likes of UKAS, CBs are formally assessed or audited against applicable, internationally recognised standards regarding their competence,

impartiality and capability. Accreditation reduces the possibility of selecting an incompetent CB, and increases the value of the certificate. Oh and by the way, don't forget to confirm their actual accreditation status with the accreditation body, as anyone may *claim* to have been accredited.

ISO/IEC 17021 lays out the principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types (such as management systems for quality, environmental protection and information security), while ISO/IEC 27006 offers additional, more specific advice for ISMS CBs.

Information security should be one of your CB selection criteria. It is not unreasonable to assume that ISMS auditors should have the professional knowledge and expertise to protect your sensitive information, but since they will be given privileged access to your organization's ISMS (and perhaps to the facilities and other assets) you need to assess the risks and treat them in the normal way. Its up to your management to determine whether these risks are material in relation to the information security risks associated with other suppliers, business partners, customers *etc*., and other risks, and so whether and how to treat them.

Legitimate, accredited ISO/IEC 27001 CBs are forbidden from auditing customers of their ISMS-related consultancy services in order to avoid the obvious conflict of interest. Your ISMS implementation consultants and advisors may, however, be able to help you find and select suitable CBs if you wish.

Implementation tip: at the very least, be sure the contract with your chosen CB incorporates a suitable nondisclosure, confidentiality or privacy clause. An ISMS CB can hardly object to you taking an interest in their information security arrangements after all, and they might just give you credit for asking!

Q: "How does the certification process work?"

A: The ISO/IEC 27001 certification process is essentially the same as that for ISO 9000 and other management systems. It is an external audit of the organization's ISMS (Information Security Management System) in three main phases:

1. **Pre-audit** - having engaged an accredited certification body, they will request copies of your ISMS documentation, your policy manual *etc*. and may request a short on-site visit to introduce themselves and identify contacts for the next phase. When you are ready, they will schedule the certification audit itself by mutual agreement.

2. **Certification audit** - this is the formal audit itself. One or more auditors from the accredited certification body will come on site, work their way systematically through their audit checklists, checking things. They will check your ISMS policies, standards and procedures against the requirements identified in ISO/IEC 27001, and also seek evidence that people follow the documentation in practice (*i.e.* the auditors' favorite "Show me!"). They will gather and assess evidence including artifacts produced by the ISMS processes (such as records authorizing certain users to have certain access rights to certain systems, or minutes of management meetings confirming approval of policies) or by directly observing ISMS processes in action.
3. **Post-audit** - the results of the audit will be reported formally back to management. Depending on how the audit went and on the auditors' standard audit processes, they will typically raise the following (in increasing order of severity):
   - **Observation** - information on minor concerns or potential future issues that management is well advised to consider;
   - **Minor noncompliance** - these are more significant concerns that the organization has to address at some point as a condition of the certificate being granted. The certification body is essentially saying that the organization does not follow ISO/IEC 27001 in some way, but they do not consider that to be a significant weakness in the ISMS. The certification body may or may not make recommendations on how to fix them. They may or may not check formally that minor noncompliances are resolved, perhaps relying instead on self-reporting by the organization. They may also be willing to agree a timescale for resolution that continues beyond the point of issue of the certificate, but either way they will almost certainly want to confirm that everything was resolved at the time of the next certification visit;
   - **Major noncompliance** - these are the show-stoppers, significant issues that mean the ISO/IEC 27001 certificate cannot be awarded until they are resolved. The certification body may recommend how to resolve them and will require positive proof that such major issues have been fully resolved before granting the certificate. The audit may be suspended if a major noncompliance is identified in order to give the organization a chance to fix the issue before continuing.

They will also issue your certificate of course, assuming you passed the test!

There are periodic follow-ups after the initial certification process for as long as the organization chooses to maintain its certification. The certificates are valid for three years so there is a formal recertification every three years, but additional interim reviews are common, especially in larger organizations.

Implementation tip: like exams, certification audits get more familiar if not easier with practice. Treat readiness reviews, internal audits and pre-assessment reviews as opportunities to learn about the audit process as well as sources of information about areas needing improvement, prior to the main certification audit. During and after the process, talk to managers and others involved in the process about how things are going, and share any good news. We'd love to hear how it went on the ISO27k Forum for instance! Treated sensibly, the external reviews are all valuable opportunities to confirm that your ISMS remains effective, and to pick up benchmarking tips from the consultants and auditors with experience of other compliant organizations.

Q: "Do we need to address or achieve *all* of the control objectives in ISO/IEC 27002?"

A: Not necessarily for certification. Remember that organizations are certified against ISO/IEC 27001, not ISO/IEC 27002. While compliance with the main body text of 27001 (the bits concerning the management system) is considered *mandatory* for certification, the control objectives in annex A (the bits concerning information security, summarized from ISO/IEC 27002) are *optional*: organizations choose whichever of those security control objectives they deem relevant and necessary to address their information security risks, then select the security controls (or indeed other risk treatments *e.g.* avoiding or transferring some risks) that they feel are applicable. As well as not necessarily selecting the whole of annex A, organizations may well introduce additional control objectives and controls, including those from other standards, laws, regulations and good practices. It's a flexible approach that caters for quite different organizations and risks.

Strictly speaking, certification does not even depend on the organization fulfilling all the security control objectives that it has selected, just so long as the management system complies with the requirements of ISO/IEC 27001. It is presumed that a compliant ISMS will successfully ensure that the security control objectives will be satisfied in due course, and indeed this is in the organization's interests, regardless of certification, since failing to meet those objectives implies a failure to mitigate unacceptable risks.

Implementation tip: be careful when scoping your ISMS, considering your information security risks and selecting applicable control objectives, because there are costs involved in meeting those objectives. The ISMS may encompass additional control objectives beyond those listed in the SoA, no problem, but must ensure that the listed objectives are addressed. Information security professionals tend to want to include and manage all the security objectives and

controls, but the business is likely to be most concerned about a smaller subset, implying a useful focus that can be used to prioritize the essential elements.

Q: "This is all very complicated and uncertain. There are so many variables! Isn't there just a simple checklist we can follow, like PCI-DSS?"

A: No there isn't. Protecting an organization's information assets is inevitably a complex challenge, considering that there are so many possible threats, vulnerabilities and impacts, and so many assets to protect.

PCI-DSS (the Payment Card Industry Data Security Standard) has a narrower scope than ISO27k, purely concerning the IT systems and processes for handling credit and debit card data, but even there it could be argued that the prescriptive checklist approach is patently inadequate (witness the number of significant card date breaches in the headlines, affecting organizations that had evidently passed their independent PCI-DSS compliance audits). Achieving and maintaining PCI-DSS compliance may seem like a substantial challenge for many organizations but in reality, PCI-DSS is barely adequate for its intended purpose. It mandates a basic, minimal suite of information security controls, some of which are known to have significant flaws (*e.g*. WEP, not recommended but still permitted under the current version 1.2 of PCI-DSS). Bare PCI-DSS compliance may be sufficient to get the QSA auditors off your back but it is not enough to protect valuable information assets.

An effective and comprehensive ISMS based on ISO27k or something similar such as SP800-53 FISMA or ISM^3 should *exceed* PCI-DSS and other third external security compliance obligations, and simultaneously generate additional business benefits through satisfying internally-derived security requirements (*e.g.* protecting valuable but sensitive proprietary data from competitors).

Implementation tip: wise up! Take a step back to consider the broader business context within which information security exists, and the myriad issues at stake. Think about the need to identify and protect *all* your information assets against *all* significant security risks. If you examine the costs and benefits honestly, investing in a comprehensive security management system is the most professional and effective way to deal with this.

You *can* start by restricting the scope of your ISMS to certain business units, functions or departments. This simplifies the problem space somewhat and gives you the chance to establish and gain experience with the management system, *but* it also limits the potential benefits and is not necessarily the best solution.

Q: What if things change *after* we are certified?

A: That depends on the nature and scale of the change. Relatively small changes to the ISMS are *expected* to occur as it naturally evolves in line with changing business needs for information security, for example through the action of various internal reviews triggering corrective and preventive actions: these should have no effect on your certification status since they are an anticipated and normal part of any ISMS. Larger scale business/organizational changes may involve significant changes to the scope of the ISMS, for example other parts of the business being integrated with the ISMS, mergers/acquisitions or downscaling/divestments: these may be substantial enough to invalidate your original certificate without at least a surveillance visit from your certification auditors, but it's impossible to give hard-and-fast rules. Whether your ISMS changes are deemed substantial enough to invalidate your certificate, or to warrant recertification, depends on several factors such as:

- The scale or size of the change/s;
- The nature or type of change/s;
- The likely impact of business/organizational changes on your ISMS and/or information security risks and hence risk treatments required;
- How long it has been since your last certification or surveillance audit, and how long before the next one; and
- The certification body's policies and practices in this regard.

Aside from the certification angle, you should definitely update your information asset and information security risk/control registers and maybe your Statement of Applicability. You may need to update your security policies and perhaps restructure the team managing and running the ISMS, which may well imply the need for a new budget. Don't forget to check your ISMS internal audit plans too, and if appropriate adapt your metrics to take account of the full ISMS.

Implementation tip: arguably the best advice is to stay in touch with your certification body, keeping them updated with (significant) changes and giving them the opportunity to say whether further surveillance visits or compliance audits are in order. Building a good working relationship with your auditors has the distinct advantage of "no surprises" on both sides, but it takes a little effort to establish and maintain the relationship, as indeed do all relationships (business or otherwise!).

ISMS auditing

Q: "I work for an Internal Audit function. We have been asked by the ISMS implementation project team to perform an ISMS internal audit as a prelude to an external/third party certification audit against ISO/IEC 27001. They are asking for a load of things from us and expect us to do the audit within a tight timescale defined on their plans. Is this information really needed? Are we (as an independent audit team) forced to give them such information? Should we perform a quick Internal Audit or take the time necessary although the certification would be postponed? Are there ISMS Audit Programme/Plan templates we can use and what other considerations should we take into account for the ISMS internal Audit? ..."

A: If you are a truly independent audit team, you do not answer to the ISMS project team and they cannot force you to provide information or do things for them in a certain way. However, as Internal Audit, you work for - or at least in conjunction with - the organization's senior management and would presumably be expected to support the organization's strategic aims. If the ISMS has management's full support [a not insignificant assumption - something your audit might want to establish!], it is reasonable for them to invite you to audit it thus fulfilling the requirements for ISMS internal audits, and arguably also to ask about your competence/qualifications to do so. However, the manner in which you perform the audit, the way you plan and perform it, is really your domain. For example, you would need to develop the audit program, schedule the work, assign suitable auditors *etc*. How much advance notice and other information to give them is up to you, although in the interests of making the audit as effective as possible, I would try to work with them on this. Right now, they are probably quite sharply focused on compliance with ISO/IEC 27001 and are simply trying to fulfil the standard's requirement for internal ISMS audits, which you should read to understand. It sounds as if they are perhaps unfamiliar with the way you normally work, and probably have a naïve view of how you would approach the job. They almost certainly presume that your audit would be entirely constrained within the scope of their ISMS whereas you would probably be interested in the wider picture, potentially including security and risk management issues elsewhere in the organization.

On a more positive note, it makes a nice change for auditors to be "invited" in by their prospective auditees! This could be an ideal opportunity for Internal Audit to get to work on the ISMS and make positive recommendations for improving the organization's information security controls, risk management, compliance and governance (at least within the scope of the ISMS for now), knowing that the

implementation team and hopefully management has the incentive to address any issues quickly in order not to stall or preclude the certification. Personally, however, I would be cautious about being too ambitious with your audit at this stage since recommending major changes could be seen as derailing the ISMS project, while a softly-softly approach would leave the door open for further ISMS audits supporting their PDCA-based internal management review and improvement activities. With an effective ISMS in place, you can expect the information security situation to be more stable as it comes under better management control, and then to improve gradually of its own accord. You have a part to play in making this happen as effectively and efficiently as possible. In particular, your independent viewpoint gives you the advantage of making sure that the ISMS is not blind-sided by some unanticipated issue that the ISMS management team was unaware of, and the chance to promote generally accepted good risk/security management practices based on the standards or other sound sources.

Implementation tip: this is a learning opportunity for all those involved, including you and your audit colleagues. Sit down with those in charge of the ISMS (both the implementation project managers and the business/information security managers who will run the ISMS in perpetuity, plus your own audit management) to talk about what they have done, what they anticipate you doing now, and how they see the relationship developing over time. An ISMS is a long-term commitment to professional information security management and that surely has to be a positive thing for audit and the organization. You probably should consider some training or familiarity with ISMS, ISO27k standards *etc*. and possibly consultancy support from auditor/s familiar with ISMS internal audits and certification audits to get you off to a flying start, unless you already have experience and skills in this area. You asked about templates for ISMS auditing: I would suggest looking to ISACA, IIA or other professional groups for some support, plus of course the ISO27k standards themselves and your existing audit procedures. In due course, though, I'm sure you would soon pick this up on the job and, by the way, it will not hurt your CV!

Q: "I am not an experienced auditor. How should I go about planning and performing an ISMS internal audit?"

A: You might start by reading ISO 19011, the ISO standard for auditing quality and environmental management systems, for general advice, plus ISO/IEC 27007 for more specific advice on ISMS audits. Your Internal Audit function, if you have one, is another obvious place to seek help and the IT audit FAQ offers more detailed guidance. ISACA is another fantastic, highly recommended resource. ISO/IEC 27008:2011 is available as a desperate last resort!

Meanwhile, the typical audit process goes something like this in my professional experience as an internal IT auditor:

1. Agree the scope (what's in and just as importantly what's out of scope?), purpose/objectives and criteria for the audit (*e.g*. man-days or elapsed time available, expected audit deliverables) with audit and maybe business management. [Each audit normally flows from some form of risk-based annual audit planning and scheduling.]
2. Review the situation and the background to the audit, considering the risks potentially of concern in the area of scope and any concerns or loose ends arising from prior audit reports, management reviews *etc*. You may need to do some initial scoping/feasibility work on the job, and check any previous ISMS-related audit reports and maybe the audit files to get a feel for the likely problem areas. Either way, try not to lose sight of your independence, in other words think about the risks and issues in broad, fairly theoretical terms, assuming nothing about the controls that one would naturally expect to be in place just in case they aren't.
3. Draw up an audit work program, Internal Controls Questionnaire (ICQ), checklist (or whatever you call it) showing the issues you intend to check and indicating in what level of detail you will check them. Leave yourself some space for notes to record findings and your initial analysis while things are still fresh in your mind.
4. Consider and plan the audit fieldwork *i.e.* how you will actually check the things of interest on your ICQ *e.g*. through interviews, observation, data analysis, sampling, testing ... Draw up your shopping list of things you will need, people you want to speak to *etc*. and reconfirm the timescale for the audit assignment: you will often have lined yourself up more work than you can reasonably complete in the time available, so revisit the scoping for clues about management's priorities for the audit.
5. Identify and contact your lead contact/s for the audit and work with them to line up and prepare for the fieldwork, hopefully sorting out many of the items on your shopping list (*e.g*. arranging initial interviews, obtaining reports, policies *etc*. that you will want to review). It's best to contact the contact as early as possible in the process: good contacts can help with the planning too, but be cynical if they try to steer you away from anything!
6. Perform the audit fieldwork, keeping your contact up to date with developments, preliminary findings, concerns, any problems conducting the audit *etc*. A helpful audit contact can act as a sounding board for emerging audit concerns and possible recommendations, and a source of additional inside knowledge. Work systematically through your ICQ.

7. Analyze the findings, generating a list of priority issues (must-fix items) and 'additional items' (often included in reports just for information, but that depends on audit working practices). My preference is to draw up a "SWOT" analysis identifying the key Strengths, Weaknesses, Opportunities and Threats - no more than about 5 or 6 items per category to keep things at a high level. You may need to revisit certain parts of the ICQ to confirm significant findings, collect additional evidence, and generally substantiate the key issues. Try to stay objective, for instance basing your work on *facts* backed by *audit evidence*.
8. Prepare a draft audit report and recommendations addressing the priority issues, and get this reviewed within the audit function, or by your manager at least. A 'file review' is normal in order to confirm that everything reportable is being duly reported, and everything reported is traceable to sound audit evidence. This requires sorting and indexing the audit evidence, cross-referencing it to the ICQ *etc*.
9. Work with senior and middle management to clarify any audit concerns and recommendations, and to align priorities and timescales with business objectives/constraints. Normally, as part of this phase, you would present and discuss the SWOT analysis, the draft audit report and the key findings and recommendations with client management. Discuss the recommendations, and seek their outline agreement to the actions arising. It's important to give management some time and space to consider anything serious, particularly if they would have to juggle priorities and assign resources to this. You may need to meet senior managers individually to explain and discuss things further, and sometimes to consider alternative approaches (business managers generally know best how to implement improvements, but you should by now have established your credibility and hence have influence).
10. Finalize the report, ideally including a firm action plan with dates and responsibilities for resolving the issues and even better something from management formally confirming that they accept the report and intend to carry out the recommendations.
11. Issue the report to the appropriate people. It may help to create and circulate a brief executive summary (maximum 1 or 2 sides) for senior management but make the full report available to those who need the details.
12. Decide whether and how to follow-up to ensure that the action plans are in fact completed properly, *if* this is audit's responsibility [it varies between organizations: in some, management is entirely responsible for completing

recommended and agreed actions]. In others, management request audit's help to check for completion.]

13. Follow-up and if necessary escalate any outstanding issues to (more) senior management. If appropriate, revisit the findings and risks to confirm if the issues raised are still of concern, and apply pressure through management to get the job done.
14. Close the audit file. Prune out the irrelevant information, keeping relevant evidence, reports, feedback from management *etc*. and making notes for the next ISMS audit. Store the audit file securely as the contents are probably somewhat sensitive.

For pure compliance audits (such as ISO/IEC 27001 certification audits), the key risks and issues relate to non-compliance with mandatory requirements laid out in the standards of course, and ISO/IEC 27006 may help. For pure management systems audits, the focus is self-evidently on the management system and processes, which are driven by ISO/IEC 27001. For more broadly-scoped ISMS internal audits, there may well be other more or equally important issues worth reviewing for the business ... like for example the small matter of whether the information security controls are adequate (see ISO/IEC 27008).

Implementation tip: personally, I prefer drawing up mind-maps to help me think through the likely risks and anticipated controls, and to structure each audit job. Process diagrams, flowcharts, swimlane charts, Ishikawa (fishbone, cause-and-effect) diagrams and so on may suit you better. Don't forget to include sufficient contingency time in your audit plan, for instance allowing you to delve more deeply into any areas of serious concern that emerge from the audit.

Q: "How can we confirm the implementation of controls selected in the Statement of Applicability?"

A: If the auditors are coming, they should be able to check that your identified ISMS controls are truly in operation, not merely listed as such in some dusty old policy manual or intranet website. Evidence is key! For example, you need to have experienced at least one incident to confirm that the incident management process actually works in practice and is not just a fine set of words in your ISMS policy manual. This is analogous to the situation with ISO 9000 where the auditors typically check that genuine quality issues have been identified through quality reviews *etc*., addressed following the stated QA processes and resolved, not just that you say you will deal with them in a certain way should they ever happen.

Clearly, it is not reasonable to wait until there has been a complete disaster to check that your contingency planning processes function correctly - there are pragmatic limits to this principle, thankfully! But you should probably have completed at least one contingency planning exercise or Disaster Recovery test including the vital post-test washup to identify things that need fixing. For common information security controls that are in action all the time (*e.g.* antivirus, access controls, user authentication, security patching), the auditors will want to check the evidence (they may call them "artefacts" or "records") relating to and proving operation of the information security management processes.

Remember, an ISMS is for life, not just for the certification process.

Implementation tip: it's best if possible to hold off the certification auditors for a few months after the ISMS is considered "done", in order to build up your stock of evidence demonstrating that the processes are operating correctly, in addition to letting the processes settle down a bit. Your implementation project plans should therefore show a short hiatus after the implementation should be finished but before the certification auditors are due to arrive, supplementing the usual contingency allowance in case of implementation delays.

Q: "How can we determine whether the control objectives are fulfilled?"

A: Fulfilment of security control objectives can be determined by management, by auditors or by others checking the controls to decide the extent to which the corresponding objectives are satisfied. Security incidents in those areas obviously suggest that the controls are less than perfect. Objectives that are not sufficiently satisfied are obvious candidates for security improvement, but the prioritization or urgency or necessity of that work depends on the significance of the risk and the degree of noncompliance. For example, a control objective to minimize malware risks may require "up-to-date antivirus software running on all applicable systems". The antivirus software used, the updating process, the range of systems to be protected, and the realities of implementing the control on a wide range of systems mean that some systems may not be fully protected right now for a variety of practical reasons, but so long as all the main/most important systems and a large proportion of the remainder are adequately protected, the organization may (or may not) be willing to accept the residual risk. Management may even make a conscious risk management decision not to insist on full implementation of antivirus if the costs of doing so on every single system outweigh the benefits.

Implementation tip: this is a risk management decision best made by managers, particularly Information Asset Owners who are accountable for

protecting information assets. Information security and risk management people can advise them, of course, but should avoid going beyond their brief and, in effect, accepting accountability for information security matters that rightfully belong to management.

Q: "Will the certification auditors check our information security controls?"

A: To a limited extent yes but the primary purpose of the certification audit is to confirm whether you have an effective ISMS in operation, not whether you have secured your information assets. It's a subtle but important difference. As Patrick Morrissey put it on the ISO27k Forum, "An ISO/IEC 27001 certificate does not mean that your organization is secure: it states that your ISMS is working. Period." The underlying principle here is that if you have an effective ISMS in operation, then the ISMS will ensure that there are adequate security controls in place. This approach also means that strictly speaking you needn't necessarily have a completely comprehensive suite of information security controls to pass the certification audit, just so long as your ISMS is adequate to ensure that it will improve in due course. The vital concern is that the organization should have information security under management control and be proactively directing and controlling it.

The certifications auditors may, however, need to do *some* substantive testing of the information security controls to confirm that you are in fact doing what you say you are doing, just as they may check that, for example, you have undertaken an information security risk analysis and duly considered the risks in you specific context in order to specify your control requirements. In other words, they will seek evidence that the ISMS processes are operating correctly and in many cases that will involve confirming that certain security controls are operational.

Implementation tip: regardless of whether the certification auditors do or do not audit the controls, the organization should still be checking its own information security controls routinely, typically through management reviews and internal audits since this is one of the "Check" processes within the PDCA cycle in the ISMS. The certification auditors may therefore ask to see some evidence that you are routinely checking your controls, for example management review or internal audit reports, along with agreed action plans to address any improvement recommendations (*i.e.* the "Act" part of PDCA).

Q: "How will the certification auditor check our ISMS internal audit processes? I'm nervous! What are the typical questions we should expect?"

A: Assuming they represent an accredited certification body, the auditor/s will have been trained and will act professionally, diligently checking compliance with the ISO/IEC 27001 standard following a standardized audit process derived from the ISO/IEC auditing and certification standards.

ISMS internal audits are a relatively small but quite important element of the ISMS in terms of continuous improvement and assuring compliance with your security policies, laws *etc*., so you can expect the auditor to explore your internal audit practices a little, more or less depending on how much time they have and how much risk they consider is associated with the internal audits as compared to other aspects of the ISMS.

A certification auditor's prime objective is self-evidently to check your organization's compliance with the standard's formal specifications, so at its most basic they will look at what ISO/IEC 27001 specifies for ISMS internal audits under clause 6 and ask you to demonstrate how you do it, using the evidence from past ISMS internal audits as proof.

The auditor will probably review and question you regarding your ISMS audit plans, procedures and report/s, exploring aspects such as:

- *How* you audited: did you perform the audit in accordance with your own audit policy/standard/process? Are your ISMS internal auditors competent (what are their qualifications and experience at ISMS or other types of audit)? Are they truly independent of the areas being audited (independence is the critical distinction between audits in section 6 of ISO/IEC 27001 and management reviews in section 7)?;
- *What* you audited: did the scope of the audit match that of the ISMS, or was it more limited in scope, in which case are you planning to fill in the gaps later?
- What you *found*: this will give the auditor clues about the state of your ISMS and may identify issues/concerns deserving further investigation;
- What was the *outcome*, in other words what did the audit achieve? Did all agreed audit recommendations (including corrective actions arising from non-conformities but possibly also more creative improvement suggestions) get fully actioned and signed-off on time and was your ISMS actually improved? More generally, how does management react and respond to audits? Do they take them seriously? Do ISMS internal audits add value to the organization?

Listen carefully to any summing up or findings or recommendations the auditor makes as there may well be some helpful suggestions about how to improve your

ISMS, and if they are stated by an independent, competent external auditor, they tend to carry weight with management. Even if the final audit report officially says “No issues, fully compliant”, the auditor may raise minor concerns, snags or improvement suggestions informally. A good auditor will also compliment your organization on certain aspects of its ISMS, and those kinds of comment make good security awareness materials. It's nice to be given a clean bill of health and to be certified compliant, but a positive comment about something your organization is doing well can really make someone's day!

Implementation tip: take it easy, don't fret! Like taking an examination, the audit should go smoothly provided you have done your homework. Preparing your paperwork in advance of the auditor's visit will help you both. Sort out your ISMS policies, audit plans, audit files, audit methods, audit reports *etc*. - get them straight and be ready to offer the information promptly if/when the auditor asks for it (don't just dump everything on them in a big pile and say “Help yourself”!). If you are well organized and helpful, it will make the auditor’s job easier *and* increase confidence in how you conduct your internal audits.

Q: “What are our options if we disagree or have an issue with the certification auditors?”

A: The accredited certification auditors hold almost all the cards in respect of certification audits. To a large extent, what they say goes since they can steadfastly refuse to issue a certificate if they believe their client is noncompliant with a mandatory requirement. ISO27k certification auditors must audit strictly against the formal specifications in ISO/IEC 27001 (no more, no less). The accreditation process, plus the standards relating to audit processes and certification, are designed to ensure that that is exactly what happens. The whole certification scheme hinges on it. Any doubt that the certification auditors have followed proper procedures and audited strictly against the formal requirements could discredit the issued certificates and, by implication, all of ISO27k. Concerns about certification audits are an order of magnitude more serious than for internal audits, and two orders more than for internal management reviews/assessments.

If a client has a concern about a certification audit finding, recommendation, or auditor, they should first discuss it with the auditor concerned and/or the assignment manager. Most things can be addressed at this informal level, with reference to the relevant standards, procedures and audit evidence. [This happens fairly often in practice. Discussion and clarification of this nature is a normal part of any audit. Thankfully it is usually the end of the matter: although one or both parties may feel a little aggrieved, they normally reach a delicate agreement and move on.]

If the concern has not been resolved or cannot be taken further at the informal level (for example, the client believes the auditor is incompetent or misguided or plain wrong about something, but the auditor and/or the audit manager disagrees), they can complain formally to the audit company senior management about the situation and try to negotiate a mutually acceptable settlement. They should of course expect a robust response from the auditor and the company management (including the re-examination and re-presentation of the audit evidence and analysis), but if there is merit to the complaint, the company should have an internal process for dealing responsibly with it. It may be handled as a supplier-customer complaint, or as an audit issue, or a certification issue, or a legal issue (more below) or all of the above. [This is quite rare but I'm quite sure it happens. I believe partners in audit partnerships are jointly liable for their work, so they will take complaints seriously if they are raised to that level, but the potential conflict of interest is obvious.]

If that complaint process fails - for example if the response is still unsatisfactory to the client, or if they feel they have not been treated professionally - they can potentially complain to the accreditation body that accredits the certification company. To get anywhere, the client would need to provide sound evidence concerning the dispute, essentially having to prove that the certification company and/or its auditors are not worthy of being accredited. The accreditation body should have a formal procedure for dealing with such complaints. [I personally have never heard of such a case, but it's certainly possible.]

The client can also complain to the professional bodies that certify and represent individual auditors - for example ISACA for CISAs. Again, they are likely to get a robust response from the professional body who will probably have a standard process to review the complaint, assessing evidence from both sides before siding with the auditors, their members (!). It would take very strong, hard evidence of professional misconduct or incompetence to persuade them to find against their members, coupled with a highly professional ethics/professional standards committee. [I am aware of occasional complaints of this nature, but most probably never see the light of day. Vanishingly few cases go beyond a temporary suspension of the member concerned, but expulsion is their ultimate threat.]

At some point in this escalation, the dispute is likely to be handed to the lawyers, implying that they will look at the standards, contracts, policies, procedures and so forth with a strict legal eye, as well as assessing the evidence relating to the dispute. Any ambiguity in ISO/IEC 27001 that led to the dispute will be brought to the fore, with each side's auditors making their case. Ultimately, it may come down to the opinion of a judge in court. [It would be an extremely serious matter if a dispute ever got to this stage, clearly, since losing accreditation would be a huge commercial setback to an audit/certification company, as well as a knock to

the accreditation and auditor professional bodies (since it is implied that they should not have accredited/certified the auditors) and again to ISO27k as a whole.]

Implementation tip: auditors and auditees are mere mortals. We all have our 'off days' on which we make more than our normal number of mistakes and errors of judgment, but none of us likes to admit to being wrong. Handling disputes sensitively can make a huge difference, for example by focusing on the factual evidence rather than the personalities and subjective opinions or prejudices of those involved, and by avoiding highly emotive words such as "incompetent" (even though that might be perfectly accurate). If all else fails, clients can choose different certification companies, and certification companies do not have to bid for every single sales opportunity.

Q: "What do we need to do to prepare for a recertification audit?"

A: Unlike the six-monthly or annual external audits which tend to focus on specific areas, the re-certification audit will give the entire ISMS a thorough once-over. Since your ISMS has been in operation for some time (at least 3 years)(, the auditor will expect to see a mature ISMS that is nevertheless moving forward, proactively responding to the inevitable changes using the PDCA/continuous improvement processes embedded in the ISMS.

This is a formal audit and can be tough for organizations that have let their ISMS drift or decay after the elation of their initial certification. *Recertification is not a forgone conclusion!* The audit's prime focus will, of course, be to confirm strict compliance with the current version of ISO/IEC 27001. The key issue is that you still have an effective and compliant management system to manage your information security.

Use this simplified 8-point checklist as a basis for planning the main things you need to get done before the auditor turns up (you will probably need a more elaborate and comprehensive plan):

1. Check that your **ISMS internal and external audits** are fully up to date, with plans in place for future audits. Are all audit findings/observations, recommendations and agreed actions either completed and closed off, or currently in progress (with clear signs of that actually happening, in practice)? Use the results of recent audits to drive forward any necessary changes and to reinforce the concept that the audits are all about making justified improvements. (It is worth double-checking that any other similar audits covering information security risks, controls and compliance are also addressed.)

2. Collate evidence of continuing **management commitment to the ISMS** such as minutes of management committee meetings, decisions and actions taken, preventive and corrective action plans and the results of follow-up or close-out actions, and budgets.
3. Complete a full **management review** of the ISMS, including your Statement of Applicability and Risk Treatment Plan. Document all findings and recommendations as preventive or corrective actions and ensure all actions are suitably initiated, allocated and managed. Try to get all significant issues closed off, or at least well under way, before the audit.
4. Review your information security **risks**. If there have been significant changes in the external business environment (*e.g.* new legal or regulatory compliance obligations, new ISO27k standards, new security partners), internal situation (*e.g.* reorganizations) or IT (*e.g.* new platforms and application systems), redo your information security risk assessment from scratch using the documented methods, and update your RTP. All risks should be treated, in other words avoided, controlled, transferred or explicitly accepted by whoever is accountable and, for significant risks, there should also be contingency plans in place in case the treatments fail.
5. Review all **ISMS documentation** (policies, standards, guidelines, procedures *etc*.) to ensure it is up to date, complete, formally approved/mandated/signed off, version controlled and made available to those who need it (*e.g.* uploaded into the ISMS area on your intranet). Ruthlessly seek out and destroy old/outdated ISMS documentation.
6. Get your information security **awareness and training** activities right up to date and ensure a training plan is in place for future activities. Ensure everyone is aware of where to find the ISMS materials and is aware of the content (a useful tip is to give everyone a shortcut to the information security documentation on their desktops). Ensure everyone is familiar with, and in fact actively complies with their responsibilities towards information security, for example any obligations arising from privacy legislation and relevant information security procedures, and .
7. Check the documentation relating to any recent information security **incidents**, for instance to confirm that corrective/preventive actions were documented and duly completed. Step back from the detail to confirm that the *process* is operating smoothly.
8. Review your information security **metrics**. Given that your ISMS has matured, are they still relevant and useful or do they need adjusting? Have you in fact been reporting and measuring against them (collate recent

evidence to prove it) and have any actions necessary been taken (check the preventive and corrective action plans)?

Get yourself round each area of the business and grill likely audit interviewees (both managers and staff) regarding their part in the ISMS. Ask them some searching questions (try the auditors' favourite "Show me..." to check that they have the evidence substantiating what they claim) and try to find where the weaknesses are before the auditor finds them - not to hide them but to address them! This is invaluable preparation/training for the auditees. Tell them up front that you are not being harsh with them but are asking stiff questions to help them prepare and make the actual recertification audit go more smoothly.

Email employees shortly prior to the audit reminding them of their responsibilities towards both information security and the ISMS audit. Give them information and tips on how to conduct themselves during the audit ('be frank, be open, be honest and use the policies, procedures and other documentation to demonstrate what you do').

Implementation tip: remember that the ISMS is a living thing, constantly adapting to changing business needs arising from evolving information security risks. It will never be perfected or finished as such but, so long as it is properly managed, reviewed and fully supported by management and indeed other employees, you will be fine. Good luck!

-- End of FAQ --

If you have questions that you would like answered, please post a message on the ISO27k Forum. We reserve the right to reproduce common or generally useful questions and answers here for the benefit of all our visitors, although we will do so anonymously and in a generic manner.

We are neither infallible nor all-knowing so please bear with us if we take a while to respond, are sometimes a bit vague, and make mistakes. If you are experienced in this field and have better, more precise or more accurate answers to the questions noted above, by all means join and respond to queries on the ISO27k Forum or get in touch. Pragmatic implementation hints and tips from those of you who have been through the process are particularly welcome. We appreciate the help as there are inevitably practical limits to the amount of free consultancy advice we can offer!

Copyright and disclaimer