



# The ISO27k FAQ

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

This version was converted to a PDF on 8<sup>th</sup> December 2010

Please check the online version at [www.ISO27001security.com](http://www.ISO27001security.com)  
for the very latest updates.

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

## Contents

<b>Introduction, scope and purpose of this FAQ.....</b>	<b>4</b>
<b>Information security vs. IT security .....</b>	<b>5</b>
Q: “The titles of the ISO27k standards mention ‘Information Technology -- Security Techniques’. Does this mean they only apply to IT?” .....	5
Q: “When creating an ISMS, is it an absolute necessity to include members from all aspects of the business (business owners, finance, legal, HR, <i>etc.</i> )? I don't see the ISMS as being IT Security driven. I see it as being driven by the business with IT Security input. Am I correct?” .....	5
<b>Learning more about the ISO27k standards .....</b>	<b>7</b>
Q: “Where can I obtain [insert name of ISO27k standard here]?” .....	7
Q: “I want to become an ISO27k consultant. I'm looking for books or courses that teach ISO27k. Is there an exam? ... ” .....	7
Q: “Are there any qualifications for ISO27k professionals?” .....	9
<b>ISO/IEC acronyms and committees .....</b>	<b>11</b>
Q: “What does ‘ISO’ mean? And what about ‘ISO/IEC’?” .....	11
Q: “What do ‘WD’, ‘CD’, ‘FDIS’ and those other acronyms prepended to draft ISO standards really mean?” .....	11
Q: “What is meant by ‘JTC/1 SC27’ and what are ‘WG’s’?” .....	12
<b>Keeping up with security standards developments .....</b>	<b>14</b>
Q: “How can I keep up with developments to the ISO 27000-series standards?” .....	14
Q: “Can I see draft ISO/IEC standards? Can I contribute to them?” .....	14
Q: “How can I get involved in the development of security standards?” .....	14
<b>Getting started on ISO27k implementation .....</b>	<b>15</b>
Q: “Should we aim for ISO27k conformance, alignment, compliance or certification?” .....	15
Q: “Can anybody share numbers on how many man-years (or man-months) are needed to implement an ISMS?” .....	16
Q: “Is it necessary to appoint an Information Security Manager to implement and run an ISMS? If so, what qualifications should the ISM possess?” .....	18
Q: “Is it possible to restrict the scope of the ISMS to just one department or business unit, at least initially? If so, how do we treat risks that require controls outside the scope of our ISMS?” .....	20
Q: “What are the differences between the Statement of Applicability (SOA), Risk Treatment Plan (RTP) and Action Plan (AP)?” .....	21
Q: “I would like to see an RTP example, with one or two risks managed, please ... I would give anything to see a little part of one... I don't know how to start... I recently finished my risk analysis and I'm really stuck here.....” .....	22
Q: “In order to conduct a risk assessment, we need a list of all of our ‘information assets’. What kinds of things should be included in the list?” .....	23

Q: “Should the risk assessment process cover <i>all</i> our information assets?” .....	24
<b>ISMS documentation .....</b>	<b>24</b>
Q: “What documents are normally part of an ISMS?” .....	24
Q: “What format and style is appropriate for ISMS documentation?” .....	24
Q: “What should we cover in our [information] security policy?” .....	25
Q: “ISO 27002 provides general rules, but I cannot translate that to match what I have at work, in real life. Any guide or advice?” .....	28
Q: “I am trying to put together a document for <i>working in secure areas (9.1.5)</i> . How much information should it contain <i>i.e.</i> is this just a one pager or a full manual?” .....	28
<b>Maturing your ISMS .....</b>	<b>30</b>
Q: “What Content Management System should we use for our ISMS?” .....	30
Q: “Is control X mandatory [for various values of X]?” .....	31
Q: “Which laws and regulations do we need to comply with, according to ISO/IEC 27002 section 15?” .....	33
Q: “What can the ISMS implementation project manager do to assure success?” .....	34
Q: “Our organisation is planning to implement metrics to measure the effectiveness of both information security and management controls. What is the starting point and process?” .....	35
<b>Information security risk analysis, assessment and management.....</b>	<b>38</b>
Q: “We are just starting our ISO27k program. Which information security risk analysis method/s could we use?” .....	38
Q: “How should I choose a risk analysis tool or method?” .....	46
Q: “What is the difference between risk assessment and audit?” .....	49
Q: “How should management define the organization’s <i>risk appetite</i> ?” .....	50
Q: “Is there a published list of information security threats? .....	51
Q: Our third party penetration testers recently found 2 medium risk and 7 low risk vulnerabilities. I disagree with the ratings and want to challenge the medium risks (some old software) before they report to the Board. What do you think?.....	52
<b>Certification against ISO/IEC 27001 .....</b>	<b>52</b>
Q: “How does my organization get certified against ISO/IEC 27002?” .....	52
Q: “OK then, how do we get certified against ISO/IEC 27001?” .....	53
Q: “What is <i>really</i> involved in becoming ISO/IEC 27001 certified?” .....	56
Q: “Will the security controls we have already implemented be sufficient for the final ISO 27001 certification?” .....	59
Q: “Who can certify us against ISO/IEC 27001?” .....	59
Q: “How does the certification process work?” .....	60

Q: “This is all very complicated and uncertain. There are so many variables! Isn’t there just a simple checklist we can follow, like PCI-DSS?” ..... 62

**ISMS auditing ..... 63**

Q: “I work for an Internal Audit function. We have been asked by the ISMS implementation project team to perform an ISMS internal audit as a prelude to an external/third party certification audit against ISO/IEC 27001. They are asking for a load of things from us and expect us to do the audit within a tight timescale defined on their plans. Is this information really needed? Are we (as an independent audit team) forced to give them such information? Should we perform a quick Internal Audit or take the time necessary although the certification would be postponed? Are there ISMS Audit Programme/Plan templates we can use and what other considerations should we take into account for the ISMS internal Audit? ...” ..... 63

Q: “How can we confirm the implementation of controls selected in the Statement of Applicability?” ..... 64

Q: “Will the certification auditors check our information security controls?” ..... 65

Q: “How will the certification auditor check our ISMS internal audit processes? I’m nervous! What are the typical questions we should expect?” ..... 66

Q: “What do we need to do to prepare for a recertification audit?” ..... 67

**Copyright and disclaimer ..... 69**

---

## Introduction, scope and purpose of this FAQ

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

## Information security vs. IT security

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

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

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

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

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

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

A: ISO27k is most definitely about **information security management systems**. IT security is of course a large part these days, given that so much information is communicated, stored and processed on computers, but non-computerized information assets (files, paperwork, printouts, knowledge) are still valuable corporate assets that deserve protection just as much as computer data, if not more so in the case of many forms of proprietary knowledge. What's

more, the average IT department does not own and hence lacks full and total control of all the computer data, systems and/or networks in the entire organization, so limiting the scope of the ISMS to IT would not necessarily protect all the data to the same degree.

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

- Information security is inherently complex and difficult to do well, while perfect security is practically unattainable. Whereas hackers, fraudsters and information thieves need only find a small chink in our defences, we must defend all points simultaneously, both around the perimeter and within. Most organizations have a plethora of technical platforms, applications and network connections, plus a raft of non-IT information assets to protect. We all face a range of internal and external threats, including the mundane but ubiquitous errors, accidents, equipment failures, bugs *etc.*
- The need for information security mirrors the use of and dependence on information, and therefore extends across the enterprise and beyond. It is not only necessary to involve representatives of the entire organization but also business partners, particularly where the organization outsources critical information processes or relies on IT and telecomms services from third parties and hence has a direct interest in their security arrangements. Customers, owners, regulators and other stakeholders share similar concerns, leading to substantial governance and compliance obligations.
- Information security threats and vulnerabilities are constantly changing. As with the capital markets, this dynamism creates both risks and opportunities for the organization, especially in competitive environments (which includes national security and government departments by the way!). Agile, security-aware organizations respond to both, but positioning information security as a business enabler is a hard sell to old-fashioned managers with outdated views.

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

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

here"). This is a useful concept because those at the top generally have the budgets and influence to make security happen.

---

## Learning more about the ISO27k standards

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

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

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

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

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

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

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

A: The best [books](#) on the ISO27k standards are the standards themselves - in other words, you should buy and read the standards. Being standards, they are quite formal in style but

readable and useful. If you are going to implement them, write policies based upon them, consult around them *etc.* you will inevitably have to become very familiar with them so buy your copies and start reading!

The three main standards are essential:

- [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](#) is the formal certification standard, the 'Specification for Information Security Management Systems'. It is especially useful if you intend to become a accredited ISMS certification auditor - the usual way of doing that is to go through a training course run by one of the information security management system accredited audit and certification bodies such as the BSI, or various training and consultancy companies. They are generally called "ISO/IEC 27001 Lead Auditor" courses.
- [ISO/IEC 27002](#) is the 'Code of Practice', a practical standard with tons of advice for those designing and implementing an information security management system. The best way to learn ISO/IEC 27002 is to use it, which means going all the way through an implementation 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. Professional organizations such as [ISSA](#), [ISF](#) and [ISACA](#) can help. Once you have made a start on your implementation, please join the free [ISO27k Forum](#) to consult with your peers.

You should also be well aware of the remaining issued ISO27k standards (e.g. [ISO/IEC 27005](#)) 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, I advise you to start by building a solid technical understanding of IT, risk and control concepts. Advice for people who want to become IT auditors in the IT Audit FAQ is useful for those planning to become "ISMS Lead Auditors" and is also pretty relevant to becoming an information security management specialist since the two fields are very closely related. Another excellent source is [www.CCcure.org](http://www.CCcure.org), especially if you are considering becoming CISSP, SSCP or CISM qualified in information security management.

[There is more advice in the next Q&A.]

**Implementation tip:** further resources are outlined on the [books](#) and [links](#) pages at [ISO27001security.com](http://ISO27001security.com) and don't forget to join the [ISO27k Forum](#) - the Forum archive is a valuable resource worth browsing or searching (it's a Google group so the search function actually works!), and members can always seek fresh answers though live dialogue.

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

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

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

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

## ISO/IEC 27001 Lead Auditor (LA)

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

1. **The highway:** spend 5 straight days on a suitable officially-recognised training course run by an officially-recognised training body, pass the end of course exam, then undertake a further 35 days of third party certification audits under the guidance of a registered ISO/IEC 27001 LA. This route is preferred by the [International Register of Certification Auditors](#) and, in Japan, [JRCA](#). The highway naturally suits students who are employed by the accredited certification bodies, since they can get both the classroom training and on-site experience from their employers.
2. **The country route:** complete some other form of ISMS/audit related training (for example modular courses comprising a day or two's training on ISMS plus 3 days on auditing), then undertake further ISMS assignments such as internal ISMS audits, ISMS-related consultancy gigs or third party certification audits, and finally pass some form of "on-site skills examination". The country route may be the best option for students not working for accredited certification bodies, but may not deliver as much assurance.
3. **The cross-country 4x4 route:** become a qualified and experienced information security professional *and* a qualified and experienced IT audit professional *and* gain

lots of real-world experience of designing, building, implementing, managing, maintaining and advising on ISO27k ISMSs. Most professionals with more than, say, a decade or two's work experience crossing these three areas have amassed valuable expertise, knowledge and battle scars, having faced many situations in the field. Some of them go on to take the highway or the country route, while others are too busy working for their clients or sharing their expertise with their employers to worry about certificates *per se*.

4. **The back alleys:** a few students and consultants evidently don't bother with the hardship of actual training, exams and/or on-the-job experience, simply adding "ISO/IEC 27001 LA" (or similar) to their CVs and email signatures and carrying on regardless ...

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

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

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

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

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

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

---

## ISO/IEC acronyms and committees

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

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

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

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

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

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

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

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

A similar sequence applies to Technical Reports.

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

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

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

**Q:** “What is meant by ‘JTC/1 SC27’ and what are ‘WG’s’?”

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

JTC1’s purpose is “Standardization in the field of Information Technology” which “includes the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information.” While there is general agreement that information security is a superset of IT security, the fact that the ISO/IEC committee is IT specific means that the ISO27k information security standards are in fact labelled IT standards.

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

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

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

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

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

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

**Please note:** the [IKSO27001security.com](http://IKSO27001security.com) website is independent of and does not belong to, nor is it endorsed by or affiliated with, ISO/IEC. Please read the online [disclaimer](#) for more.

---

## Keeping up with security standards developments

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

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

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

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

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

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

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

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

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

A: Contact your local national standards body (e.g. [BSI](#), [NIST](#)) to find out about any special interest groups and committees working in the information security arena. If you can spare

the time to get involved with standards specification, development and/or review, contact your local ISO/IEC JTC1/SC27 representative/s to volunteer your services.

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

---

## Getting started on ISO27k implementation

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

A: Yes.

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

- **Conformance** (here meaning a general intent to apply the ISO27k standards) is a basic starting point, achievable at little cost for any organization that takes information security seriously. However, the 'general intent' bit implies a fair amount of management discretion about which specific parts of the ISO27k set are going to be used, and more importantly to what extent they are to be adopted. Conformance gives little if any assurance to third parties about the organization's information security status. It's practically meaningless without further information (for example which ISO27k standards have been implemented, and to what extent? Is the organization merely planning to adopt the ISO27k standards at some future point, or has it already done so? Does it actually have a working ISMS??). However, some people confuse "conformance" with "compliance": just remember that conformance starts with a con...
- **Alignment** is about as worthless as conformance. It could mean practically anything. Putting all your ISO27k standards in a neat row on the bookshelf is one form of alignment ...
- **Compliance** (meaning a more rigorous, comprehensive and systematic adoption of the ISO27k standards) is the next level which typically involves the organization implementing an ISMS of some form (ideally using ISO/IEC 27001) along with a suite of information security controls (ideally using ISO/IEC 27002). The organization *asserts* that it is compliant with standards but may or not offer any proof. The value of the assertion by

itself depends largely on whether the organization is both competent at information security management and trustworthy.

- **Certification** *normally* means formal certification of the organization's ISMS against ISO/IEC 27001 by an accredited certification body. This in turn means that the organization's ISMS has been independently audited by competent ISMS certification auditors to confirm that the management system fulfills all the mandatory requirements of ISO/IEC 27001, and is operating correctly. *It is a moot point as to whether this means the organization is actually secure in any real sense* since certification auditors need not necessarily probe too deeply into the presence, design and/or operation of the information security controls: their primary interest is in to check the management system not the information security. That said, it is commonly assumed that an effective ISMS which complies fully with ISO/IEC 27001 will in fact be supported by a reasonably comprehensive and effective suite of information security controls, and that the organization is proactively managing and continually improving them.

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

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

**Q:** "Can anybody share numbers on how many man-years (or man-months) are needed to implement an ISMS?"

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

1. **Level of senior management support.** Definitely *the #1 factor* in my book, as just noted above. Affects most of the rest of this list. Itself depends on management's understanding of what will be or is involved in the implementation, and what are the business drivers and anticipated positive outcomes for the organization when the ISMS is in place and certified. Can be overcome to some extent by information security awareness activities, business cases, and general schmoozing, focusing specifically

on these issues for the Execs and dealing positively with their concerns. Hint: it pays to work one-on-one with individual managers, not address just some faceless “management”.

2. **Level of middle/junior management understanding and support**, particularly in areas such as IT, HR, Risk Management and Legal/Compliance. Tends to follow #1 but not necessarily in dysfunctional organizations. Can also be mitigated/improved through security awareness, schmoozing *etc.* Make friends and influence these people by showing them how the ISMS will make their jobs easier and more effective.
3. **Experience, capabilities and diligence of ISMS implementation team** comprising the team leader (probably but not necessarily the Information Security Manager) plus assorted team members. Can be boosted by reading and training, plus of course this website and the [ISO27k Forum](#). It is also worth considering targeted consultancy assistance to benefit from others' experiences (both good and bad!). Includes expertise in project and change management, and political astuteness: remember this is *NOT* repeat *NOT* a purely technical project within IT!
4. **Organization's information security maturity level** when starting the project, and their desired goal level when the implementation phase can be considered “finished”. Usually unstated and difficult to pin down. Worse than that, it's a moveable feast that will shift as the project proceeds, typically because improved information security risk assessment processes identify ‘risks and opportunities’ [for improvement] that weren't even appreciated in the beginning (ah, ignorance is bliss) ...
5. **The organization's actual/true level of information security risk**. This factor rather self-evidently affects the amount and quality of security controls necessary, and hence the nature of the ISMS required. A military or high-profile organization in an intensely competitive market or highly regulated industry will *probably* end up with a rather different ISMS than, say, a bicycle shop.
6. **Existing compliance load and experience** e.g. PCI DSS, DPA, FISMA and particularly ISO 9000 or similar *ISO management systems* expertise within the organization. The need for compliance with externally-imposed information security-related laws, regulations, contractual terms *etc.* may be driving the ISMS implementation project forwards, but equally this pressure tends to divert many of the self same resources from their ISMS implementation activities.
7. **Level of understanding and support for the ISMS project in related functions** such as IT, risk management, finance, HR, legal/compliance, physical security, audit, plus key business functions (*i.e.* the political and commercial powerhouses of the organization). Make no mistake: if your ISMS does not have - or at least if the implementation project cannot generate - sufficient genuine friends in such functions, you are stuffed. Ignore this factor at your peril.
8. **Strategic fit** between the putative ISMS claimed/actual benefits and the organization's stated/actual business goals. Finding, creating and/or making explicit the points of alignment (such as obviously shared objectives *etc.*) can be the key *both* to surmounting any speed bumps on the road to ISMS nirvana *and* generating ISMS success metrics that management simply cannot ignore.

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

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

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

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

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

**Must haves:**

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

**Highly recommended:**

- Professional IT or similar technical background (e.g. former IT system/network administrator, analyst, developer, project manager, operations, IT disaster recovery/contingency planner/manager)
- Project and personnel management experience, good at scheduling and managing time, people, budgets, tasks *etc.* and working to dynamic priorities
- Excellent communication skills, both written and oral, able to demonstrate the ability to write well and present confidently, evangelically even (check in the interview process)
- Business management experience & expertise, ideally **MBA** material, with knowledge of the organization's business situation, strategies and goals
- IT audit skills (e.g. able to assess risks, ask the right questions and get to the bottom of things, plus write and present formal management reports), ideally qualified to **CISA** or equivalent
- Hands-on experience of ISMS design and implementation (e.g. actively contributing member of the [ISO27k Forum!](#))
- Process- and quality-oriented (demonstrated ability to identify and deliver continuous process improvements, knowledge/experience of ISO 9000 and ITIL/ISO 20000) plus people skills (e.g. generally gets along with all types of person yet self-confident and assertive enough to lay down the law when required without being aggressive)
- Highly organized, structured and self-motivated, "driven" even
- Negotiation skills
- Pragmatic rather than overtly academic, theoretical or idealistic outlook
- Works well under stress induced by conflicting priorities, frequent "interrupts", limited resources, unreasonable/unrealistic expectations and often negative perceptions about the value and role of information security
- Knowledge of, and ideally familiarity with, the ISO27k standards
- Can competently and confidently explain the differences between threats, vulnerabilities and impacts, giving relevant examples

**Nice to haves:**

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

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

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

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

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

- **Controlling** the risks through Service Level Agreements (typically with other business units or departments of the same organization) or contracts (with third parties) that specify certain security requirements, and perhaps technical and/or procedural controls for example a defined process for identifying and dealing with information security incidents affecting the trans-border information flows;
- Knowingly **accepting** the risks, albeit preferably with suitable contingency arrangements in place in case they materialise;

- **Transferring** the risks through some form of insurance, agreed liabilities *etc.*;
- **Avoiding** the risks [by not restricting the scope!].

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

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

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

**Implementation tip:** rather than deliberately and consciously restricting the scope of the ISMS as you suggest, it may instead be worth talking in terms of a “pilot implementation” in whichever area/s you choose. This minor wording change implies that, provided it is successful, the pilot *will* be expanded to become a full-scope implementation ...

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

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

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

[ISO/IEC 27000](#) should help resolve any remaining confusion.

**Implementation tip:** don't get too hung up on the acronyms and titles of the documents. It is conceivable that one or more of them may be dropped when ISO/IEC 27001 and 27002 are

revised. Concentrate on their primary purpose, which is to document the links between information security risks, control objectives and controls.

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

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

21. Risk: network infection by worms and similar malware, causing network outages, data damage, unauthorized access to systems and various consequential damages/losses including incident investigation and cleanup costs.

Risk treatments: mitigate the risk primarily through antivirus controls, plus network, system and data logical access controls, plus incident management, backups, contingency plans, plus policies, procedures and guidelines.

22. Risk: serious fire in the data centre, causing loss of datacentre IT services for an extended period.

Risk treatments: avoid risks by taking care over the location and construction of the data centre, including any post-build modifications. Also avoid excessive storage of flammable materials including magnetic media (e.g. locate the media archive elsewhere on site). Physical security controls including fire alarms, extinguishers etc., coupled with fire evacuation procedures and training. Also insurance cover against fire damage. Also avoiding excessive reliance on the data centre through dual-siting of critical network devices and servers.

23. Risk: corporate prosecution for copyright abuse.

Risk treatments: avoid copyright abuse through using a centralised software and license inventory, regularly audited and reconciled both internally (e.g. actual number of installations <= licensed number) and against installed software on corporate IT systems (e.g. searching for additional software not listed in the inventory), coupled with various compliance measures, policies and procedures. Also restrict physical site access to authorized persons, limiting the potential for license snoopers ...

24. Risk: unreliable commercial software causing Blue Screen Of Death at the worst possible moment.

Risk treatments: specify and test security aspects in software procurement process. Maintain software. Accept the residual risk for Windows.

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

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

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

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

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

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

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

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

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

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

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

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

---

## ISMS documentation

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

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

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

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

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

There are some drawbacks though:

1. You need the skills and tools to design, prepare, publish and maintain the website, or at least easy access to someone who does that.
2. Web pages (like this one!) don't usually print out very well, so for things that people want to print and refer to, comment on, or whatever, you may need to supply printable versions (e.g. PDFs) to download and print from the same web pages.

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

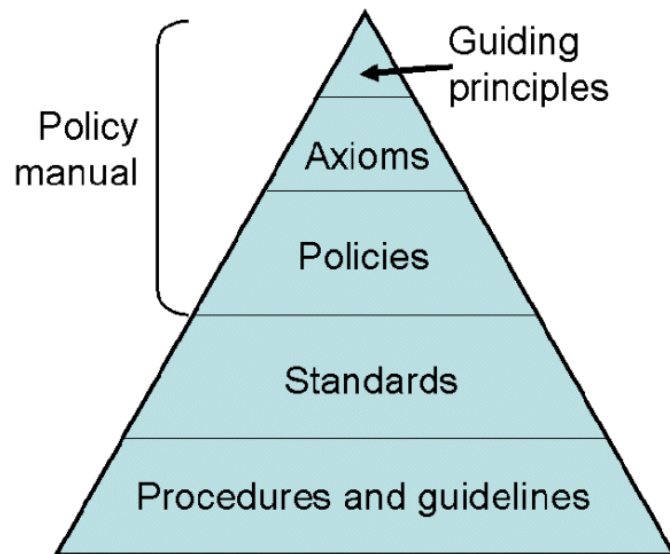
**Implementation tip:** it definitely helps to have a consistent style/format for each type of material, and even better some consistent elements on all of them to bind them into a coherent suite. Do you have an ISMS logo, perhaps, with which to 'brand' the documentation and security awareness materials?

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

**A:** It's up to you - well, strictly speaking, it's up to your management. See [section 5 of ISO/IEC 27002](#) for a decent outline of what the policy should cover, as a minimum. However, the current versions of both '27001 and '27002 are somewhat cryptic, talking about both an "ISMS policy" and an "information security policy" without actually explaining exactly what they really mean by those terms, what the differences might be *etc.* [It is *conceivable* that the original authors were actually thinking about the same thing but accidentally used different words, and that difference has subsequently taken on a life of its own! It's something that

several SC27 members noted as an issue and is being addressed during the current revision of the standards. Sorry we can't be more specific right at this moment: we are literally trying to figure it out for ourselves! The revision process will take time so meanwhile everyone just has to make the best of it and hope that your certification auditors are reasonable about it (we've not yet heard of any that aren't!).]

My personal preference is for a [comprehensive security policy manual](#) following the structure of [ISO/IEC 27002](#) and supported by technical standards (e.g. "Baseline security standard for Windows 2003"), procedures, guidelines and other [security awareness materials](#):



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

Two styles of information security policies are common:

1. Individual policies covering specific security issues such as "Email security policy" and "Network access control policy". Typically these are quite formally worded and define security responsibilities of key groups, functions, teams or people. They may include introductions and explanations to aide reader comprehension, and should reference relevant documents at higher and lower levels of the policy hierarchy. They should be technology-neutral and succinct - ideally no more than a few pages.
2. A comprehensive policy manual containing succinct policy statements reflecting the whole of [ISO/IEC 27002](#), with numerous embedded cross-references between related

policy statements and to related axioms, standards, procedures and guidelines. The manual functions as a master index for the entire policy suite, which helps avoid overlaps, gaps and (worst of all) conflicts.

### **Many organizations use *both* styles of policy.**

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

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

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

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

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

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

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

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

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

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

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

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

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

- Write;

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

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

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

Your policy development process will, in time if not now, come up against the challenge that many potential subject areas *could* be covered by multiple policies, looking at similar issues from different angles. "Working in secure areas", for instance, begs obvious questions about what constitutes "working" (do you mean just employees, for instance, or does it apply to contractors, cleaners, maintenance people, even security guards on patrol?), and how you have identified and defined "secure areas" (is there a physical risk assessment process? Does it take into account the security risks associated with information assets in each area? Does it adequately cover information that is in use, in storage or in transit? Are you dealing with classified information, whether internally classified or national security classified). You can carve up all your controls in numerous ways, and (trust me!) it is very easy to end up with a totally unworkable mess of overlapping, conflicting and yet gappy policies if the overall policy development process is not itself well managed. Again, my advice is to think and plan comprehensively from the outset, using [ISO/IEC 27001](#) and especially the more detailed [ISO/IEC 27002](#) as a basis for your policy set, since:

1. The ISO27k standards' authors (members of committee ISO/IEC JTC1/SC27) have put a lot of work into figuring where each potential subject area is 'best' covered. ISO27k is reasonably comprehensive in coverage but the option remains to extend it if you need more. ISO/IEC 27002, in particular, incorporates numerous cross-references between applicable areas where appropriate rather than duplicating controls;

2. ISO27k constitutes good practice, in other words it is a sound basis for information security risk management, accepted worldwide;
3. Even where an arbitrary decision has been made about which heading suits some topic, it is specified thus in an international standard which makes it OK to copy that;
4. ISO27k provides a generally understood common vocabulary and structure, meaning your '27001 certification auditors, ISMS consultants and any new ISMS-aware employees will be instantly familiar with the layout and general content of your policy suite.

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

---

## Maturing your ISMS

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

A: We cannot recommend a specific CM 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. Anyway, on that understanding, here are some free/open source and commercial Content Management System (CMS), Document Management System (DMS), Learning Management System (LMS) and Policy Management System (PMS) options to consider in your evaluation:

1. **Alfresco** is an enterprise CMS available in free and commercial versions.
2. **Bizdoctor** from Claritus Consulting has ISMS policy management and training options.
3. **CENTRE** from ITG.
4. **Core Business Solution** from Core Business Solutions.
5. **Documentum** from EMC.
6. [Drupal](#) is a popular generic open source CMS.
7. **Entropy** from BSI.
8. **ISIS** (Information Security Intranet Solution) from Insight Consulting (now part of Siemens) was built around BS7799. It's not clear whether this product is still available.
9. **ISOsystemPlus** from Netcomm is a CMS with modules supporting compliance with various standards, including ISO/IEC 27001 (although they refer to ISMS as "Information Safety Management System" so make of that what you will).
10. **Liferay Portal** is an enterprise web platform that includes a webdav fileserver portlet and uses Role Based Access Control.

11. **LiveLink** from OpenText.
12. **Rainbow Portal** is an open source CMS built on ASP.Net and C#.
13. **RealISMS** from Realiso Corp has functions supporting risk assessment, policy management and continuous improvement.
14. **Rulesafe** from Secoda lets you define information security policies, generate awareness and check compliance.
15. **SecureAware** from Neupart is specifically designed as a CMS/LMS/PMS for an ISO27k ISMS. It lets you define and promulgate security policy statements, create training and testing exercises based on the policy, assess and manage information security risks and compliance, manage business continuity *etc.*
16. **Security Governance System (SGS) 27k** was developed by Flexeye for its customer BT. "As well as improving the quality of your ISO27001 projects, SGS 27K will save you up to 50% of the effort involved with the management of compliance or certification."
17. **Sharepoint** is Microsoft's general-purpose CMS.
18. **VigilEnt Policy Center** from NetIQ is an intranet based security PMS.

Hungry for more CMS options? Wikipedia has a useful [table listing CMSs](#).

Please [let us know](#) about other CMS, LMS, PMS and similar systems designed to support ISMSs and ISO27k. We haven't used most of them and are not recommending any, merely providing basic information to help you decide what's appropriate for you.

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

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

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

1. Yes, you need X because it is a basic security control that everyone needs. You'd be silly/negligent/risking the farm not to have it.
2. No, X is not needed because we don't have it, therefore we consider it neither good practice nor best practice nor recommended.
3. That depends - I'm a consultant with lots of letters after my name but you'd have to pay me \$\$\$\$ to answer your question.
4. No, X is unnecessary because it is more costly than the incidents it prevents. Unless we are really unlucky anyway. Do ya feel lucky, punk?

5. You tell me: have you assessed the information security risks and identified a troubling risk that control X might mitigate? Have you decided that it would be better to implement X than some other risk treatment (avoid the risk, transfer the risk, accept the risk)? Is X the most cost-effective control in this situation? Does X adequately mitigate the risk and, ideally, others too yet without making the situation worse through additional complexity, procurement/management costs or whatever? Is X feasible?
6. Yes because NIST/COBIT/SOX/a little bird says so.
7. Yes.
8. No.
9. Yes because it is “mandatory”, according to [insert favorite authority figure here].
10. No because it is “optional” and/or was not explicitly listed in black and white as absolutely mandatory by [insert favorite authority figure here too].
11. Yes because it's the law [in country Y].
12. Only if your policies, plans, strategies, technical architecture, or internal standards say so.
13. Yes if there is a positive ROSI [Return On Security Investment], no if the ROSI is negative or if someone has seeded “reasonable doubt” or if there is something sexier on management's agenda this afternoon.
14. Yes, absolutely - I am a vendor selling X. X is all you need. X is better than sliced bread. I'd sell both my kidneys to buy X ...
15. Yes because we will get a bad audit report and/or grief from HQ if we do not have X.
16. Not necessarily now but it will definitely be required in the future. Trust me.
17. No because we cannot afford it at the moment.
18. No because if you have it, then we have to have it too, else we will appear behind the times and that is BAD.
19. Yes because we have it and you are Behind The Times.
20. Do you even have to ask? Doh!

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

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

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

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

decision on a rational basis. If the risk analysis and/or their reasoning and decision making processes were fundamentally flawed, the auditor would have grounds to complain and (in the case of a certification audit) perhaps refuse to certify, although even this outcome is not absolutely certain.

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

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

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

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

1. **Privacy** or data protection acts if you are handling personal data (client data or employee data).
2. Computer misuse act or equivalent laws about **hacking**, unauthorized network access, malware *etc.*
3. **Telecommunications** laws about lawful/unlawful interception *etc.*

4. General **business laws** around company structure, taxation, governance (e.g. SOX), HR, health & safety, building codes, fire escapes *etc.*
5. Other **general laws** e.g. theft, fraud, misrepresentation, deception ...
6. **Consumer** laws concerning how your company represents its products, warranties, fitness for purpose, merchantability, quality (and by implication, security) *etc.*
7. **Contract** law concerning contracts with third parties (suppliers, partners, customers), liabilities, commitments *etc.*
8. **Intellectual property** protection laws including copyright, patents and trademarks, protecting both your own IP and that of third parties.
9. **Industry-specific laws and regulations** e.g. finance industry (banking laws, money laundering), PCI-DSS, govt & defence industry (freedom of information, official secrets, critical infrastructure, terrorism ...), medical (more privacy requirements, sometimes regulations about data formats) *etc.*
10. **International** laws, or rather the laws of foreign jurisdictions, if your company does business with foreigners, uses overseas facilities or services *etc.*
11. **++ Others:** speak to your lawyers/corporate legal counsel about this, and/or your compliance function if you have one. Aside from the more obvious laws and regs about information security, several “non-IT” laws have an impact on IT and information security in the sense that the laws concern protecting or using or abusing information, or concern business processes and individual activities which are often computerised. Therefore there can be compliance obligations affecting the way the IT systems and information processes are designed and/or used, even from “non-IT” laws.

**Implementation tip:** compliance with externally-imposed obligations can be an important driver to implement an ISMS, not least because it can take some of the weight off management’s shoulders

**Q:** “What can the ISMS implementation project manager do to assure success?”

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

- Become familiar with the business you serve. Get to know the department heads and the challenges they face. Try to see information security risks and controls from their perspectives, and look hard for situations in which strong, reliable information security is taken for granted or presents opportunities for new business activities that would otherwise be too risky.
- Cultivate business champions for information security in key areas, for example by talking to sales people on how they win business and what would help them be more successful, asking R&D people about the importance of keeping research secrets from commercial rivals, and checking how finance department satisfies SOX and similar integrity obligations.

- Make friends with colleagues in related functions such as risk management, compliance, internal audit, site security/facilities and IT. Take time to explain to them how an ISMS will support what they do, and garner their explicit support for the implementation project. These people are often influential with senior management.
- Present ISO27k as a **practical solution** to current and future business problems rather than an academic set of controls. Solutions are more palatable than controls. Focus on the business outcomes of the ISMS rather than the ISMS itself. Continue to sell the ISMS as a solution to business needs and encourage other managers involved with security to adopt a similar business-focused attitude. Seek out and exploit strategic alignments.
- Remember that if the business is to adopt ISO27k and take on board a culture change, it should be perceived as empowering and enabling not restrictive and disabling.
- Tone down the technobabble and learn business-speak. Remember, IT is only *part* of the ISMS albeit an important one. Make a special effort to reach out to, inform and engage senior management up to board level: their understanding and support for the ISMS will facilitate the numerous changes necessary to business processes and systems as they are secured, and conversely their active or passive resistance will make your job *much* harder. Consider starting your management-level security awareness activities early.
- Celebrate successes. Take every opportunity to write-up and share situations in which information security helps the organization mitigate risks. Case studies and direct quotations from managers or staff who appreciate the value of the ISMS all help to spread the word: security is as much about saying “Yes!” as “No!”

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

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

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

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

First I recommend reading the ISO27k implementation guidance paper from the free ISO27k Toolkit on [ISO27001security.com](http://ISO27001security.com). It proposes a set of 39 information security metrics aligned with the 39 key sections of ISO/IEC 27002, which will give you a basic starting point and

some ideas of things perhaps worth measuring but be patient. More importantly, the paper also lists some metrics-related references that you should check out, for example [“You are what you measure”](#) by Hauser and Katz.

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

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

It may seem too early but it's almost certainly worth talking to your management about what they might expect during this metrics design phase. Look at what kinds of metrics they get from other management systems. Find out what they actually use *versus* what they get, and look for clues about what works 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 anything really worthwhile. They are ‘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? The [Hauser and Katz paper](#) is worth re-reading here as it's all too easy to drive changes the wrong way through the inappropriate use of metrics and targets.

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

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

**Implementation tip:** as well as the book "**Security metrics: replacing fear, uncertainty and doubt**" by Andrew Jaquith (~US\$34 from [Amazon](#)) which offers excellent advice, I'd also recommend "**Information security management metrics: A Definitive Guide to Effective Security Monitoring and Measurement**" by Krag Brotby (~US\$64 from [Amazon](#)). It's not a metrics cookbook ('Measure these 35 things every week ...'), but a general treatise on management metrics and their utility in relation to managing, controlling, directing and improving information security. Krag is strong on the difference between strategic and operational metrics. If you make the effort to read and think about it and the other references mentioned above, it will give you a good grounding in the field and a framework to decide what metrics you and your management really really want.

---

## Information security risk analysis, assessment and management

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

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

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

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

One thing to take care over, though, is how to resolve the inevitable discrepancies in the results from different methods. A crude policy such as "Pick whichever recommends the least costly controls and minimise only the obvious risks" is no better than "Pick the most comprehensive and minimise all the risks". The analyses are merely decision support tools to guide management, who still need to make the vital decisions about how much security investment is appropriate, how much risk can be tolerated, how much certainty is really needed in the decision process, and when to make any needed information security improvements. Resolving such dilemmas requires management vision and experience,

coupled with expert analysis/advice ... and gut feel. Good luck ... and don't neglect your contingency plans!

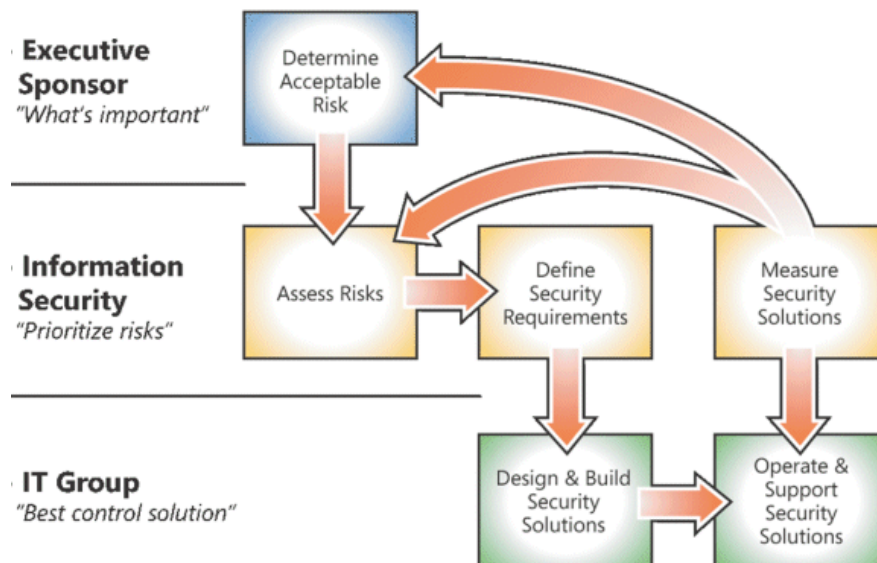
Below is a very brief introduction to a number of information security risk analysis/risk management methods, standards, guidelines and tools, plus some aimed at supporting GRC (governance, risk and compliance) and even SIEM (Security Information and Event Management). *Please note that we are not selling or endorsing any of them, nor do we earn commission or advertising income from 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. **AdaptiveGRC** from Audit2 facilitates combined assessments against multiple compliance obligations;
2. **Alive-IT** from Controll-IT is a tool supporting business continuity planning;
3. **AMS9000** by Northwest Controlling Corporation Ltd. is workflow software supporting compliance audits against standards such as ISO/IEC 27001;
4. [AS/NZS 4360:2004](#) is a well-respected risk management standard published jointly by Australia Standards and New Zealand Standards. [HB 436:2004](#), a handbook of risk management guidelines, is designed to accompany and expand on AS/NZS 4360. HB 436 includes and explains the text of the standard;
5. **BITS** (a US financial services industry forum) published a [risk assessment spreadsheet](#) - not a full RA method as such but could form the basis of a process;
6. **BWise GRC** builds on process/risk management and compliance expertise, helping organizations manage corporate obligations plus enterprise risks;
7. [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;
8. [chaRMe](#) is an open source information security risk management support tool being developed by Secopan. The tool is available as a VMware appliance and has a German, English and Chinese (Mandarin) user interface;
9. **Citicus ONE** is a risk management system from Citicus, based on [FIRM](#). And now with the ability to accept inputs using an iPad or iPhone;
10. **ClearPriority** "continuously monitors your enterprise systems, networks and applications. The platform captures, monitors and assesses - in real-time - complex risk factor interdependencies that span geographies, departments and lines of business";
11. **CMS Information Security Risk Assessment (RA) Methodology** is the Centers for Medicare and Medicaid Services' guide to their method for analyzing information security risks, derived from NIST SP800-30;

12. [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 auditors;
13. **Control Compliance Suite** from Symantec supports compliance with information security requirements through process automation, coupled with point-in-time controls assessment and real-time monitoring of risks and threats;
14. **Control Path** supports information security risk management for internal business purposes and vendors, policy management and business impact analysis;
15. [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;
16. **Countermeasures** by Alion supports risk assessment and controls selection with a particular focus on physical security and NIST SP800-53;
17. **CRAMM**: (CCTA Risk Assessment and Management Methodology), originally developed for UK Government use, comprises a risk assessment tool plus a range of utility functions to help information security managers plan and manage information security;
18. [Delphi](#) is essentially a forecasting technique involving successive rounds of anonymous predictions with consolidation and feedback to the participants between each round. It can be applied to predicting information security risks with no less chance of success than the other methods shown here;
19. [DIY](#) (Do It Yourself) methods - see below;
20. [EBIOS](#) from the Central Information Systems Security Division of France is available in several European languages. There is a [freeware tool](#) supporting the method;
21. **ERA** from Methodware Ltd. supports risk assessments, internal audits, compliance initiatives and corporate governance;
22. **FAIR** (Factor Analysis of Information Risk) is a proprietary information security risk analysis method from Risk Management Insight LLC, partially described in Creative Commons documents;
23. **FIRM\*** (Fundamental Information Risk Management) is described by the ISF as a detailed yet practical approach to develop an 'information risk scorecard'. FIRM is one of the ISF's most successful risk analysis methods. Implementation guidelines are provided;
24. [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;
25. **FRAP** (Facilitated Risk Assessment Process), a qualitative method for assessing information security risks associated with an IT system through facilitated workshops and questionnaires, is described in Tom Peltier's book [Information Security Risk Analysis](#);

26. **GAIT-R** (Guide to the Assessment of IT Risk) is part of the IIA's top-down GAIT method/guidance to identify and assess key IT risks and the associated IT controls within the organization. Unfortunately for the rest of us, it is only available to IIA members :-)
27. **GRC Manager** (Governance, Risk, and Compliance Manager) from Oracle "automates the management of internal controls and improves the efficiency of an organization's compliance processes. GRC Manager monitors business process risk and control performance across the enterprise, automatically highlighting areas of control weakness, and initiating corrective actions with automated loss and investigations management.";
28. **GStool** is software supporting users of the IT-Grundschutz IT Baseline Protection Manual from the German Federal Office for Information Security (BSI) in both German and English;
29. **Iconium Policy Manager** from Logicalis "acts as the glue between all of the steps required to effectively deliver and manage up-to-date policies, procedures and guidelines to the entire organisation";
30. **IRAM\*** (Information Risk Assessment Methodologies) is not itself an RA method or tool but rather an ISF project looking at several RA methods and tools, I think, like the [ENISA project](#);
31. The UK's Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC) and ALARM, The National Forum for Risk Management in the Public Sector, jointly produced [A Risk Management Standard](#) in 2002. It encompasses all forms of organizational risk, not just information security, using terms defined in ISO Guide 73;
32. **IS2ME** (Information Security to the Medium Enterprise) outlines a process designed by consultants Samuel Linares and Ignacio Paredes for evaluating a small-to-medium-sized organization's information security risks in order to derive pragmatic control requirements that can be implemented quite rapidly. The [original](#) is in Spanish;
33. **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;
34. **ISO 31000** is a draft ISO standard based on AS/NZS 4360 and others such as COSO-ERM. When released around mid-2009, it will provide guidelines 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.*;
35. **ISO/IEC Guide 73:2002** "Risk management -- Vocabulary -- Guidelines for use in standards" is not a method or standard but a 16-page glossary of risk-related terms. It was originally written as an internal ISO/IEC guide to encourage the consistent use of terminology by committees writing risk-related standards, but when published found more general acceptance. It *may* be superseded by [ISO/IEC 27000](#);
36. **ISO TR 13335**: this multipartite ISO Technical Report is a precursor to [ISO/IEC 27005](#);

37. **MAGERIT** (Metodologia de Analisis y Gestion de Riesgos de los Sistemas de Informacion) is available for free in Spanish and English;
38. **Marion** is an obsolete risk management method based on [Mehari](#);
39. **Mega Suite** supports the management of audit, risks, controls, incidents, policies, compliance, action plans and metrics;
40. **Mehari** is a free risk analysis and management method in several European languages developed by [CLUSIF](#) (Club de la Sécurité de l'Information Français). The 2010 version adopts terminology and concepts from [ISO/IEC 27005](#), but is presently only available in French (English and Spanish versions are due out later in 2010);
41. **MetricStream** “eases complying with many regulations governing data retention, privacy, confidential information, financial accountability and recovery from disasters [to] reduce the cost of compliance.”
42. **Meycor KP** from Datasec is “specifically designed to develop, implement and host ISO Management Systems, particularly the ISO/IEC 27001:2005 standard [...plus...] Quality and Environmental Management Systems, COBIT, and ITIL to the maintenance of Business Continuity Plans and Security Policies.”
43. **Microsoft’s security risk management guide** consists of a 129-page document and a set of Excel worksheets delivered as a typical Windows installation package. The process (outlined below) combines quantitative and qualitative analysis, Return On Security Investment (ROSI) and other best practices. The Microsoft Security Assessment Tool (MSAT) partially automates the process through more than 200 questions covering infrastructure, applications, operations, and people;



44. **Modulo Risk Manager** supports GRC programs from gap analysis and risk assessment through to ongoing operations and management;

45. **NetChk Compliance** from Shavlik “automates the management of critical system and security configuration settings on your network - while mapping those settings back to stated security policies and compliance requirements”;
46. **NetIQ** tools support security and compliance management, largely by consolidating and analyzing vulnerabilities and log information from IT systems and other tools;
47. [NIST SP 800-30](#) “Risk Management Guide for Information Technology Systems” is a free 55-page PDF download;
48. [NIST SP 800-39](#) “Managing Risk from Information Systems - An Organizational Perspective” is currently available as a draft (published April 2008);
49. **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for security, owned/managed by CERT. It takes a business rather than technology-centric view of security risks. [OCTAVE Allegro](#) is, as the name suggests (to musicians if not the unfortunate owners of possibly the worst British car model ever produced by Austin!), a quick version of OCTAVE;
50. **Paisley GRC** products from ThomsonReuters “provide unique profiles for each user group, a central data repository and common functionality for risk assessment, reporting and issue tracking across GRC disciplines”;
51. **PCR** (Perceived Composite Risk) by professors Bodin, Gordon and Loeb in Communications of the ACM, volume 51 number 4 (April 2008) uses the Analytic Hierarchy Process, taking into account the expected loss (similar to ALE), the expected severe loss (worst case scenario), and the standard deviation of loss (reflects inaccuracies in the analysis) to rank alternative security investments economically.
52. **Polaris** from Brabeion “manages policies, automates IT controls monitoring, and measures what actually occurs against what business policies, internal governance, and regulatory sources demand”;
53. **Proteus Enterprise** is a comprehensive risk management support tool by Information Governance Ltd. and distributed by BSI. In relation to information security, it supports online compliance and gap analyses, business impact and risk assessment, business continuity, incident management, asset management, rôles, policies and action plans, with versions for single users, consultants and enterprises;
54. **PTA** (Practical Threat Analysis) is described by PTA Technologies as “a calculative threat modeling and risk assessment methodology that assist security consultants and analysts in assessing the risks in their systems and building an appropriate risk mitigation policy” [*sic*];
55. **RA2 art of risk** is risk analysis software from Aaxis that claims to be “more than just a risk assessment tool - it covers a number of security processes that direct businesses towards designing and implementing an ISMS”;
56. **Risicare** software supports French-speaking users of the *Mehari* method;
57. **Risk Asset Professional (RAP)** and **Compliance Assessment Professional (CAP)** products from Consult2Comply support information security risk/compliance assessments and management reporting;

58. **RiskClipper** from Maximus “is envisioned to be the tool for holistic enterprise risk management” according to the sales blurb, a lofty claim indeed but it must be OK because it uses “a radical methodology” ...;
59. **Risk Commander** from Cybertrust had modules aimed specifically at supporting risk analysis, compliance and management in financial and health organizations. Since Cybertrust was taken over by Verizon Business, the product seems to have disappeared;
60. **Risk IT** from IT Governance Institute/ISACA is similar to [COBIT](#) and [Val IT](#), but focuses on the management of risk;
61. **Risk Manager** from Modulo is a decision support tool supporting compliance, gap and risk assessments against a variety of IT security-related laws, regulations and standards using a database of around 10,000 information security controls (!);
62. **RiskOptix** from Chapman Technology Group Inc. is another decision support tool aimed at risk assessment, with a Web front end and Excel back end;
63. **RiskPAC** from CPACS LLC provides a framework for collating and assessing the results of risk assessment questionnaires to recommend possible controls, particularly in relation to business continuity;
64. **Risk Reporter** from ACR2 is aimed primarily at assessing and collating information on risks relating to FISMA compliance, but also covers HIPAA and others;
65. **RiskVision GRC** from Agilience supports the management of policies, compliance, enterprise risk, vendor risk, threats and vulnerabilities, and privacy;
66. **Riskwatch** “software programs do the entire risk assessment for you making it easy to incorporate governance, risk and compliance into management initiatives”;
67. **RM Studio** is a product from Icelandic company Stiki;
68. **RSAM** from Relational Security Corporation is yet another decision support tool for risk assessment;
69. **SARA\*** (Simple to Apply Risk Assessment) from ISF does what it says on the tin in four phases: planning; identification of business security requirements; vulnerability assessment and control requirements; and reporting;
70. **SecureVue** from eiQ Networks claims strengths in information security policy management, communications and operations security and compliance. The tool’s database holds over 5,000 technical and functional controls (!);
71. **Security Risk Management Toolkit** is a collection of documents, spreadsheets *etc.* supporting information security risk analysis;
72. **SmartSuite** from Archer Technologies supports “processes for managing the lifecycle of corporate policies and objectives, analyzing and managing risks to your business, and demonstrating compliance”;
73. **SOMAP** (Security Officers Management and Analysis Project) offers an open source [infosec risk assessment guide](#) and [infosec risk management handbook](#);
74. **Spectra** from Compliance Spectrum supports compliance with a raft of information-security related laws, regulations and standards, including policy management, compliance audits and evidence management;

75. **SPRINT\*** (Simplified Process for Risk Identification) from ISF is intended to be a quick and easy methodology for assessing information security risks and proposing controls for 'important but non-critical systems' (SARA is better suited to critical systems);
76. **STAR** (Security Targeting and Analysis of Risks) is a method developed for the IT Security function at Virginia Tech - click their [Next:resources](#) link to access the explanatory files, forms and spreadsheets;
77. **Stochastic** modeling methods using [Markov chains](#), stochastic [Petri nets](#), [Monte Carlo simulation](#), [Bayesian](#) or other statistical techniques and probability theory are commonly applied to estimate uncertain risk values from incomplete data in the financial industry, but have some potential for systematically examining information security risks;
78. **Verinice** is a free open source tool for a variety of platforms supporting ISMS implementation and operations using the [BSI IT-Grundschutz standards](#), currently only available in German;
79. **Visible Security** from Security Works supports risk profiling, security policy, security assessment and security metrics/reporting activities, taking a comprehensive approach to information security risk management;
80. **vsRisk** risk analysis software from Vigilant Software supports ISO/IEC 27001.

\* Most ISF (Information Security Forum) materials are only available to ISF members :-)

If you are confused at which way to turn, [ENISA's standardized comparison of risk analysis and risk management methods and tools](#) might help (browse the selection from the left hand menu). We are not recommending the methods and products/tools listed above, merely providing some options for your consideration. If you know of other information security risk analysis tools, products and methods worth including (for free!) in this FAQ, please [get in touch](#).

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

That said, be wary of naive attempts to quantify and compare risks mathematically for example using simple products of risk factors such as threat, vulnerability and impact values, or worse still summing those values. This is all figurative, informal arithmetic, not

mathematically let alone scientifically sound by any means. There are problems as a result of:

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

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

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

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

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

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

- **Quantitative or qualitative:** opinions vary on the relative value of quantitative *versus* qualitative methods. Few information security or risk management professionals would recommend truly quantitative analysis of information security risks in all circumstances due to the shortage of reliable data on incidents (probabilities and impacts), although they are potentially useful in some more narrowly-defined situations. One solution to this dilemma is to use quick/simple qualitative risk assessments followed by risk analyses on selected 'high risk' areas using more detailed qualitative or quantitative methods;

- **Scope:** are you purely looking at “information security risks”, or risks in a broader sense, and what do you understand by “information security risks” anyway? Which information assets are you concerned with? These questions are very much linked to the scope of your ISMS and need to be thrashed out by management in order to compile your Statement Of Applicability (SOA);
- **Scaleability:** are you looking to support a relatively simple analysis of risks for a single process or IT system, an organization-wide analysis, or all of the above? Will you be completing the analysis just once or repeatedly, and if so how often? If you intend to gather and analyze vast amounts of data over time, you will probably prefer tools based on databases rather than spreadsheets;
- **Maintainability and support:** some methods use clever decision support software to support those undertaking the analysis, whereas others are procedural or can be supported by generic tools such as spreadsheets. Clearly, therefore, they vary in the amount of technical expertise required to install, configure and maintain them. Home-grown tools can be more easily and cheaply modified in the light of your experiences compared to commercial tools (at least until the original developer departs, unless he/she made a conscious effort to document the system!) whereas commercial tools tend to be slicker and more polished. Commercial software having flexibility as a key design goal may give the best of both worlds;
- **Usability:** some methods and tools lead the user through the risk analysis process a step at a time, whereas others are more free-form but arguably assume more knowledge and expertise of the users. Some attempt to reduce the information gathering phase to simplistic self-completion questionnaires for risk non-specialists, others require competent risk analysts to collect the data;
- **Value:** by this we mean the benefits to your organization from the tool, offset by the costs of acquiring, using and maintaining the tool. *Purchase price is just one factor.* An expensive tool may be entirely appropriate for an organization that will get loads of value from the additional features. A cheap or free tool may prove costly to learn, difficult to use and limited in the features it offers ... or it may be absolutely ideal for you. Your value judgment and final selection is the end result of the evaluation process. You may even decide to adopt more than one for different situations and purposes!

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Compliance audits are a particular type of audit that assess the extent to which the in-scope processes, systems *etc.* comply with applicable requirements or meet their obligations laid down in laws, regulations, policies and standards. In the case of ISMS certification audits, for instance, certification auditors from an accredited certification body check that the ISMS complies with and fulfils the requirements in [ISO/IEC 27001](#). There is also an element of risk

assessment in compliance audits, however, since noncompliance can vary in gravity between purely inconsequential (e.g. trivial spelling mistakes in information security policies) and highly material (e.g. a complete lack of documented information security policies). Issues at the lower end of the scale (as determined by the auditors) may not necessarily be reported while those at the higher end will definitely be reported to management and will probably result in a refusal to certify the ISMS compliant until they are adequately resolved.

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

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

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

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

But that is not to say that risk assessment, measurement and comparison is totally pointless, rather that the results should be treated with a great deal of caution since there are clearly significant margins for error. Large differences in calculated probabilities or impacts of certain information security risks and incidents may be meaningful, whereas small differences may not. Where you draw the line between big and small is down to your own experience in this area, your trust in the numbers and analysis, the reasons for differentiating them, and gut feel.

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

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

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

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

A: Yes, in fact there are several. [ISO27k Forum](#) members have used the following:

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

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

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

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

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

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

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

**Implementation tip:** third party security testers, like IT auditors, are independent of the organization and hence often see things in a new light. They bring experience and knowledge of the outside world. This is a valuable perspective that insiders lack, so don't just dismiss what they tell you out of hand without considering it properly and ideally discussing it openly with them. However, their independence means they may not fully appreciate the business context for information security, for example competing investment priorities. It is your management's role to take decisions and allocate resources in the best interests of the organization, so give them the information to help them do their job.

---

## Certification against ISO/IEC 27001

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

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

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

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

[ISO/IEC 27001](#) lays out a formal specification for an ISMS, with the emphasis very much on ‘management system’ rather than ‘information security’. The management system element of an ISMS is more easily specified in a generic yet formal way than the information security controls, and therefore ISO/IEC 27001 is the standard against which organizations are formally certified (see below).

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

**Implementation tip:** read the standards!

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

**A:** DNV has a helpful [overview of the process](#).

First obtain and read the standard. We recommend obtaining [ISO/IEC 27000](#) (provides a glossary of terms and an outline of the whole ISO27k series, useful for explaining them to management), [ISO/IEC 27001](#) (the ‘certification standard’ which summarizes the process of implementing an Information Security Management System ISMS) plus [ISO/IEC 27002](#) (which gives more detail on the nature of the ISMS). ISO/IEC 27002 contains a reasonably comprehensive set of 39 key control objectives for information security and lists a whole load

of good practice security controls that are commonly used to satisfy those control objectives. I tend to speak of ISO/IEC 27002 as a menu of information security controls from which you need to pick your meal. You make your order (select the specific controls) using a risk analysis process which is briefly mentioned in section 4 of the standard, and is covered in more detail in yet another ISO/IEC standard, [ISO/IEC 27005](#).

Next you need to plan and conduct some form of information security risk analysis. In reality, you first need to set the scene with management and then line the relevant parts of the organization and people up to ensure they engage with the risk analysis process. They need to be reasonably open to the concept of improving their information security controls and you will probably need to engage suitable risk/security experts to make this process as painless and effective as possible (hopefully you are lucky enough to have the resources on board already, otherwise you have to choose between building the competence in this area or buying-in expertise in the form of contractors/consultants). The risk analysis may be called a 'gap analysis' or 'ISO27k review' since it may make sense to compare your existing controls against the advice in the standard, looking for weaknesses and omissions as you go, or you may prefer to do a zero-base risk analysis, assuming that there are not controls in place. The advantage of the latter approach is that you might identify unnecessary controls that can perhaps be deinstalled later.

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

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

With management backing, you now implement the security improvements. Easier said than done! It could be a mere formality if your setup is already very security aware and competent in this area. It could be an extremely arduous job if you are starting from a low base, such as an organization which has habitually underinvested in information security, has made strategic changes in its use of, and dependence on, IT (e.g. it has started using the Internet for business processes/transactions and communications, rather than simply for promotional

websites), or where there are no clear accountabilities for information security. It is impossible for me - or indeed for you - to say how long or how costly this phase will be for you until you have completed the previous steps, and even then you can only estimate.

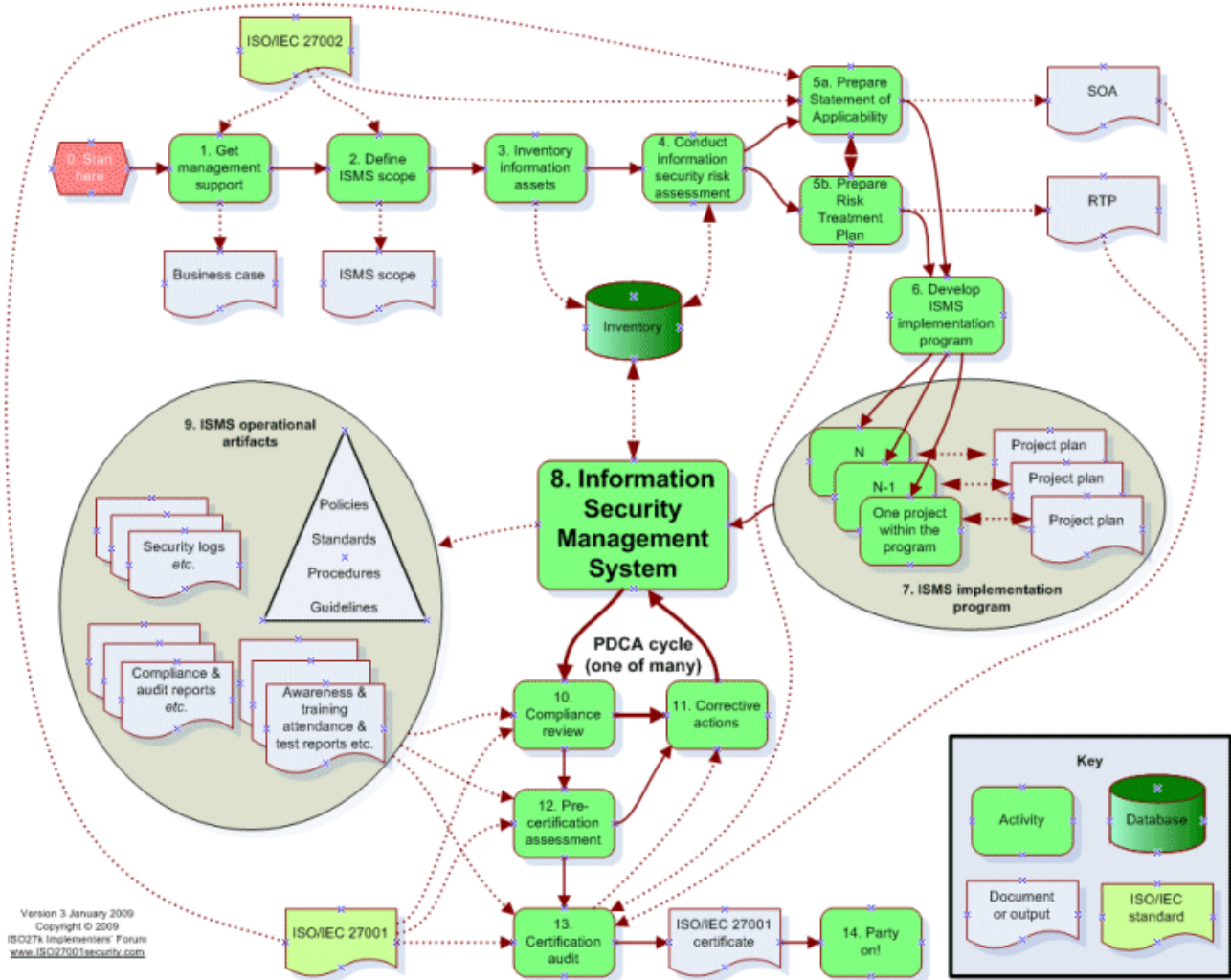
With the improvements well under way and security gradually becoming an inherent part of business-as-usual, it's time to think forward towards ISO/IEC 27001 certification. Like other management systems standards from ISO, ISO/IEC 27001 is process-focused - it helps set up a management system for information security comprising a suite of management processes loosely relating to the Plan-Do-Check-Act Deming cycle normally found in ISO 9000 quality management systems.

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

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

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

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



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

1. **Get management support** - easier said than done! This typically involves raising management's awareness of the costs and benefits of having a [ISO/IEC 27001](#) compliant ISMS. A great way to start is to raise management's awareness of some of the key current information security risks and potential good practice controls (drawn from [ISO/IEC 27002](#)) that are not yet in place, perhaps through a "gap analysis" (outline risk assessment) followed by a business case and/or strategy for the security improvement (ISMS implementation) program.
2. **Define ISMS scope** - what businesses, business units, departments and/or systems are going to be covered by your Information Security Management System?

3. **Inventory your information assets** - the inventory of information systems, networks, databases, data items, documents *etc.* will be used in various ways *e.g.* to confirm that the ISMS scope is appropriate, identify business-critical and other especially valuable or vulnerable assets *etc.* (more below)
4. **Conduct an information security risk assessment** - ideally using a recognized formal method but a custom process may be acceptable if applied methodically. More advice below.
5. (a) **Prepare a Statement of Applicability** - according to [ISO/IEC 27000](#), the SoA is a “documented statement describing the control objectives and controls that are relevant and applicable to the organization’s ISMS”. Which of the control objectives from [ISO/IEC 27002](#) are applicable to your ISMS, and which are irrelevant, not appropriate or otherwise not required? Document these management decisions in your SOA; and in parallel ...  
(b) **Prepare Risk Treatment Plan** - [ISO/IEC 27000](#) describes the information security RTP as “a plan that identifies the appropriate management actions, resources, responsibilities, timeliness and priorities for managing information security risks”.
6. **Develop ISMS implementation program** - given the scale, it is generally appropriate to think in terms of an overall program of individual projects to implement various parts of [ISO/IEC 27002](#), for example one project for each of the main sections of the standard. Which resources can you call upon, direct, use, borrow or persuade to build or supplement your core ISMS implementation team? You will probably need experienced information security professionals (particularly to lead the team) and support from a variety of related functions such as Internal Audit, Risk, Compliance, HR, Finance and Marketing, not just IT. You are advised to plan the work in risk-priority-order where possible *i.e.* tackle the biggest risks early so that, whatever happens to your program of work in practice, it has had a good go at knocking down the main issues and can demonstrate real progress, even if it then falters for some reason. Also, early wins are a source of helpful positive feedback: this is an important aspect to the program which as to be seen to be effective by management, as well as actually being effective. If all the program does is interfere with business, annoy managers and cost a packet, it is hardly going to be on the shortlist of “things we really must keep doing next year”!
7. **Run the ISMS implementation program** - through the individual project plans, the implementation team sets to work to implement the controls identified in the RTP. Conventional program and project management practices are required here, meaning proper governance, planning, budgeting, progress reporting, project risk management and so forth. If the program is large, seek professional program management assistance.
8. **Operate the ISMS** - as each project in the program fills in part of the ISMS, it hands over a suite of operational security management systems and processes, accompanied by a comprehensive set of policies, standards, procedures, guidelines *etc.* *Operating the ISMS has to be an ongoing routine activity for the organization: this is not a one-shot project!* The Information Security Management function needs to be established, funded and directed, and many other changes are likely to be required throughout the organization as information security becomes part of the routine.

9. **Collect ISMS operational artifacts** - 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 artifacts are crucial evidence that the ISMS is operating correctly. You need to build up sufficient artifacts to prove to the auditors that the system is operating, stable and effective.
10. **Review compliance** - are you actually doing what you said you were going to do? Section 15 of [ISO/IEC 27002](#) covers compliance with both internal requirements (corporate policies *etc.*) and external obligations (such as laws and industry regulations). The ISMS itself needs to incorporate compliance testing activities which will generate reports and corrective actions. Internal compliance assessments, and perhaps external/independent assessments (audits, penetration tests *etc.*) are therefore routine activities in a mature ISMS. The ISMS operational artifacts produced in step 9 are a major source of evidence for such compliance activities - they give the auditors something to test.
11. **Undertake corrective actions** - to improve the ISMS and address risks. The “Plan-Do-Check-Act” Deming cycle is central to the ‘management system’ part of ISMS and should result in continuous alignment/re-alignment between business requirements, risks and capabilities for information security. As with quality management systems, the idea is to give management a means of controlling information security management processes systematically such that they can be continually monitored and improved, not least because perfect security is an unattainable goal in any real world situation.
12. **Conduct a pre-certification assessment** - when the ISMS has stabilized, an accredited certification body or other trusted, competent and independent advisor is invited by management to check whether the ISMS is functioning correctly. This is largely a compliance assessment but should ideally incorporate some independent review of the scope, the SOA and RTP to make sure that nothing important has been missed out of the ISMS, especially as the business situation and information security risks have probably changed in the months or years that it will have taken to implement the ISMS. It is a golden opportunity for your organization to identify and tie up any remaining loose ends before the actual certification audit. It’s also a good low-impact way to get to know the auditors.
13. **Certification audit** - when management is happy that ISMS is stable and effective, they select and invite an accredited certification body to assess and hopefully certify that the ISMS complies fully with [ISO/IEC 27001](#). The auditors will check evidence such as the SOA, RTP, operational artifacts *etc.* and will attempt to confirm that the ISMS (a) is suitable and sufficient to meet the organization’s information security requirements in theory *i.e.* it is correctly specified; and (b) actually meets the requirements in practice *i.e.* it is operating as specified.
14. **Party party** - seriously, when it’s all over, celebrate your success. You’ve earned it! More than that, your [ISO/IEC 27001](#) certificate is a valuable asset. The organization should be proud of what it has achieved, knowing of course that information security is never really “done”. With your certified ISMS operating normally, take a good look at the information security arrangements in place at your supply chain: are your suppliers,

partners and customers also certified? Are they certifiable? Do they need your encouragement? If you haven't already done so, please join the [ISO27k Forum](#) to share your experience with others who are in the process.

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

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

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

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

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

**A:** ANY certification bodies, registrars or whatever they are called, who have been properly accredited by their ISO/IEC-recognised national standards bodies' accreditation services are empowered to assess organizations for compliance with [ISO/IEC 27001](#) and grant recognized certificates of compliance. This is the beauty of international standards and the formal accreditation processes operated by ISO/IEC and the national standards bodies.

"Accredited" means their certification practices have been checked to ensure that the certificates issued are legitimate, trustworthy and meaningful. If just anyone could issue certificates, the certificates and hence ISO27k as a whole would soon lose value and be discredited. The formality in the process builds and maintains confidence and trust.

Individual auditors are accredited by 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.

The UK Accreditation Service (UKAS) maintains a partial list of [certification bodies that are accredited to certify against ISO/IEC 27001](#) - check the final column in the table. The German equivalent of UKAS is [TGA](#), and in the US it's American National Standards Institute (ANSI), though ANSI has delegated this to the [American Society for Quality National Accreditation Board](#) (ANAB). For other countries, see [here](#).

You can cross-check using the [register of ISO/IEC 27001 certificates](#) which identifies the accredited bodies that issued the certificates, and has a separate list of them [here](#).

If you know of other properly-accredited ISO/IEC 27001 certification bodies, please [let us know](#).

As to whether a given accredited certification body or auditor will be keen to travel to your particular location to do the certification audits, however, I guess that depends on the \$\$\$ on offer. The accreditation process (*i.e.* checking that certification bodies are competent and suitable to assess clients against [ISO/IEC 27001](#)) is itself the subject of [ISO/IEC 27006](#).

**Implementation tip:** it's a free market so shop around. The formalized accreditation process means that there is no harm in going to a lesser-known certification body since (in theory at least) they all work to essentially the same quality and performance standards. Remember that ISMS certification bodies are strictly forbidden from also offering [lucrative] ISMS consultancy services to the same clients to avoid the obvious conflict of interest.

**Q:** "How does the certification process work?"

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

1. **Pre-audit** - having engaged an accredited certification body, they will request copies of your ISMS documentation, your policy manual *etc.* and may request a short on-site visit to introduce themselves and identify contacts for the next phase. When you are ready, they will schedule the certification audit itself by mutual agreement.
2. **Certification audit** - this is the formal audit itself. One or more auditors from the accredited certification body will come on site, work their way systematically through their audit checklists, checking things. They will check your ISMS policies, standards and procedures against the requirements identified in ISO/IEC 27001, and also seek evidence that people follow the documentation in practice (*i.e.* the auditors' favorite "Show me!"). They will gather and assess evidence including artifacts produced by the ISMS processes (such as records authorizing certain users to have certain access rights to certain systems, or minutes of management meetings confirming approval of policies) or by directly observing ISMS processes in action.

3. **Post-audit** - the results of the audit will be reported formally back to management. Depending on how the audit went and on the auditors' standard audit processes, they will typically raise the following (in increasing order of severity):
- **Observation** - information on minor concerns or potential future issues that management is well advised to consider;
  - **Minor noncompliance** - these are more significant concerns that the organization has to address at some point as a condition of the certificate being granted. The certification body is essentially saying that the organization does not follow ISO/IEC 27001 in some way, but they do not consider that to be a significant weakness in the ISMS. The certification body may or may not make recommendations on how to fix them. They may or may not check formally that minor noncompliances are resolved, perhaps relying instead on self-reporting by the organization. They may also be willing to agree a timescale for resolution that continues beyond the point of issue of the certificate, but either way they will almost certainly want to confirm that everything was resolved at the time of the next certification visit;
  - **Major noncompliance** - these are the show-stoppers, significant issues that mean the ISO/IEC 27001 certificate cannot be awarded until they are resolved. The certification body may recommend how to resolve them and will require positive proof that such major issues have been fully resolved before granting the certificate. The audit may be suspended if a major noncompliance is identified in order to give the organization a chance to fix the issue before continuing.

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

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

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

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

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

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

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

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

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



## ISMS auditing

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

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

On a more positive note, it makes a nice change for auditors to be “invited” in by their prospective auditees! This could be an ideal opportunity for Internal Audit to get to work on the ISMS and make positive recommendations for improving the organization's information security controls, risk management, compliance and governance (at least within the scope of the ISMS for now), knowing that the implementation team and hopefully management has the incentive to address any issues quickly in order not to stall or preclude the certification. Personally, however, I would be cautious about being too ambitious with your audit at this stage since recommending major changes could be seen as derailing the ISMS project, while

a softly-softly approach would leave the door open for further ISMS audits supporting their PDCA-based internal management review and improvement activities. With an effective ISMS in place, you can expect the information security situation to be more stable as it comes under better management control, and then to improve gradually of its own accord. You have a part to play in making this happen as effectively and efficiently as possible. In particular, your independent viewpoint gives you the advantage of making sure that the ISMS is not blind-sided by some unanticipated issue that the ISMS management team was unaware of, and the chance to promote generally accepted good risk/security management practices based on the standards or other sound sources.

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

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

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

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

want to check the evidence (they may call them “artifacts” or “records”) relating to and proving operation of the information security management processes.

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

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

**Q:** “Will the certification auditors check our information security controls?”

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

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

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

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

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

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

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

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

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

Listen carefully to any summing up or findings or recommendations the auditor makes as there may well be some helpful suggestions about how to improve your ISMS, and if they are stated by an independent, competent external auditor, they tend to carry weight with management. Even if the final audit report officially says "No issues, fully compliant", the

auditor may raise minor concerns, snags or improvement suggestions informally. A good auditor will also compliment your organization on certain aspects of its ISMS, and those kinds of comment make good security awareness materials. It's nice to be given a clean bill of health and to be certified compliant, but a positive comment about something your organization is doing well can really make someone's day!

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

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

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

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

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

1. Check that your **ISMS internal and external audits** are fully up to date, with plans in place for future audits. Are all audit findings/observations, recommendations and agreed actions either completed and closed off, or currently in progress (with clear signs of that actually happening, in practice)? Use the results of recent audits to drive forward any necessary changes and to reinforce the concept that the audits are all about making justified improvements. (It is worth double-checking that any other similar audits covering information security risks, controls and compliance are also addressed.)
2. Collate evidence of continuing **management commitment to the ISMS** such as minutes of management committee meetings, decisions and actions taken, preventive and corrective action plans and the results of follow-up or close-out actions, and budgets.

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

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

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

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

---

-- End of FAQ --

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

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

## Copyright and disclaimer



This work is copyright © 2010, [ISO27k Forum](#), some rights reserved. It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](#). You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum at [www.ISO27001security.com](http://www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.

This document is not legal advice, nor is it information security advice. It is a generic/model document provided for information only that should be tailored to suit individual circumstances. It is provided without any warranty or promise of fitness for purpose. It is incomplete and may be inaccurate and out of date. *Use at your own risk.*