The ISO27k FAQ

Answers to **F**requently **A**sked **Q**uestions about the **ISO/IEC 27000-series information security standards**

This is a static PDF offline version as of December 2019.

The online version at www.ISO27001security.com
is updated from time to time, more often than this document.

This FAQ 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.

1. Basic questions relating to ISO27k

FAQ: "The titles of several ISO27k standards mention 'Information Technology -- Security Techniques'. Does this mean they are IT-specific?"

A: No, certainly not! The formal titles simply reflect the original name of the joint ISO + IEC committee that oversees their production, namely SC 27 "Information Technology -- Security Techniques", itself a subcommittee of JTC 1 "Information Technology".

ISO/IEC JTC 1/SC 27 adopted a new name in 2019: it is now "Information security, cybersecurity and privacy protection". The new name will gradually find its way into the standards as they are revised and published.

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:

> "The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, network and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards."

Generally speaking, an organization's most valuable information assets belong to business units, departments or functions other than IT Department. IT typically owns, manages and is accountable for protecting the shared IT infrastructure (*i.e.* the main corporate IT systems and networks providing shared IT services to the business) which is a substantial information asset in its own right. However, in information security terms IT typically acts as a *custodian* (but not *owner*) for most business data on the systems and networks, including content belonging to other parts of the organization or to suppliers, customers, business partners, sales prospects, stakeholders and other third parties.

This distinction has important implications. Information asset 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 Information Security and/or IT, they remain accountable and must ensure that information security is adequately funded, directed and supported to achieve the necessary level of protection. Likewise, Information Security and IT generally act as advisors and custodians with a duty to protect the information/data placed in their care, but they are not ultimately accountable for most information security incidents, breaches and impacts that occur as a result of unwise risk management decisions (such as under-funding security or accepting risks) made by the actual information asset owners.

Implementation tip: when assessing and treating information risks, focus primarily on critical business processes and valuable business information rather than the supporting IT systems and data. The modern approach to corporate governance means that naive or duplicitous business managers can no longer blame and cower behind IT if they make inappropriate decisions or fail to act in order to identify

and protect vital information assets. However, they often need help to appreciate and fulfil their security obligations.

FAQ: "Where can I obtain [*insert name of any ISO27k standard here*]?"

A: ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 and all the other published ISO27k standards may be purchased directly from the ISO store or from the various national standards bodies and commercial organizations. **Shop around for the best deal.**

It is worth checking for localized/national versions of the standards. Several national standards bodies release translated versions of the standards in their local languages. They go to great lengths to ensure that the translations remain true to the originals, although naturally this takes time.

ISO27k standards can be purchased as electronic documents or printed hardcopies. In addition to single-user PDFs, standards bodies may license electronic versions of the standards for multi-user internal corporate use - handy to make the definitive standards available on your intranet.

Implementation tip: Google!

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

A: The best reference sources on the ISO27k standards are the standards themselves - in other words, you should buy and read the standards (see above). 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 a certification auditor by taking an "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 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 others.
- 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 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 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 governance, risk and control concepts, and establishing your own expertise, experience, competence and hence credibility.

Implementation tip: don't forget to join the ISO27k Forum. If you are struggling with particular ISO27k-related issues, the archive of Forum messages well worth browsing or searching (it's a Google group so the search function works well), and members can always seek fresh answers to unique, current issues or challenges.

FAQ: "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 ISO27k-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 ISO27k-related designations are as follows.

ISO/IEC 27001 Lead Auditor (LA)

The term "**L**ead **A**uditor" 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 ISO27k/audit related training (for example modular courses comprising a day or two's training on ISO27k plus 3 days on auditing), then undertake further ISO27k 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 allegedly 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 ISO/IEC 27001, a number of IT training companies offer commercial ISO/IEC 27001 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 ISO/IEC 27001 LAs, do not rely on a candidate's claimed ISO/IEC 27001 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 7.1.1 (screening) for sage advice on this very point.

Note: ISO/IEC 27021 lays out the skills and competencies expected of professionals in this field. Training providers are hopefully aligning their public course curricula with the standard, hence the course-completion certificates will have more meaning and value.

Implementation tip: in our considered 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, general information security and IT audit qualifications such as CISSP, CISM and CISA, and general business management qualifications such as MBAs.

Advice for people who want to become IT auditors in our IT audit FAQ is useful for those planning to become lead auditors and is also relevant to becoming an information security management specialist since the fields are very closely related.

FAQ: "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."
- **CSA** (Cloud Security Alliance) is "the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud €"from providers and customers, to governments, entrepreneurs and the assurance industry€" and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem."
- **InfraGard.** "InfraGard is an 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 Forum is 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."
- **OWASP** (Open Web Application Security Project). "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 and deep 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.*

FAQ: "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 telecoms organizations and practices 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 sold and used internationally.

Implementation tip: we have tried to use "ISO/IEC" consistently throughout this site when referring to applicable standards, but we know it's a mouthful. In casual conversation, management reports, security awareness materials, social media *etc.* "ISO" is *good enough* for most purposes. Don't sweat the small stuff.

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

A: The acronyms indicate the progress of International Standards sequentially through the drafting and approval stages:

1. **PWI** = **P**reliminary **W**ork **I**tem - initial feasibility and outline scoping activities
2. **SP** = **S**tudy **P**eriod - preparing the NWIP
3. **NP** = **N**ew **P**roposal or **NWIP** **N**ew **W**ork **I**tem **P**roposal - the formal scoping phase, clarifying the proposal *
4. **WD** = **W**orking **D**raft (1st WD, 2nd WD *etc.*) - standard content development ("preparatory") phase

5. **CD** = **C**ommittee **D**raft (1st CD, 2nd CD *etc.*)- quality control phase, addressing editorial matters and typoos *
6. **FCD** = **F**inal **C**ommittee **D**raft - ready for final approval (voting) *
7. **DIS** = **D**raft **I**nternational **S**tandard - nearly there, hold your breath *
8. **FDIS** = **F**inal **D**raft/**D**istribution **I**nternational **S**tandard - just about ready to publish, pinch your nose and count to 100 *
9. **IS** = **I**nternational **S**tandard - published! Yay!
10. **TR** = **T**echnical **R**eport - published! See next Q&A.
11. **TS** = **T**echnical **S**pecification - published! See next Q&A.

* At several stages during the standards development process, national standards bodies that belong fully to ISO/IEC JTC 1/SC 27 are invited to vote formally on the standards and submit comments, particularly to explain why they disapprove of anything.

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. "Fast" is of course a relative term.

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

Lately the committee has taken to using **CRM** to mean not the obvious Customer Relationship Management, oh no, but **C**omment **R**esolution **M**eeting.

FAQ: "Aside from International Standards, what are TRs and PASs and ...?"

A: ISO/IEC publishes a range of different types of standards, as well as covering a number of different subjects:

- An **International Standard (IS)** is the most common form of ISO/IEC standard, including product/technical standards, test methods, 'codes of practice' (good practices) and management standards. An IS "provides rules, guidelines or characteristics for activities or for their results, aimed at the achievement of the optimum degree of order in a given context". Most aim to describe the final objective without prescribing the method of getting there (although they don't all meet that aim!). The review cycle is 5 years (maximum).

- A **Technical Specification (TS)** is a standard on an immature subject that is still being developed, and is not quite ready to become a full IS. Feedback is encouraged in order to drive further development and lead, eventually, to the release of an IS. Internally within the committee, final drafts are called **PDTS** Proposed Draft Technical Specifications.
- A **Technical Report (TR)** is informational in style rather than providing firm guidance. It may draw on surveys and 'informative reports', and may attempt to describe the 'state of the art'. Internally within the committee, final drafts are called **PDTR** Proposed Draft Technical Reports.
- A **Publicly Available Specification (PAS)** responds to an urgent need to drive consensus on some emerging topic. Alternative and perhaps incompatible views may be expressed by parallel PASs from different expert streams. A PAS is supposed to be replaced by a TS or IS, or withdrawn, within 6 years.
- An **International Workshop Agreement (IWA)** is essentially an alien PAS produced outside of the ISO/IEC world - for example by some technical or industry body. It too has a maximum life of 6 years.

FAQ: "What is meant by 'JTC 1/SC 27' 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 (that is, members of ISO, in other words national standards 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.

JTC 1'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 unfortunate fact that the ISO/IEC committee is IT specific means that the ISO27k information security standards are in fact labelled IT standards.

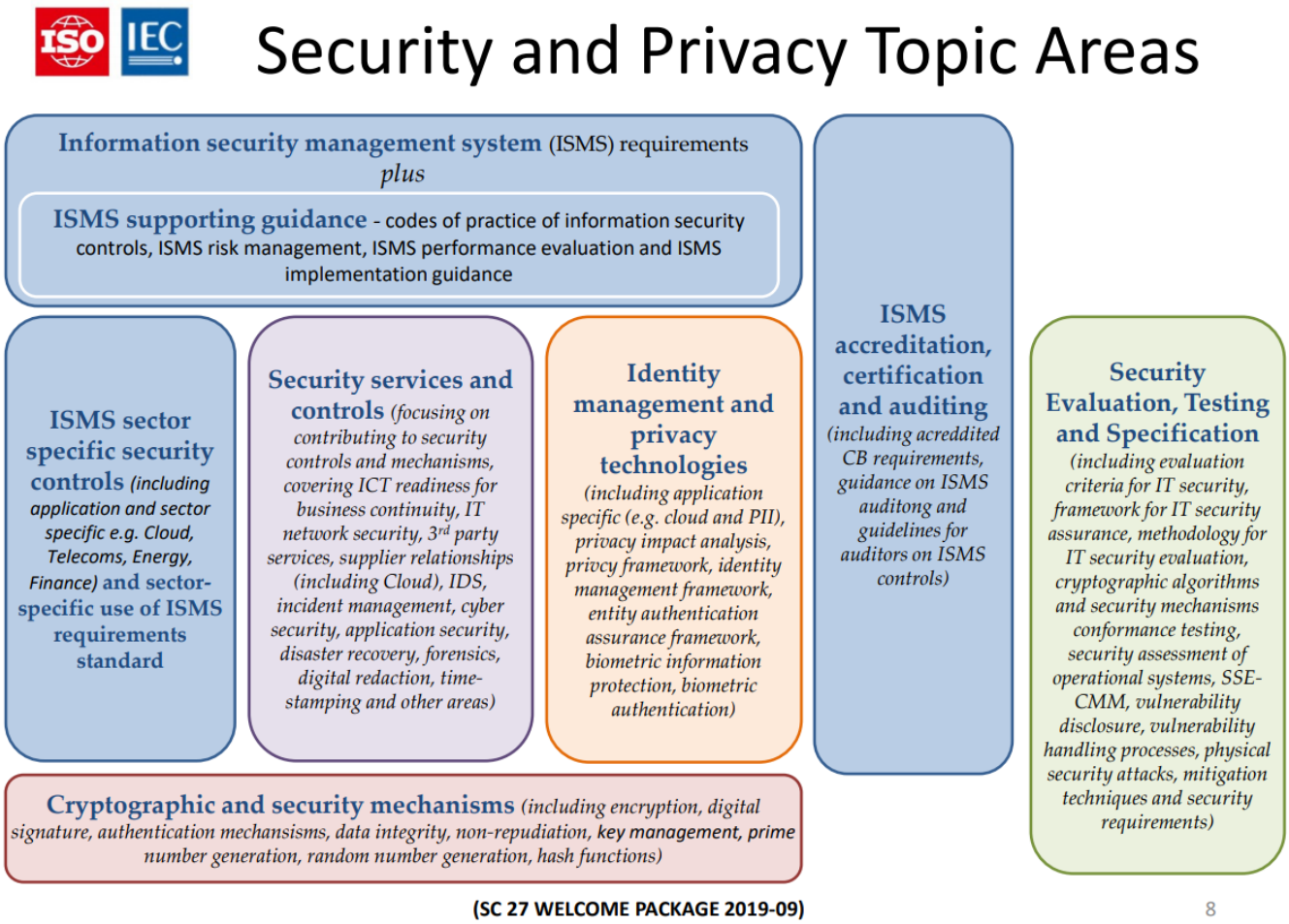
In ISO-speak, "SC" is a "Sub-Committee". **SC 27** is the main (but not the only!) ISO Sub-Committee responsible for numerous information security standards. SC 27 is a Sub-Committee of ISO/JTC 1. SC 27's "Standing Document 1" (SD1 - one of several) lays out its key processes in 50 pages of excruciating detail.

SC 27 owns and maintains *more than 200 standards* of which around a quarter are actively progressing at any one time. SC 27, in turn, has carved-up its workload across five **WGs** (Working Groups):

- **SC 27/WG1 - Information Security Management Systems**: responsible for developing and maintaining ISMS standards and guidelines, identifying requirements for future ISMS standards and

guidelines, maintaining the WG1 roadmap and liaising/collaborating with other organizations and committees in relation to ISMS;

- **SC 27/WG2 - Cryptography and Security Mechanisms**: cryptography, cryptographic algorithms, encryption, authentication, key management, digital signatures and all that;
- **SC 27/WG3 - Security Evaluation, Testing and Specification**: Common Criteria, evaluation methods, protection profiles, security capability maturity models *etc*.;
- **SC 27/WG4 - Security Controls and Services**: responsible for a variety of standards covering intrusion detection, IT network security, incident management, ICT disaster recovery, use of trusted third parties, business continuity, application security, cybersecurity and outsourcing. Some of these also fall into ISO27k;
- **SC 27/WG5 - Identity Management and Privacy Technologies**: does pretty much exactly 'what it says on the tin' (the title is self-explanatory). Includes biometrics.



Find out more about the inner workings of SC 27 in the welcome guide.

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 CFA (Committee For Acronyms) somewhere in ISO/IEC land!].

Aside from SC 27, various other subcommittees are working on security-related matters, such as:

- **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 privately owned and is NOT an official organ of ISO/IEC. Please read our disclaimer for more.

FAQ: "How can I keep up with developments in ISO27k?"

A: An easy way to keep in touch with developments is to join the ISO27k Forum. Don't forget to bookmark this website and call back every so often to check the news.

Another option is to Google ISO/IEC 27000 or related terms. Professional information security-related organizations such as ISSA and ISACA, and journals such as EDPACS, are increasingly discussing or publishing articles on ISO27k. There are a few ISO27k groups on Linkedin and other social media, of variable quality.

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

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

A: Contact your local national standards body (*e.g.* BSI, NIST, SNZ) 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 JTC 1/SC 27 representative/s to volunteer your services.

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: get involved in the drafting and review process!

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, a privilege to be able to collaborate with professional peers who are committed to ISO27k.

2. Get going on your ISO27k implementation

FAQ: "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 the design, development or implementation phases 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 or management-level metrics, such as maturity scores against the recommendations in ISO/IEC 27001 and 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 (including the ISMS Management Reviews formally required by ISO/IEC 27001 section 9), committees, teams or groups on security and risk-related matters (*e.g.* risk and business continuity 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/the business needs from information 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 or 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 or 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. Focus! It takes planning, preparation and prioritization to exploit the techniques that work best in your organization, and to spot and respond to the opportunities that *will* arise in due course as your ISMS is launched and gradually matures.

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

A: Yes. Next question?

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. Lining up a bunch of 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 may not be able to provide any proof. The value of the self-assertion depends largely on whether the organization is both competent at information security management and trustworthy.
- **Certification** *normally* (but not necessarily) 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 fulfils all the mandatory requirements of ISO/IEC 27001 in terms of its structure/design, *and* there is evidence that it is operating correctly. Nevertheless, *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 concern is to validate the *management system* not the *information security***. That said, there's a fighting chance that an ISMS which complies fully with ISO/IEC 27001 *is* in fact supported by a reasonably comprehensive and effective suite of information security controls, and that the organization is proactively managing and continually improving its information security arrangements.

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 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 already, the incremental cost of certification is relatively low whereas the benefits of independent assurance can be significant. Why would you *not* go the whole hog? If a third party claims but cannot demonstrate compliance (ideally by accredited certification), it begs the obvious question: why they don't have the certificate to prove it?

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

A: How many do you have? 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 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 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, privacy, 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 assurance 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 support from these 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 budgeted or committed levels. It's no good 'trying to make the time for this'.
11. **Scope** of the ISMS *e.g.* business units to be included, supplier relations included or excluded. Counter-intuitively, perhaps, scope is not a primary factor since a basic level of effort is always required to design and implement the management system, regardless of how widely it is applied throughout the organization. Scoping the ISMS too narrowly-scoped may actually create more work for the implementation team as well as unduly constraining its business value!
12. String length ☺

Implementation tip: check out the implementation project estimator - a simple spreadsheet tool provided in the ISO27k Toolkit. If it turns out to be wildly inaccurate, we would welcome your assistance to improve it for future users.

FAQ: "Is it necessary to appoint an Information Security Manager to implement and run an ISMS? If so, what qualifications should he/she possess?"

A: Yes, in practice an ISMS needs a nominated **I**nformation **S**ecurity **M**anager, **C**hief **I**nformation **S**ecurity **O**fficer 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 that a minimum of about 1% of an organization's total employees should work purely in information security (a greater proportion in any organization for which information is a vital corporate asset hence information security is a critical business issue). Small organizations may not have the luxury of a dedicated full-time ISM/CISO 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, or even managed service providers specializing in compliance, communications, collaboration and continuity) as necessary, both for the additional pairs of hands and more importantly their brains, expertise 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 certified compliant to ISO/IEC 27001)
- 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
- Good knowledge of, and ideally implementation experience with, the ISO27k standards
- Can competently and confidently explain the differences between threats, vulnerabilities and impacts, giving relevant examples

Nice to haves:

- Knowledge of COBIT, FISMA, 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 or consultancy experience with a variety of organizations, and the accumulated wisdom that often comes with a long grey beard

Implementation tip: good, competent, experienced information security professionals 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!

FAQ: "Should our CISO report to Quality, be part of the IT Operations department or report directly to the General Manager of the business unit?"

A: The question hints at a governance issue, maybe, or a naive misunderstanding. Generally speaking, the **C**hief **I**nformation **S**ecurity **O**fficer is, by definition, part of the C-suite comprised of all the CxOs - CEO, CIO, CTO, CFO, CRO, C3PO *etc*., in other words the most senior level of executive managers in the organization. The reason is that the organization *as a whole* is dependent on information, which therefore requires securing. The CISO's purview, then, extends across the entire organization, while the risks associated with information are such that information security is a strategic business matter, requiring senior management involvement.

"Quality" in the modern sense of quality assurance is also an issue that affects the entire organization and has strategic aspects ... but quality and information security are not closely aligned. Squeezing them into the same function suggests than neither is being taken seriously.

IT Operations is generally a function or team within the IT Department with an important role providing internal IT services, but that's only *part* of the information risk and security landscape. What about knowledge management, intellectual property protection, trade secrets, privacy compliance, business continuity, physical security for information, commercial cloud services and other concerns? This smacks of today's myopic focus on "cybersecurity", meaning security for IT systems, networks and computer data: those are indeed an important *part* of the risk and security portfolio, but not all. *Ignore the rest at your peril.*

The business unit GM *may* be the most senior executive manager in that part of the organization, or a non-specialist manager, or even a nondescript middle manager depending on how the role is defined. The fact that the questioner referred to the *business unit* GM implies that there may be other GMs in other business units (or divisions, sites *etc.*), and probably a senior executive management team for the entire organization or group ... which would be the ideal place for the CISO's strategic perspective across the whole lot.

Organizational structures and reporting lines, plus the objectives for all senior positions, are a matter for senior management, especially in such a critical area as information risk and security. This is part of corporate governance, a key responsibility and in fact accountability for senior management: if things ever go badly wrong (*e.g.* a serious compliance incident such as a privacy breach, or a business-threatening hack, ransomware infection, fraud or whatever), hard questions *will* be asked of senior management. A response along the lines of "We had no idea: this was delegated to some relatively junior part of the organization and we don't trouble ourselves with such trivia" is distinctly lame, unconvincing and unprofessional.

Implementation tip: work with everyone in the C-suite (particularly those in areas such as IT, risk, security, compliance and HR) first to help them understand the issues, and then come to an agreement on the role, objectives, seniority, reporting lines, alliances *etc. if* a CISO is the right approach for your organization. It makes little sense to work on any one aspect without also considering the rest in the corporate governance context.

FAQ: "When creating an ISMS, is it absolutely necessary to include members from non-IT parts of the business (business owners, finance, legal, HR, *etc.*)?"

A: The short answer is ***YES!***

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 telecoms 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 the 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: senior management should focus on identifying suitable information asset 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 asset 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 risk assessment. The responsibility for security cascades naturally through the organization but accountability sticks 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, or not. They also have the strategic vision and broad business/market knowledge to determine the value and hence amount of protection needed for business information.

FAQ: How do we define the scope of our ISMS?

A: First decide the boundaries (*i.e.* which parts of your organization are going to be subject to the ISMS and which parts if any are not) and applicability of the ISMS (*i.e.* what does the ISMS apply to and protect - usually 'information' or 'information assets'), then write it down. QED.

Scoping the ISMS is an important *business* decision, best made by senior managers who appreciate what the ISMS is all about and understand what it does for the business. Unfortunately, however, there's a chicken-and-egg situation here: before the ISMS is approved, designed and implemented, few senior managers are likely to have much of a clue about what the ISMS is, let alone how valuable it will be ... so it's a very good idea to put some time and effort into explaining things in a way that make

business sense. A good business case for the ISMS, for instance, will describe the approach in general terms, laying out the anticipated business benefits and the costs, and giving management various options.

Here's a bunch of questions typically of interest to management that you might like to consider if not explicitly address in the business case and associated chats, discussions, presentations, project plans *etc*.:

- Why do we need an ISMS? What will it do for us? How much will it cost? How long will it take to get going? Will it consume all our information security resources?
- We've managed without an ISMS until now: why the change? What prompted this proposal?
- Isn't this something that IT should be doing? What is the relevance to the rest of the organization? Why are you even asking *me* to get involved?
- Don't we have this already?
- What are our options? Do we HAVE to have an ISMS, for some reason, or is this a strategic matter? What approaches could we take? Why go down the ISO27k route instead of, say, NIST SP800-53 or PCI DSS or COBIT ... or just continuing as we are doing now?
- How deeply should we get into this? Can we scrape by with the bare minimum and still reap most of the benefits, or do we need to make a serious investment and go for broke? What else can we squeeze out of this opportunity?
- What do other departments, experts, advisors and influencers think about this? Who else is or should be involved? Are they all fully engaged with and supportive of the proposal, or might they be upset if this goes ahead? Can we cope with the changes of power and relationships that are likely to happen? Do the changes promise to be beneficial overall?
- Is this something our competitors are doing? Is there any competitive advantage in doing this? Is it more advantageous than all the other stuff we could be doing?
- What barriers are there or might there be, and what can/should we do about them?
- If we decide to go ahead, when is the best time to do it? What else will be affected? What are the risks associated with the implementation project?
- Who should run it? What kinds of skills and competencies do they need? Can we afford to divert them from other duties onto this? What about the rest of the team?
- How big should we go? Should we limit the ISMS to certain parts of the organization, whether just for now or for good? Are they parts of the organization that should not be included in the ISMS for various reasons (*e.g.* because they are too busy with other initiatives, struggling with other challenges, about to be outsourced ...)?

So you see that scoping is just one of many issues on the table.

Implementation tip: there's a lot to be said for making the actual formal scope statement very simple *e.g.*:

"The Information Security Management System (ISMS) protects information belonging to, or under the custody of, ACME Inc. of Texas, USA."

- or -

"ACME's Information Security Management System (ISMS) protects information located in or associated with ACME's offices in Roadrunner Gulch, TX, and Coyote Valley, NM."

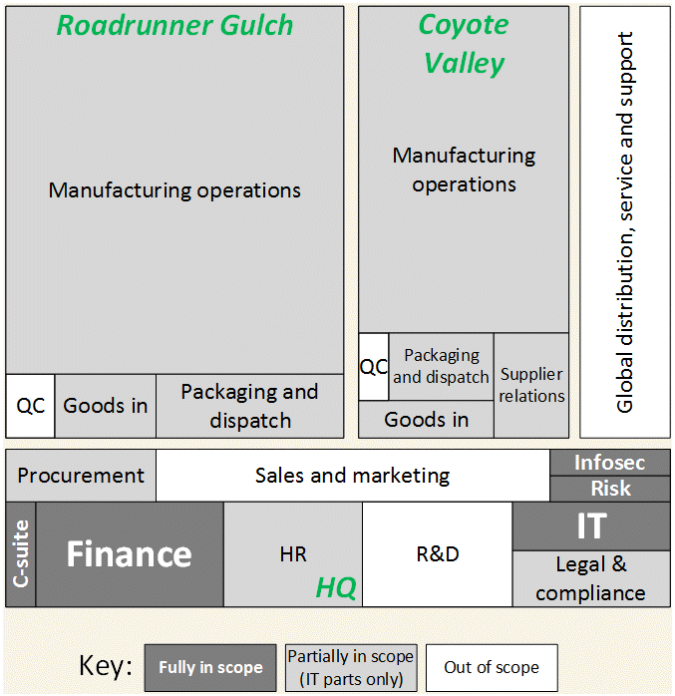
- or -

"The scope of ACME's Information Security Management System (ISMS) includes the Head Office in Roadrunner Gulch, TX, the Procurement Department in Coyote Valley, NM, and the IT function in Mumbai."

- or -

"The Information Security Management System (ISMS) protects information belonging to, or under the custody of, ACME Inc. of Texas, USA, except for the corporate locations overseas."

- or even:



[A scope diagram such as this qualifies as "documented information" and so fulfils the requirement in ISO/IEC 27001 section 4.3. It's OK to be creative.]

FAQ: "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 information risks that go beyond 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 the supplementary question implies.

There are several serious drawbacks to limited-scope ISMSs:

- Failure to gain the valuable business benefits of world-standard information security in the rest of the organization.
- Discontinuities in the way information risks are managed (analysed, treated, discussed …) across the organization.
- Failure to align information security and business strategies, missing out on the broader strategic, commercial, risk management, loss reduction, compliance, governance, management, continuous improvement and other advantages which accrue to an organization that has information security firmly under management control.
- Likely unmanaged information risks in the rest of the organization, and probably a distinct lack of understanding/appreciation of many of those risks if the processes of risk information security analysis, not just the ISMS, are restricted to the in-scope parts.
- Demonstrates a lack of full commitment to information security by senior management, obvious to anyone who actually bothers to look at the formal scope and SoA.
- Need to apply security controls at the perimeter of the ISMS, including some within the organization, since the rest of the world is "outside" the ISMS and hence to some extent untrusted.

The scope boundary can be a problem since, by definition from the ISMS perspective, everything outside the scope is inherently less trustworthy than that within. Information risks within scope of the ISMS will need to be assessed and treated, including risks affecting the information flowing into or out of the scoped area and information risks that are entirely external to it. The treatments that you select to deal with these boundary and external information 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;

- **Sharing** the risks through some form of insurance, agreed liabilities, contracts, SLAs *etc.*;
- **Avoiding** the risks [by not unduly 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 initial 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. It's not all bad.

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

FAQ: "Why do some organizations restrict the scope of their ISMS?"

A: There are *at least* 23 reasons to de-scope or constrain an ISMS to particular business units, departments, locations or whatever:

1. It's a pilot or a starting point, a way to gain experience, see how it works and set things up in preparation for a larger implementation "at some future point".
2. It's a pilot or a starting point, a way to gain experience, see how it works and set things up in preparation for a larger implementation that is actually planned as part of an documented and approved business/security strategy. (NB Reason 1 =/= Reason 2)
3. Markedly different information risks and hence information security requirements in various parts of the organization *e.g.* international businesses with conflicting legal and regulatory compliance obligations, or large organizations comprised of multiple, largely independent, companies/operating units.
4. Lack of time – there's an urgent need to "get certified" and a certificate is all that matters right now.
5. It's too risky to go for a full-scope implementation – "we might not pass the certification audit (because we only fully control the in-scope part)"
6. Political constraints *e.g.* if information security is seen by management as an IT matter, so it's IT's problem and IT can do what it likes so long as no one else is affected.

7. Skunk-works *i.e.* the in-scope area is implementing the ISMS secretly, under the radar of senior management in general, for various dubious reasons.
8. Stakeholder demands *e.g.* if The Minister or A Major Customer insists on certified ISO27k compliance, so 'all they need' is the parchment.
9. Stakeholder demands *e.g.* if The Minister or The Owner insists, for some external (and probably ill-advised or misguided) reason, that the scope be limited.
10. Genuine budget or resourcing constraints [for legitimate reasons, not just because of arbitrary decisions by management] meaning that a narrow-scope ISMS is all that can possibly be achieved, at the moment anyway.
11. The ISMS is needed to address a specific, narrow compliance obligation such as PCI DSS or privacy: nothing else really matters.
12. Myopia or blinkers - a fundamental lack of understanding and support from management (especially senior/powerful people) concerning the all-encompassing nature and wider value/benefits of *information* security, probably reflecting limited security awareness or perhaps bad experiences in the past.
13. Myopia - short-sightedness, narrow perspective, lack of ambition, inexperience, cluelessness and/or extreme naiveté by the information security professionals concerned.
14. The in-scope business unit/departments/whatever is a fully independent operating unity, just like a separate company.
15. To cut corners and give the appearance of being concerned about information security while spending the least amount possible to do so.
16. "Because everyone else does it that way" - follow-the-herd mentality.
17. Brains-in-neutral - it never even occurred to anyone that the ISMS might be applicable to, and benefit, the entire organization.
18. Because they were (wrongly?) advised to do so by some self-proclaimed expert, or possibly by an experienced consultant, professional advisor or auditor who seriously doubts the organization needs, or is capable of implementing, a full-scope ISMS.
19. Lack of genuine commitment to information security: the ISMS is just a fad, a nice line on someone's CV or marketing brochures.
20. Lack of foresight, vision and ambition, self-doubt, small balls.
21. Genuine management doubts about the value of the ISMS, reflecting misunderstandings and distrust in the motives of those promoting the ISMS.
22. Too many other commitments and initiatives (including other management systems?) – a change management overload and management/resourcing crisis.
23. Because the rest of the organization already has something better, or at least a different way of managing information security, that is deemed incompatible with ISO27k.

24. Others? People can be very creative in thinking up reasons *not* to implement an ISMS across the entire organization.

Some of these are genuine, legitimate reasons, valid for certain limited circumstances, but many are spurious.

Implementation tip: scoping the ISMS appropriately is an important strategic decision that should be made by senior managers, for example discussing, comparing and choosing between a set of scope options. Ideally, the options should lay out the costs and benefits over the entire lifecycle of the ISMS, several years at least, to enable their pros and cons to be assessed.

FAQ: "We need an inventory of our information assets. How do we do that?"

A: Errrr, are you sure? What makes you say that?

ISO/IEC 27001 does not formally *demand* that you have an information asset list, inventory, register or whatever: it is one of the discretionary/suggested controls listed in Annex A. Technically, since it is not strictly mandatory for certification *i.e.* specified in the main body of 27001, you could decide to break with convention and not bother with an information asset inventory at all but if so you had better be ready to explain and justify that curious decision to the certification auditors! It begs questions such as "If you don't even know what information assets you own or are responsible for, how can you be sure you have dealt with the associated risks?" In theory there are approaches and situations which don't necessarily involve inventories (or lists or registers or databases ….) but in practice I can't envisage any real-world situation where such an approach would be sensible.

'27001 Annex A links to ISO/IEC 27002 with further advice. '27002, in turn, refers to ISO/IEC 27005, which says:

> *"Asset identification should be performed at a suitable level of detail that provides sufficient information for the risk assessment. The level of detail used on the asset identification will influence the overall amount of information collected during the risk assessment. The level can be refined in further iterations of the risk assessment."*

By mentioning iterations, it is perhaps hinting at the idea of doing a high level assessment first, assessing broad categories or groups of information asset, then in successive cycles going into more detail as appropriate. You might, for instance:

- Conduct a high level risk assessment across all your known information assets, crudely lumped together for the first run
- Sort the information asset groups in order of the assessed risk levels
- Analyse information assets with the highest risks in more detail, perhaps breaking down the categories/groups to get more specific
- Systematically work your way down to the lower risk items until it's time to re-start the cycle (*e.g.* an annual information risk update)

Alternatively you could:

- Conduct a high level risk assessment across all your known information assets, crudely categorized or grouped for the first run
- Carve up the information assets into, say, 4 groups: critical, high, medium or low
- Draw up a schedule of risk analysis and treatment activities that addresses and reviews the critical risk items every quarter, the highs every third of a year, the mediums twice a year and the lows once a year
- Break down groups of information assets into smaller chunks as appropriate
- Review and update the risk categorization as relevant throughout the year during the work, and perhaps revisit it as a whole once a year to plan the following year's work

Alternatively:

- Start by specifying the risk levels *e.g.* high, medium and low, with defined criteria [get your buckets ready]
- Search out your information assets, briefly assess them and assign them to the corresponding risk level [chuck things in the buckets]
- Take a closer look at those in the medium level, and a much closer look at the highs, leaving the lows to fend for themselves [rummage through the buckets]
- Once a year revisit the risk level criteria, review the classified items for any anomalies, and decide the approach, resources *etc.* for the following year [perhaps kick the bucket!]

Otherwise:

- Adopt or adapt basically the same approach used currently elsewhere in the organization to identify, assess/analyse and treat other kinds of risks (*e.g.* financial, strategic, market, compliance and/or health and safety risks), with adjustments as appropriate to suit the particular needs and context of information risk.

This is not a definitive or comprehensive list of options. You might prefer variants on or combinations of the above, or the Monty Python option ("And now for something completely different").

Bear in mind that, under ISO27k, you have a lot of latitude to go with the approach that suits your specific organization. You can design it and put it into effect, along the way generating records/documents/evidence/collateral with which the certification auditors can confirm that you have:

1. Determined a sensible approach that makes sense in your situation;
2. Followed the approach as intended - you've done what you set out to do; and
3. Governed and managed the entire process/approach sensibly, systematically making fine adjustments or more substantial changes if appropriate to improve the process in the light of experience (*e.g.* risks that turned out to be more serious or more frequent than expected, plus incidents that 'came out of nowhere' implying failures or weaknesses in your information risk management activities) and perhaps other changes going on in parallel (*e.g.* a corporate strategy to be bolder and push harder when economic conditions look promising, and to retrench and be more

careful when things look bleak; or pressure from the authorities or stakeholders to be more careful in respect of certain types of information risk, asset, incident or control).

Implementation tip: as to how to do actually it, the key is to categorize or group similar information assets together. By 'similar', we are really getting at the information risks associated with the information assets *i.e.* the threats, vulnerabilities and business impacts, rather than criteria used to group them in other contexts (*e.g.* by platform/vendor, type, value, age, location, asset code or whatever).

For a kick start, you may find that IT, Finance, Procurement, HR or other functions already maintain lists, databases or inventories of various information assets for their own purposes such as:

- Managing and maintaining software versions, updates, patches and perhaps licenses;
- Providing software, hardware or user support;
- Doing backups;
- Configuration management;
- Network address management;
- Intellectual property management;
- Accounting and auditing;
- Relationship or vendor management;
- Training; or
- For insurance purposes.

Be very careful, though, or you could easily find yourself taking on a massive burden to consolidate, rationalize, verify, update, maintain and manage disparate information inventories for the entire enterprise! Ultimately that may well be the most sensible strategic approach but don't lose sight of your tactical, near-term goal to get an ISMS up and running. It may pay to grab useful information from other functions without (at this stage) promising to give them anything in return!

FAQ: "What/how much detail should our information asset inventory include?"

A: A *reasonably* comprehensive inventory of your information assets would be useful for purposes such as:

- **Avoiding gaps and overlaps** - such as classes or items of information that *everybody* presumes are *someone else's* concern, or conversely those sexy ones where everybody wants a piece of the action;
- **Risk assessment and treatment** - making sure that all information assets have been duly assessed and treated;
- **Ownership and accountability** - clarifying exactly who is accountable for protecting valuable assets, and being certain that they know it;
- **Prioritization** - within reason, it makes sense to put more effort into protecting the most valuable and vulnerable information assets, than the relatively low-value and more robust ones. Generally

speaking, it also helps to tackle the biggest information risks early-on, not least because the information security program will start on a high if it makes real inroads into the organization's total risk profile and knocks back the things that keep management and other stakeholders awake at night;

- **Asset management and exploitation** - for organizations that revolve around intellectual property, the total value of information assets can far exceed the value of all other corporate assets combined, so of course information needs to be carefully managed. There may be accounting and other business or strategic reasons also, such as valuing the organization for mergers and acquisitions, or to negotiate better rates with the banks and other lenders;
- **Staying on top of significant changes** - for instance recognizing when new classes or types of information asset come into being, or when values or risks change markedly as a result of business activities or substantive changes in the organization's situation.

Building, maintaining, using and managing the information asset inventory is one of the capabilities a mature ISMS is likely to incorporate, but it may pay to start at a simpler, more basic level and let things gradually develop and mature from there over, say, a year or so.

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 - or more broadly information process-related assets including business relationships with service providers such as your web site hosting providers.
- Human information assets ("people are our greatest assets" is literally true if you take due account of their abilities, skills, expertise and the wealth of unwritten knowledge and understanding known as experience and wisdom).

[That classification is based on a list originally submitted to the ISO27k Forum. **A much more comprehensive version of this list is available in the 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: whereas you or your colleagues might have in mind the idea of compiling and maintaining an inventory *all* your information assets, that's a costly and probably futile approach. Luckily, it's not strictly necessary. A list of the most significant/valuable information assets is probably good enough to get you started.

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

A: The previous Q&A addressed a very similar point. In practice, it's probably too much work to risk-analyse everything in depth so consider instead a two-phase process:

1. A broad but shallow/high-level risk assessment to categorize your most valuable information assets and distinguish those that deserve more in-depth risk analysis from those that will be adequately 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 elsewhere in the FAQ.

Implementation tip: 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) by remembering 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.

FAQ: "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 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 favourite authority figure here].
10. No because it is “optional” and/or was not explicitly listed in black and white as absolutely mandatory by [insert favourite 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 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!

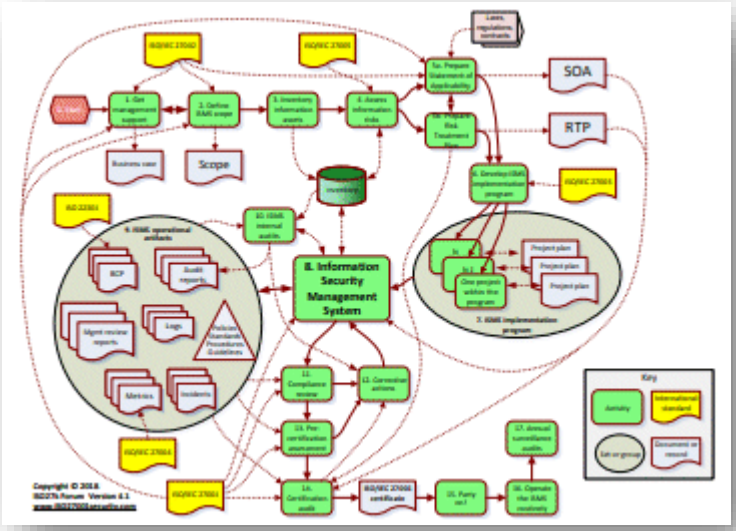
The basic rationale, from an audit point of view, is that yes, management can decide not to apply any of the recommended information security controls in Annex A of 27001 or the whole of 27002 that most other organizations consider essential *provided* they can justify that decision on a rational basis. 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.

FAQ: "I'm struggling to make sense of and apply ISO 27002's generic security recommendations to my organization. Any guide or advice?"

A: There is no definitive answer for your question: 'it all depends' is the classic consulting response. The process diagram ► 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 the time you spend 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.

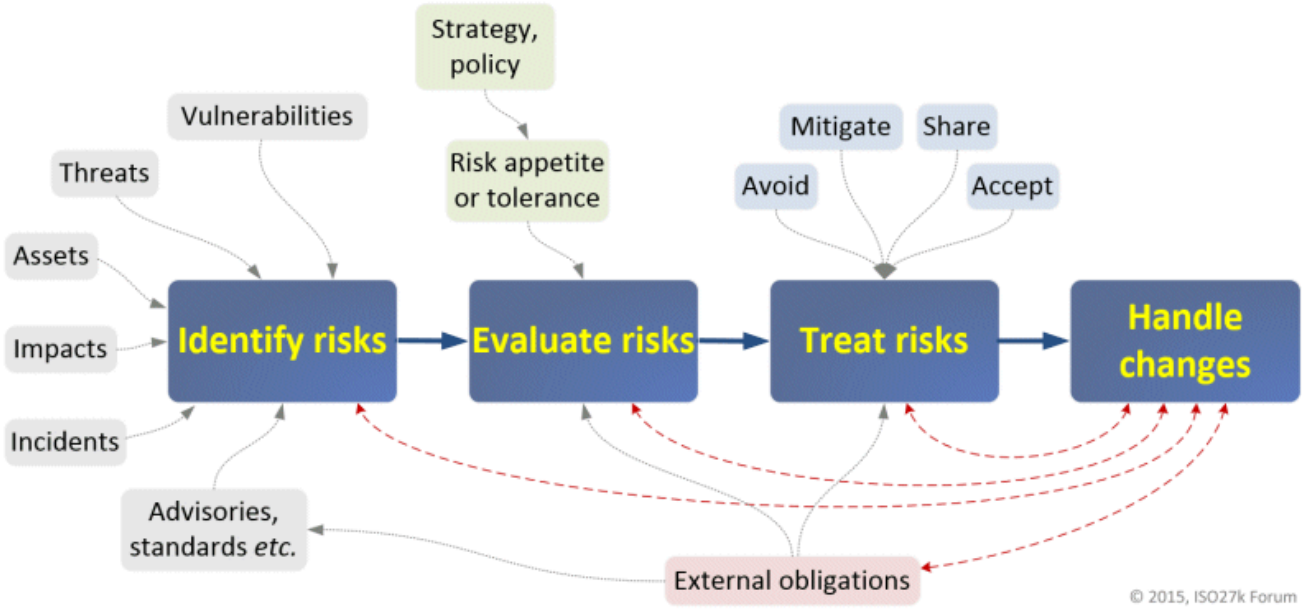
3. Information risk management

FAQ: What is Information Risk Management?

A: I'm not being facetious when I say that IRM is the *management* of *risks* to *information:*

- *Management* implies someone proactively identifying, assessing, evaluating and dealing with risks on an ongoing basis, along with related governance aspects such as direction, control, authorization and resourcing of the process;
- *Risks*, in this context, are the possibilities of harm;
- *Information* is the valuable meaning or knowledge that we derive from data, in other words the content of computer files, paperwork, conversations, expertise, intellectual property and so forth.

The process diagram sums it up:



The first stage of the process is to *Identify* potential information risks. Several factors or information sources feed-in to the *Identify* step, including:

- *Vulnerabilities* are the inherent weaknesses within our facilities, technologies, processes (including information risk management itself!), people and relationships, some of which are not even recognized as such;
- Threats are the actors (insiders and outsiders) and natural events that might cause incidents if they acted on vulnerabilities causing impacts;
- Assets are, specifically, information assets, in particular valuable information content but also, to a lesser extent, the storage vessels, computer hardware *etc.* many of which are relatively cheap commodities these days;
- Impacts are the harmful effects or consequences of incidents and calamities affecting assets, damaging the organization and its business interests, and often third parties;

- Incidents range in scale from minor, trivial or inconsequential events up to calamities, disasters and outright catastrophes;
- Advisories, standards *etc.* refers to relevant warnings and advice put out by myriad organizations such as CERT, the FBI, ISO/IEC, journalists, technology vendors plus information risk and security professionals (our social network).

The *Evaluate risks* stage involves considering/assessing all that information in order to determine the significance of various risks, which in turn drives priorities for the next stage. The organization's appetite or tolerance for risks is a major concern here, reflecting corporate strategies and policies as well as broader cultural drivers and personal attitudes of the people engaged in risk management activities.

Treat risks means avoiding, mitigating, sharing and/or accepting them. This stage involves both deciding what to do, and doing it (implementing the risk treatment decisions).

Handle changes might seem obvious but it is called out on the diagram due to its importance. Information risks are constantly in flux, partly as a result of the risk treatments, partly due to various other factors both within and without the organization.

Down at the bottom of the diagram, we've acknowledged that the organization often has to respond to *External obligations* such as compliance and market pressures or expectations.

FAQ: "We are just starting our ISO27k program. Which information 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 maturity in risk analysis and information security management, its size and complexity, industry, ISMS status and so forth. While ISO/IEC 27005 offers general advice on choosing and using information 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 risk analysis methods and tools exist (see the list below for starters), 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.

By the way, it is perfectly acceptable, advised even, for an organization to use multiple 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 aspects of concern, and then to change to other more detailed in-depth methods to examine those particular aspects more fully. Furthermore, some risk analysis methods are favoured by the experts in functions such as audit, risk management, health and safety, penetration testing, application design and testing, and business continuity management: there is no real benefit in forcing them to abandon their favourite methods and tools just to conform

to ISO27k. In fact, the differing perspectives, experience and insight these methods, tools and experts bring could prove very valuable (*e.g.* health and safety people assess "hazards" using methods remarkably similar to ours, while safety-critical is conceptually the same as business-critical).

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 risk analysis and 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. **Analog Risk Assessment (ARA)** is a deceptively simple method to analyse, report, compare and consider risks subjectively according to the relative probabilities of occurrence and impacts;
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. **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;
4. **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;
5. **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 risks with no less chance of success than the other methods shown here;
6. **DIY** (Do It Yourself) methods - see below;
7. **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;

8. 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** back in 2002. It encompasses all forms of organizational risk, not just information risk, using terms defined in ISO Guide 73;

9. **ISO 31000** 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*.;

10. **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;

11. **Mehari** is a free open-source (Creative Commons) risk analysis and management method in several European languages developed by CLUSIF (**Clu**b de la **S**écurité de l'**I**nformation **F**rançais) and CLUSIQ. It has adopted terminology and concepts from ISO/IEC 27005 and provides a spreadsheet tool;

12. **NIST SP 800-30** "Risk Management Guide for Information Technology Systems" is a free PDF download from NIST. An accompanying guideline is also available and also free;

13. **NIST SP 800-39** "Managing Risk from Information Systems - An Organizational Perspective" is another freebie from NIST, paid-for by U.S. tax-payers;

14. **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 ever), a quick version of OCTAVE;

15. **Risk IT** from IT Governance Institute/ISACA is similar in style to COBIT and Val IT but focuses on risk;

16. **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 risks;

17. **Verinice** is a free open source tool supporting the BSI IT-Grundschutz standards. It's very nice.

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

By the way, **DIY** (**D**o-**I**t-**Y**ourself) 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 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 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 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 analyse 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 useful goodies.

FAQ: "How do we *choose* a risk analysis tool or method?"

A: Read ISO/IEC 27005 for starters! If that is not enough, try the following tried-and-trusted almost universal spreadsheet-based method to evaluate your options and choose the tools, methods, software, cars, partners, holiday destinations, political parties, employers, employees, careers, lifestyles, widgets ...

First shortlist and look over the available methods and tools, thinking carefully about your requirements. What do you expect the method or tool to achieve for you? Which factors and/or features are most important? Are there any things that you would want your chosen method or tool *not* to do (*e.g.* gobble up excessive 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 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 risks" or risks in a broader sense, and what do you really mean by "information risks" anyway: are you in fact concerned about risks to information assets, or business risks that happen to involve information, or something else? Furthermore, 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);
- **Scalability**: 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 analyse 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 (such as members of the ISO27k Forum) 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 hardly satisfies this criterion;

2 = "OK": tool/method barely satisfies this criterion;

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

4 = "outstanding": tool/method exceeds our 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 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, it is generally worth adopting the same or a similar approach at least at the start. Your colleagues are likely to be more comfortable with what they know, and hence it should be easier to get them to focus on the analysis rather than the method being used. Within reason you can also pick out useful parts of methods or processes piecemeal, rather than necessarily adopting the entire set. Remember, risk analysis is a tool, a step on the way not a destination in itself.

FAQ: "Is it OK to determine and multiply threat, vulnerability and impact ratings to calculate our information risks?"

A: Although commonplace, such an approach is technically incorrect if, as is usually the way, your threat, vulnerability and impact ratings are of the form 1 = low, 2 = medium, and 3 = high. Using more categories and ratings, or adding instead of multiplying the values doesn't help. The point is that conventional arithmetic does not work correctly with such numbers.

Numeric values such as 1, 2 and 3 indicating counts or quantities of the instances of something are called **cardinal numbers**. The second value (2) indicates exactly twice the amount indicated by the first (1), while the third value (3) indicates exactly three times the first amount. Conventional arithmetic is applicable to cardinals.

Alternatively, numbers such as 1, 2 and 3 can indicate positions within a defined, ordered set of values, for example 1st, 2nd and 3rd places in a running race. These **ordinal numbers** tell us nothing about how fast the winner was going, nor how much faster she was than the runners-up: the winner might have led by a lap, or it could have been a photo-finish. It would be wrong to claim that the 3rd placed entrant was 'three times as slow as the 1st' *unless* you had additional information about their speeds, measured using cardinal values and units of measure: by themselves, their podium positions don't tell you this. Some would have it that being 1st is all that really matters anyway: the rest are all losers! Conventional arithmetic doesn't apply to ordinals such as threat, vulnerability or impact values of 1, 2 or 3 (or 0,1,2,3,4,5 or whatever you happen to use).

Alternatively, 1, 2 and 3 might simply have been the numbers pinned on the runners' shorts by the race organizers. It is entirely possible that runner number 3 finished first, while runners 1 and 2 crossed the line together. The fourth entrant might have hurt her knee and dropped out of the race before the start, leaving the fourth runner as number 5! In this case, these are **nominal numbers**, labels that just happen to be numeric. Phone numbers and post codes are further examples. Again, it makes no sense to multiply or subtract phone numbers or post codes because they do not indicate quantities like cardinal values do. If you treat a phone number as if it were a cardinal value and divide it by 7, all you achieved was a bit of mental exercise: the result is pointless. If you ring that number 7 times, you still will not be connected! Standard arithmetic makes no sense at all with nominals.

When we convert ordinal values such as low, medium and high, or green, amber and red, risks into numbers, they remain ordinal values, not cardinals, hence conventional arithmetic is inappropriate. If you convert back from ordinal numbers to words, does it make any sense to try to multiply something by "medium", or add "two reds"? Two green risks (two 1's) are not necessarily equivalent to one amber

risk (a 2). In fact, it could be argued that the risk scale is non-linear, hence extreme risks are *materially* more worrisome than most mid-range risks, which are of not much more concern than low risks. Luckily for us, real extremes tend to be quite rare!

Financial risk analysis methods (such as SLE/ALE, NPV or DCF) attempt to predict and quantify both the probabilities and outcomes of incidents as cardinal values, hence standard arithmetic applies but don't forget that prediction is difficult, especially about the future (said Neils Bohr, shortly before losing his shirt on the football pools). If you honestly believe your hacking risk is precisely 4.83 times your malware risk, you are sadly deluded, placing undue reliance on the numbers and predictions.

Implementation tip: risk values calculated from numbered categories tell us only about the relative positions of the risks in the set of values, not how close or distant they are ... but to be fair that is usually sufficient for prioritization and focus. Personally, a **R**ed-**A**mber-**G**reen spectrum tells me all I need to know, with sufficient precision to make meaningful management decisions in relation to treating the risks.

Note: *attentive readers may have spotted that the method described above for evaluating risk management tools inappropriately applies simple arithmetic to category labels. Suck it up! It works! Do as I say* and *as I do!*

FAQ: "We have taken over operations for a data center which belongs to and was previously operated by our client. We have expanded our information asset inventory to include not just our own assets but also the data centre assets belonging to our client. How should we handle risk-assessing our client's information assets?

A: Ideally, work with your client relationship people to involve the client directly in the risk analysis. Helping your client's management to understand and elaborate the information risks relating to their assets will clarify what they expect of your organization in respect of information security services, and will ensure that your colleagues appreciate what is expected of them.

If the client is unwilling or unable to engage fully with the risk analysis, you should at least assess the information risks relating to the contract and services from your organization's perspective, including the risk that the client may have unrealistic or inappropriate expectations about the information security services you are providing for them.

For example, you presumably take regular backups purely for your own operational reasons, routinely backing up the operating system and application software, configuration details, disk structures *etc*. However, the client may mistakenly believe that you are also backing up all their vital business data, even if they have never formally specified this as part of the contract or Service Level Agreement with your organization ... you can probably see where this is headed. Imagine the fallout if something goes terribly wrong one day, for instance a disk fails or is accidentally overwritten. You should be able to replace the disk and restore the directory structure, but you may not be able to recover the client's data. Maybe you have a full-disk image backup, but it is several days or weeks old whereas the client thought you were doing real-time disk mirroring!

You are probably well advised to consider your client's information risks anyway, even if they don't want to know. A serious information security incident involving the data centre will almost certainly damage your customer relations, could lead to legal arguments over the contract/SLA and in the worst case could put the client out of business.

Note that similar considerations apply in other circumstances where the organization handles information assets belonging to third parties - customers' personal data and credit card details, for instance. You may need to analyse and treat their risks on their behalf even if they are incapable or can't be bothered to do so, since you just *know* they will try to take you to the cleaners if some disaster harms their precious information. They may claim that you have failed in an 'implied duty of care', a term so vague and ambiguous that the lawyers will have a field day.

Implementation tip: this may be an opportunity to sell your client some security/risk consultancy services! Either way, have your pet lawyer take a *very* careful look at any contracts or SLAs relating to third party information assets in your care to be crystal clear about your information security obligations and liabilities.

FAQ: "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.

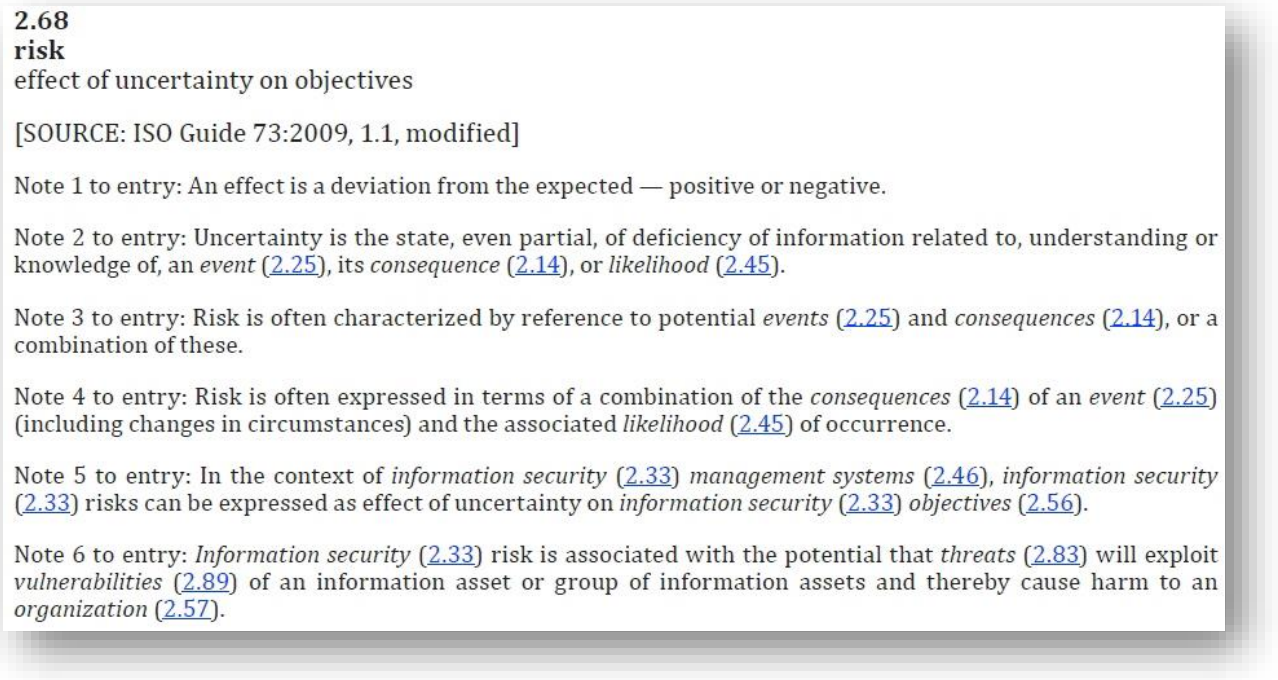
The risk assessment process is potentially auditable, by the way, while auditors are also concerned about audit risks (for example the possibility that their sampling and checking may fail to identify or highlight something truly significant, such as a rogue trader).

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.

FAQ: "Is threat assessment, threat modelling, threat analysis, vulnerability assessment, vulnerability modelling, penetration testing, business impact analysis, threat-vulnerability analysis, IT auditing ... or whatever ... the same as risk analysis, risk modelling, risk assessment ... or whatever ...?

A: Yes and no. Strictly speaking, these are all different, or rather they should all be interpreted differently but, in practice, there is much variation in the way the terms are used. In your particular organization, situation, classroom or what-have-you, one or more of these terms may well be in common use, meaning something more or less specific. The terms may even be formally defined in some manner, for example in the organization's risk or security policies, procedures and standards, in laws and regulations, in contracts *etc.* That's all very well but the people using the terms are not all experts in this field, and to be fair even the experts sometimes disagree, with good reason.

Consider the meaning of *risk* for example. As far as I personally am concerned, *risk* means either (1) the combination or coincidence of one or more threats acting on one or more vulnerabilities to cause one or more impacts on something (*i.e.* normally the organization, but sometimes risk relates to an individual business unit, system, person, location, information or other asset *etc*., or to several); or (2) an estimate of the probability and impact of some event, incident, situation *etc.* ISO/IEC 27000 has versions of those two definitions, plus several others:



2.68
risk
effect of uncertainty on objectives

[SOURCE: ISO Guide 73:2009, 1.1, modified]

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an *event* (2.25), its *consequence* (2.14), or *likelihood* (2.45).

Note 3 to entry: Risk is often characterized by reference to potential *events* (2.25) and *consequences* (2.14), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the *consequences* (2.14) of an *event* (2.25) (including changes in circumstances) and the associated *likelihood* (2.45) of occurrence.

Note 5 to entry: In the context of *information security* (2.33) *management systems* (2.46), *information security* (2.33) risks can be expressed as effect of uncertainty on *information security* (2.33) *objectives* (2.56).

Note 6 to entry: *Information security* (2.33) risk is associated with the potential that *threats* (2.83) will exploit *vulnerabilities* (2.89) of an information asset or group of information assets and thereby cause harm to an *organization* (2.57).

"Effect of uncertainty on objectives" is the official - but perhaps not the clearest and most helpful - definition for the ISO27k standards, hence all those explanatory notes. It is very generic.

Anyway, moving swiftly on, threat modelling, analysis or assessment normally explores the range of threats that are of some concern to the organization, identifying, evaluating and sizing them, assessing their capabilities, resourcing, motivation, objectives *etc.* The analytical process usually focuses on active/deliberate threats, although accidents, mistakes and natural disasters are at least as capable of causing harm. Similarly with external and internal threats, combinations of threats (*e.g.* looters following a flood) plus as-yet-unknown threats: a comprehensive threat model, picture or landscape will cover all possibilities.

Vulnerability assessment, often conducted in the technical sphere but actually a more broadly applicable method, is about finding and assessing the weak points (again in organizations, systems, locations, people, processes *etc*.) that might be exploited, assessing them also in terms of severity, exposure, nature, obviousness *etc*. Vulnerability assessment is at the heart of penetration testing, application system security testing *etc*.

Business impact analysis, often conducted in the context of business continuity management, is about working out the likelihood and scale of consequences to the organization and its business, business interests, business partners and other stakeholders if various incidents came to pass.

Bringing the results of those three analyses together is one way to assess, analyse or model risks – but often we just go directly to an assessment of credible risk scenarios based on the kinds of damaging incidents that have happened (to us or others). Auditors and risk professionals are good at this stuff, along with security/risk-aware managers *etc*.

Personally, I find the analog risk assessment method helpful, directly considering the probability and consequences of various kinds of incident to figure out which are the scariest. Some people prefer quantitative and "semi-quantitative" methods … and actually there is merit in using a combination of methods for a more comprehensive view of risk - which is pretty much what ISO/IEC 27005 advises.

Finally, I'll just briefly mention that there may be gross and/or subtle differences of meaning between terms such as 'analysis', 'assessment' and 'modelling'.

Implementation tip: if you find all these risk-related terms and methods confusing, join the club! They are very commonly misunderstood, misinterpreted and mistaken. Read and think carefully about the formal definitions in ISO/IEC 27000, and indeed in other standards and books, for a more accurate and complete picture. Be careful in how you express yourself on risk matters, and remember that other people may not share your particular understanding of the terms.

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

A: Apart from certain limited circumstances, most "real world" information 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 (which is what contingency planning is all about). 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 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.

FAQ: "Which compliance obligations are relevant to information security and ISO27k?"

A: There are *loads* of them! Although **I A**m **N**ot **A L**awyer, just to get your brainstorming started here's a simple but incomplete listing of the *general types or categories* of laws, regulations and contracts/agreements that have some relevance to information security and ISO27k:

- Banking & finance *e.g.* financial reporting, tax, credit, money laundering, company accounts, credit cards (PCI DSS and more) …
- Business continuity, critical national infrastructure …
- Commercial contracts & agreements *e.g.* confidentiality agreements, digital signatures, product guarantees, advertisements/offers/promises, maintenance and support agreements, Internet/distance selling, invoices, PCI DSS again, plus other obligations with business partners, suppliers, customers, advisors, owners *etc.* …
- Corporate governance, obligations on its Officers, independent oversight/audits, company structure …
- Cryptography – standards, laws and regs *e.g.* restrictions on use & export of strong crypto
- Defamation, libel, slander ...
- Employment *e.g.* disciplinary process, pre-employment screening/background checks, contracts of employment, codes of conduct …
- Environmental *e.g.* monitoring for polluting discharges & limits
- Ethics, morals, cultural and religious aspects *e.g.* Sharia law
- Fraud, identity theft, misrepresentation, embezzlement …
- Freedom of information – enforced disclosure …
- Hacking, malware, denial of service, unauthorized access to information systems and networks …
- Health and safety *e.g.* safety-critical control systems, fire exits, building standards/codes, industrial control systems, working conditions, hazards …
- Insurance and risk *e.g.* terms & conditions, excesses, disclosure of relevant facts ...
- Intellectual property rights - copyright, trademarks, patents, DMCA, trade secrets …
- Military/governmental stuff: spying, official secrets & classification, terrorism, organized crime …
- Permits and licenses to operate (in some industries and markets) …
- Porn, paedophilia, discriminatory/offensive materials, threatening behaviour, coercion …

- Privacy, data protection, personally identifiable information …
- Technical standards and interoperability *e.g.* ISO27k (!), TCP/IP, WPA2, Windows compatibility, Java compliance ...
- Wiretapping, surveillance, CCTV, monitoring, investigation, forensics …
- Others ...

As if that list is not enough already, as well as domestic laws and regulations, you should also consider whether the laws, regs *etc.* in other countries might also be applicable.

Oh and by the way, we're on shifting sands: this is constantly evolving through changes to the legislation and 'case law'.

Aside from being familiar with all the obligations, someone needs to be on top of the associated policies/contracts/agreements/standards/codes, awareness/education/training, compliance assessments and enforcement aspects. For example, do you have the policies and procedures in place to deal with exceptions and exemptions? Do you need to check compliance and perhaps enforce your organization's obligations on third parties *e.g.* confidentiality agreements with suppliers or business partners?

Implementation tip: personally, I favour the approach of treating this as a risk management issue *i.e.* analyse and consider the potential threats (*e.g.* investigation or discovery), the vulnerabilities (*e.g.* various practical and economic constraints on the extent of your compliance), and the impacts (*e.g.* enforcement actions, penalties, bad publicity, increased oversight). The organization (plus the individuals within it) has choices, strategic options, to make about when and how it complies with its obligations, in other words how it treats the risks. Full compliance is not necessarily appropriate in every situation, potentially creating opportunities for commercial advantage (cutting corners to cut costs). Furthermore, "full compliance" is not always entirely possible, in the same way that "complete security" is an oxymoron. Security is asymptotic.

Warning: assuming you are an information security professional looking into this stuff, **be very wary of being expected or even perceived by your colleagues and especially management as an expert:** even qualified professional lawyers specialise within the field because it is too broad for anyone to be entirely competent across the whole lot. In an organizational context, the 'officers' of the corporation (normally senior management, execs and non-execs) are the primary owners of most of the compliance issues. They are the ones who are primarily **accountable** for the organization's compliance, or lack of it. Don't take on their mantle! By all means offer general advice and guidance but leave them with the compliance burden and, for your and their protection, *explicitly* recommend that they seek competent legal advice. Once again, for good measure, **IANAL and this is not legal advice.**

FAQ: "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. **Exemptions** are the way to formalize risk management decisions accepting identified information risks.

For example, imagine that an IT systems audit has identified 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. The preferred response is to bring the system into line with the policies. However that is not always possible. If instead the IAO's decision is to accept the risk, an **exemption** to the specific policy 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** by simple extension of their accountability for protecting their information assets.

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.

*** Note:** your organization may use different words for these two concepts, such as exceptions and waivers, or exemptions and waivers, or even exemptions and exceptions with their meanings reversed.

The specific terms don't particularly matter *provided* they are defined, the distinction is clearly understood *and* they are used consistently.

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!

FAQ: "Is there a comprehensive catalogue of information risks?"

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

- ISO/IEC 27005 Annex C is a basic starting point, a few examples of threats to set you thinking;
- IT Grundschutz Catalogue (the baseline IT protection manual) includes an *extensive* threat catalogue, exhausting if not exhaustive;
- ISO/IEC 27002 and several other ISO27k, NIST SP800 and other information security and privacy standards, laws and regulations are, in effect, incomplete information security control catalogues that at least mention threats and vulnerabilities;
- Mitre's **CVE** (**C**ommon **V**ulnerabilities and **E**xposures) is a useful, well-regarded catalog of cybersecurity (meaning primarily technical/IT system) vulnerabilities. Again, not *totally* comprehensive but close enough for government work.
- Mitre's **CAPEC** (**C**ommon **A**ttack **P**attern **E**numeration and **C**lassification) is a structured catalog of cybersecurity 'attacks' *i.e.* how some threat agents exploit some vulnerabilities.

Good information security textbooks are worth checking too, for example:

- Cem Kaner's Testing Computer Software has a lengthy, structured appendix listing common software errors, some of which create vulnerabilities;
- 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** (**S**poofing identity, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service and **E**levation of privilege) - again it's not comprehensive but a decent approach to figuring out your own.

Most information risk analysis and management support tools, systems, methods and advisories include examples if not lists of stuff to consider.

Finally, Google is your friend.

Implementation tip: those are all generic catalogues. They may be useful reminders of the general types of stuff worth considering 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, Health & Safety, IT, HR, Operations *etc.* to develop more specific lists of threats, vulnerabilities,

impacts and controls that are relevant to your particular context and business situation. Pore over your organization's incident records and past risk assessments for clues and inspiration. Publish your own catalogue/s on the corporate intranet to remind workers of the wide range of issues of concern to Information Security and the business, inviting your readers to contribute?

FAQ: "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 network hacks 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.

FAQ: "I'm confused about '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 are reduced but not eliminated, usually, and the controls may fail in action (*e.g.* antivirus software that does not recognize and block 100% of all malware, or that someone accidentally disables one day);
- **Eliminated risks** are *probably* no longer risks, but even then there remains the possibility that your risk analysis was mistaken (*e.g.* perhaps you only eliminated part of the risk, or perhaps the risk materially changed since you assessed and treated it), 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);
- **Shared 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). Remember that the manager/s who made the decision to transfer the risk are accountable for that decision if it all goes pear-shaped ...

... and in fact the same point about accountability applies to all decisions made by everyone. If a manager does not explicitly treat an identified risk, or arbitrarily accepts it without truly understanding it, they are in effect saying "I do not believe this risk is of concern": that is decision for which they can be held to account.

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**. Oh and **denied risk** is that which someone determines is simply incredible or so unlikely/remote that it is practically non-existent – like for instance the possibility of planes crashing into *both* of the World Trade Center twin towers.]

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 risks. There is a strong link here between risk, security, incident and business continuity management.

3. ISM documentation

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

A: I would suggest putting your ISMS documentation online, typically on the corporate intranet or a similar communal directory/shared area. There are several advantages to this approach:

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 policy changes for feedback, but make sure that area is easily identified as such *e.g.* with a different coloured page background and an explicit statement that these are drafts, not the current, live, versions of your policies.]

There are two 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 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 perfectly OK to have some fun too, using more creative security awareness materials such as quizzes, crosswords, seminar/workshops and prize draws. The idea is to

draw people in and engage them, provide useful, readable content, not scare them off forever with miles of impenetrable red tape.

Implementation tip: It definitely helps to have a consistent style/format for each type of material, and even better consistent elements on all of them to bind them into a coherent, professional suite. Do you have an ISMS logo, perhaps, with which to 'brand' the documentation and your other security awareness materials? Do you employ professional authors? Do they use templates and styles consistently?

FAQ: "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 or 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. Concentrate on their primary purpose, which is to document the links between information risks, control objectives and controls.

FAQ: "I would like 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 Risk Treatment Plan 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.

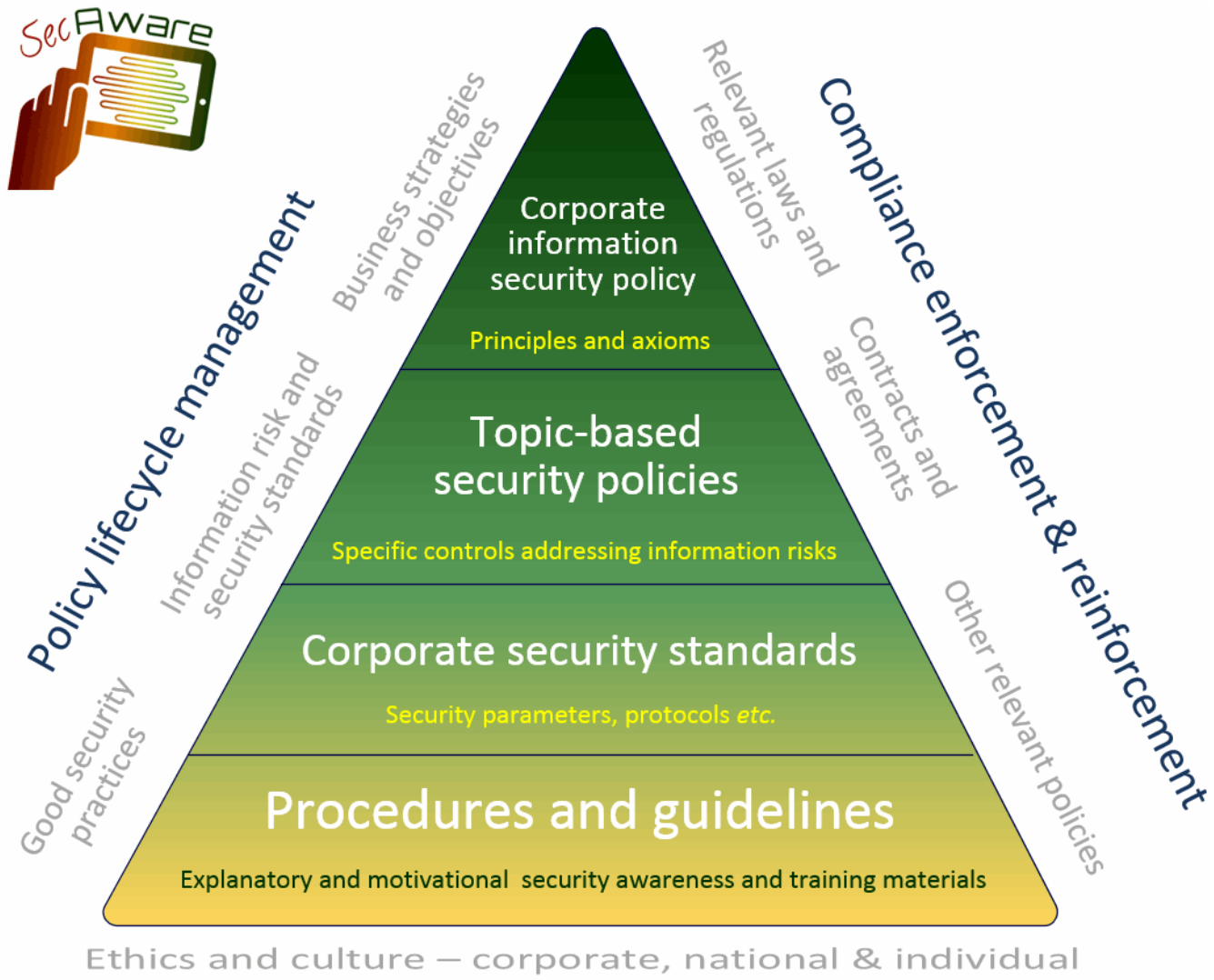
Implementation tip: You could set this up as a table or matrix, since many risks will require some combination of treatments and, in virtually all cases, "accept residual risk" is a necessary evil:

Risk	Treatment			
	Reduce	**Avoid**	**Accept**	**Transfer**
1. Name or describe an information 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				

FAQ: "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 ISO/IEC 27002 for a decent outline of what the policy should cover, as a minimum.

Although your approach may well differ, my *personal* preference is the pyramid structure shown below, the shape reflecting greater volumes and details in the lower levels.



The principles, axioms and policies should be formally reviewed and mandated by management, demonstrating their support for 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 C-suite: 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?).

Individual policies covering specific information security topics or issues such as "Email security policy" and "Network access control policy" tend to be quite formal but need not be stilted. They typically specify 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.

Corporate security standards expand on the high-level policies with technical details needed for their implementation.

Most organizations publish the entire policy suite on the corporate intranet because:

1. The online set *is* the definitive reference - no more wondering about whether printed policies are still current or have been superseded;
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.

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.

FAQ: Do we need an 'ISMS manual'

A: whereas an 'ISMS Manual' might have been appropriate under the previous version of the standard, it is no longer necessary.

In accordance with ISO/IEC 27001, '**Context of the Organization**' is a useful place in which to declare the scope of the ISMS and state related legal, regulatory and contractual requirements or obligations.

It is worth cataloguing and describing your ISMS documents in a Document Control section. As well as making it easier to keep the documents under control, to know what they are about and to reference them properly by name, the certification auditors will appreciate a neat list of the key ISMS documents that need to be controlled - and you will have a shopping list of the things the auditors are most likely to ask for. For bonus marks, identify the owners, revision status and date of next scheduled review.

Implementation tip: repeating or duplicating information in the ISMS remains a *bad* idea because it (a) makes the system bigger and more complex, and (b) increases the likelihood of document control non-conformities if the duplicates somehow become out-of-synch. It's much better to specify something (such as, say, a cloud computing security policy) once, definitively, and refer to it from elsewhere without repeating it. [Thanks to Dave Anders of SecuraStar for this Q&A.]

FAQ: "I am trying to put together a document for *working in secure areas*. 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!).

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 JTC 1/SC 27) 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 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 suite of policies, the *entire* edifice, right now. You can work on it piecemeal, one policy, standard, procedure or guideline at a time. 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.

5. ISMS Maturity

FAQ: "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. Be crystal clear about the business objectives for the CMS. 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.

FAQ: "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.

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

A: [Important *caveat*: **I A**m **N**ot **A L**awyer. This is not legal advice. I don't charge by the minute. I wear neither tailor-made suits nor wigs.]

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 and regulations concerning lawful/unlawful interception *etc*.
4. General **business laws** around company structure, taxation, governance (*e.g.* SOX), business records, HR, health & safety, building codes, fire escapes *etc*.
5. **Other 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, trademarks and trade secrets, 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, government & defence industry (freedom of information, official secrets, critical infrastructure, terrorism ...), medical & healthcare industry (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 (and processes information on) foreigners, uses overseas facilities or services, has an Internet presence *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, ISO/IEC 27002:2005 section 15 *could have* been interpreted to mean that it concerned 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 SC 27 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.

FAQ: "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 *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 influenceable 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.

FAQ: "What can the ISMS implementation project manager do to ensure success?"

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

- Become familiar with the business you serve. Get to know the department heads and the challenges they face. Try to see information 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 to make 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.

FAQ: "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? What metrics should we use?"

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

It is unrealistic to expect 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 risks, controls and metrics that matter to your particular organization.

Metrics-related references that you should check out include:

- ISO/IEC 27004 - the current version is well-written and useful, a big improvement over the initial release;
- PRAGMATIC Information Security Metrics by Krag Brotby and Gary Hinson - an eminently practical guide for security practitioners;
- IT Security Metrics by Lance Hayden - IT-specific, explains the **GQM** (**G**oal-**Q**uestion-**M**etric) approach;
- 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;
- NIST SP800-55 Performance Measurement Guide for Information Security - focused on measuring FISMA compliance but the principles are broadly applicable. It is 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 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!

Implementation tip: see SecurityMetametrics.com for an FAQ on security metrics and security maturity metrics designed to support ISO/IEC 27002. 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 management with the Answers, what are their Questions? Why are those Questions relevant - what business objectives or Goals are at stake? Work with management to figure *that* out and, believe me, the rest is a breeze. The **G**oal-**Q**uestion-**M**etric method eloquently described by Lance Hayden in IT Security Metrics is an excellent approach.

6. ISMS audit and certification

FAQ: "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. They may not appreciate your role in life, nor the value you can bring to the party. 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 (*e.g.* pure compliance auditing). 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 and 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!

FAQ: "I am an inexperienced 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 and ISO/IEC 27008 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 recommended resource.

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. Analyse 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 and 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 use mind-maps to help me think through the likely risks and anticipated controls, and to structure each audit job. Process diagrams, flowcharts, swim lane 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.

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

A: Auditors should 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 policies. 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 certificate.

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.

FAQ: "How can we ascertain 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 obviously suggest that the controls are less than perfect ... so one way to identify controls and objectives worth a close look is to rummage through your information security incident records and reports for evidence or hints about missing or ineffective controls. Make a special effort to tease out and re-evaluate longstanding issues. Don't be hoodwinked into ignoring issues that "have always been a problem" or "will never be solved": if they are in scope of the audit or review, they are almost certainly worth checking. An experienced, competent IT auditor's unjaundiced eye and techniques for assessing and reporting on such issues might just unblock the drains and help the organization achieve real progress.

Control 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 primarily a risk management or business decision for the 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.

FAQ: "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 (meaning fully compliant with ISO/IEC 27001) 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.

> Stephen Middleton proudly told us "We have today been recommended for certification after a 7-day stage 2 audit. We showed the external auditor our event log with both major and minor NC's raised by our internal audits and this gave us a big tick for managing non conformance as part of our ISMS."

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 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).

FAQ: "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 that has adopted ISO/IEC 27006, the certification 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 relevant information promptly if/when the auditor asks for it (be nice: 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, reduce stress *and* increase confidence in how you conduct your internal audits.

FAQ: "What are our options if we dispute the findings 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. ISO/IEC 27001 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 genuine concern about a certification audit finding, recommendation, or auditor, they should first discuss it with the auditor 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 "an understanding" - a delicate agreement or a truce at least - 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 audit 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 or 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 or certification company, as well as a knock to the accreditation and auditor professional bodies (since it is implied that they should not have accredited or 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 and explicit requirements in the standard rather than the personalities and subjective opinions, passions or prejudices of those involved. It's perfectly reasonable to ask "Show me" - and that goes equally for both auditees and auditors (*e.g.* if an auditor is asking you for or to do something that you do not believe is required by the standard). Avoid highly emotive words such as "incompetent" (even though that might be perfectly accurate!). If things are getting fraught, take a break to chill out. If all else fails, clients can choose different certification companies, and certification companies do not have to bid for every single sales opportunity ...

FAQ: "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 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).

Implementation tip: read the standards!

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

A: 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 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 - see ISO/IEC 27005.

Next you need to plan and conduct some form of information 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 and 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 or 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 or 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.

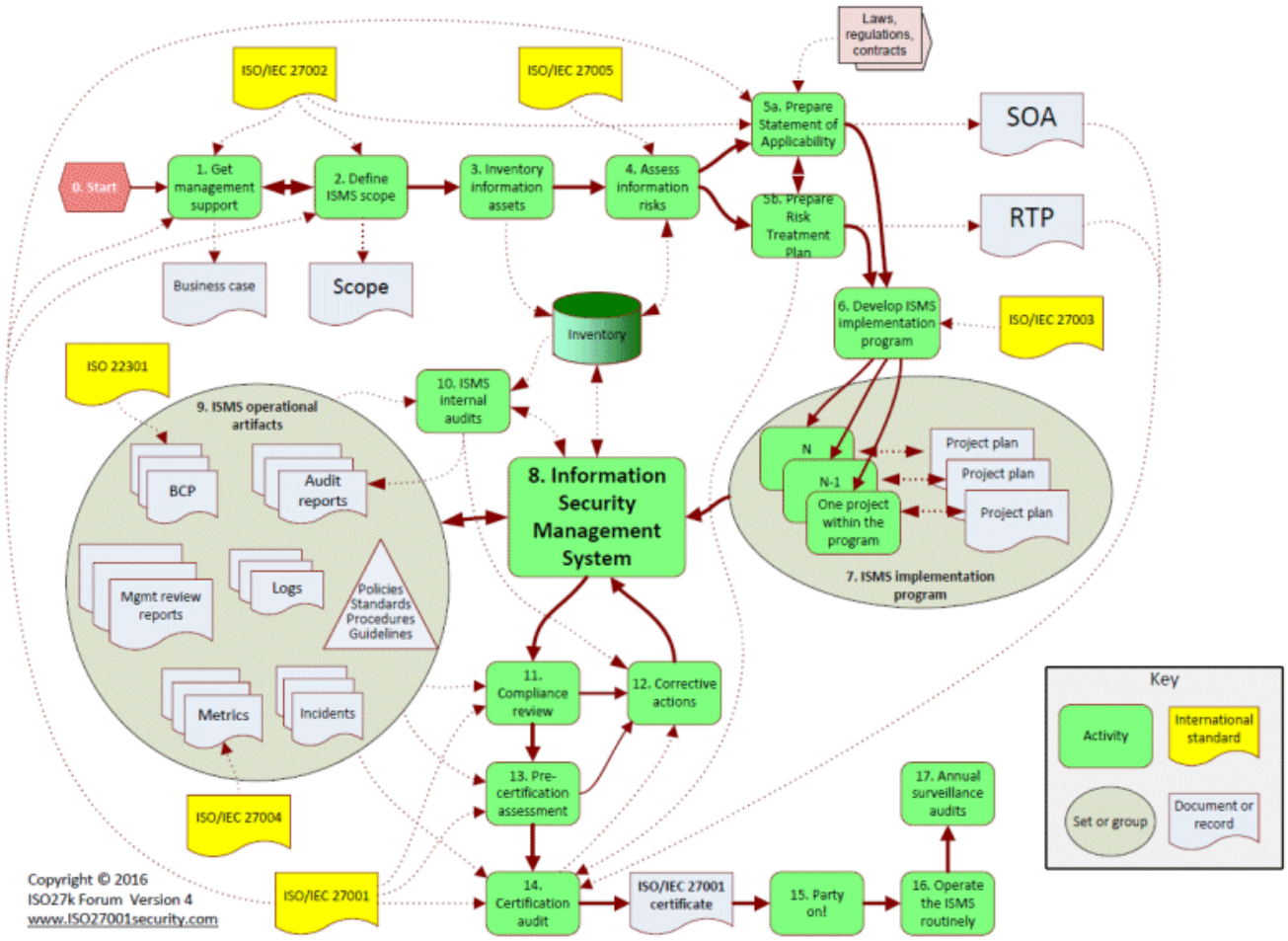
With the improvements well under way and security gradually becoming an inherent part of business-as-usual, it's time to think forward towards ISO/IEC 27001 certification. Like other management systems standards from ISO, ISO/IEC 27001 is process-focused - it helps set up a management system for information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

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.

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

A: See the overview ISMS implementation and ISO/IEC 27001 certification process diagram or grab the Visio original or a higher-resolution PDF (and check the ISO27k Toolkit for other languages):



The flow chart gives a high level view of the major steps in the process. This is a generic summary - 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 an ISO/IEC 27001 compliant ISMS. A great way to start is to raise management's awareness of some of the key current information risks and potential good practice controls (drawn from ISO/IEC 27002) that are not yet in place, perhaps through a "gap analysis" (an outline risk assessment and overview of the work needed to achieve compliance) 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 risk assessment** - ideally using a recognized formal method but a custom process may be acceptable if applied methodically. There's more advice in the risk management section of this FAQ.

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 a team leader) and support from 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. **Audit the ISMS** - *internal* auditing of the ISMS will be a routine part of it. The idea is to have competent and independent reviewers (*ideally* trained and experienced IT auditors) take a good look at the ISMS, review the evidence (ISMS operational artefacts plus other documentation such as information security policies and procedures), consider that in relation to the risks and opportunities to the organization, and make recommendations. Compliance with the formal requirements of ISO/IEC 27001 (see step 11) *may* be a major part of the audits but a competent internal audit function will generally be more interested in how well the ISMS meets the organization's requirements as a whole: gaining an ISO/IEC 27001 compliance certificate is probably just one of several business reasons for implementing the ISMS and investing in information security management. Identifying and addressing the organization's information risks in a structured, systematic, comprehensive, prioritized and coherent manner is the bigger goal.

11. **Review compliance** - are you actually doing what you said you were going to do? 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.

12. **Undertake corrective actions** - to improve the ISMS and address risks. The 'management system' part of the ISMS should result in continuous alignment between business requirements, information 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.

13. **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 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.

14. **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 artefacts *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.

15. **Party party** - seriously, getting certified marks the end of the implementation phase, a substantial milestone for the team and the organization so celebrate your success. You've earned it! More than that, your ISO/IEC 27001 compliance 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" ...
16. **Operate the ISMS** - it should be business as usual now. Other things to consider as your ISMS settles becomes routine and gradually matures include (1) taking a good look at the information risks and security arrangements in place elsewhere in your business network: are your suppliers, partners and customers also certified? Are they certifiable? Do they need your encouragement? (2) Using and maturing your security metrics to continue identifying and making improvements. (3) (4) If you haven't already done so, please join the ISO27k Forum to share your experience with others and participate in the global community.

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.

FAQ: "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 good practice security controls, supporting a comprehensive ISMS! Controls already in place won't be wasted but (in my experience) some will probably need improvements, most likely documentation for a start and probably some extensions to cover the entire breadth of 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 (particularly those that directly support the organization's business and risk management objectives) and those imposed by compliance obligations such as SOX, PCI DSS, privacy laws *etc*.

FAQ: "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. More likely, they will specify what *must* be addressed ("major **N**on **C**ompliances") and verified before they will issue the certificate, plus other things that *should* be addressed ("minor NCs" and niggles). At the end of the day – which may be some weeks *after* the certification audit once they are satisfied that the major NCs are fixed - the certification auditors must decide 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.

FAQ: "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 to third parties if it is issued by a recognized **C**ertification **B**ody (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 CBs, 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…

Implementation tip: find your national accreditation body or bodies listed here. Contact an accreditation body for details of the CBs they have accredited in your area. Read on for advice on choosing between the CBs ...

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

A: 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. It's up to your management to determine whether these risks are material in relation to the information 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!

FAQ: "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' favourite "Show me!"). They will gather and assess evidence including artefacts 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 niggles, minor concerns or potential future issues that management is well advised to consider;
    - **Minor N**on **C**ompliance - 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 N**on **C**ompliance - 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!

Following the initial certification process there are periodic follow-ups (usually called "surveillance audits", sometimes CAVs "Continual Assessment Visits") 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 these 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.

FAQ: "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 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 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.

FAQ: "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, so many assets to protect, so many factors to take into consideration.

PCI DSS (the **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard) 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 was not recommended but was still permitted under 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 all your valuable information assets.

An effective ISO/IEC 27001 ISMS using a comprehensive suite of controls drawn from ISO/IEC 27002 (and/or indeed other security standards such as SP800-53 FISMA) should satisfy and in fact *exceed* PCI DSS and other externally-imposed security compliance obligations, while simultaneously generating additional business benefits through satisfying internally-derived security requirements (*e.g.* protecting valuable but sensitive proprietary data against damage or unauthorized access by 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 long-term solution.

FAQ: 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 or 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 and organizational changes on your ISMS and/or information 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 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!).

FAQ: "What do we need to do in preparation for a re-certification audit?"

A: Unlike the six-monthly or annual surveillance audits which tend to focus on specific areas, a 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. *Re-certification 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 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 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 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 mitigating controls fail.
5. Review all the **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 or outdated ISMS documentation.
6. Get your information security **awareness and training** activities right up to date and ensure a plan is in place for future activities. Ensure everyone knows where to find the ISMS policies and related 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.

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 (again, 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 can actually produce solid 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 or 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 re-certification audit go more smoothly.

Implementation tip: email employees shortly before the recertification 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, records and other documentation to demonstrate what you do'). This is a classic security awareness opportunity!

Remember that the ISMS is a living thing, constantly adapting to changing business needs arising from evolving information 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 further 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