What are ISO Standards? Why are they Important to You?

ISO standards are not just for the large enterprises, they are of benefit to start-ups, micro businesses, SMEs and large undertakings alike.

Some discerning customers such as Government departments, local authorities, blue-chip companies etc require their suppliers to be ISO certified, regardless of the size of the supplier's business. In some cases it is a pre-requisite and your bid could be disqualified if the required ISO certifications are not held.

If you have an ISO certification it tells your customers a lot about your business and gives them an ongoing assurance because maintaining an ISO certification requires ongoing independent auditing to ensure compliance. It allows a small business to 'punch above its weight' when competing with other businesses.

So what are ISO standards and what is needed to become certified?

Firstly - It is not necessary to purchase the standards in order to read them or learn about them. The Manchester Library allows you to view most ISO and British standards online free of charge. Go to:
http://www.manchester.gov.uk/info/200062/libraries/110/online_reference_library/4
Click on 'British Standards Online'. This logs you into the British Standards Online web site where you can view ISO standards. Access is read-only, you can't save, copy or print the standards as that would be a breach of copyright.

There are many ISO standards, covering virtually every business sector and industry type. For ICT businesses the most popular ISO standards are:-

- ISO 9001:2008 – Quality Management System
- ISO/IEC 27001:2013 – Information Security Management System
- ISO/IEC 20000-1:2011 – IT Service Management System
- ISO 22301:2012 – Business Continuity Management System

Depending on the nature of your organisation, the number of employees and the sites you have, you may have obligations for Health & Safety and/or Environmental Management. A few of the relevant ISO standards are:-

- ISO 14001:2004 – Environmental Management System
- OHSAS 18001:2007 – Occupational Health & Safety Management System
- ISO 50001:2011 – Energy Management System

Other popular ISO standards which are relevant include:

- ISO 31000:2009 – Risk Management
- ISO 26000:2010 – Corporate Social Responsibility

An organisation can gain certifications against any or all the above standards apart from ISO 31000 and ISO 26000. These two are for guidance only.

Most of the above standards, which an organisation can be certified against, have one or more associated guidance documents to help you implement a management system which will comply with the standard. e.g. ISO 22313:2012 is the guidance document for the ISO 22301:2012 business continuity standard.

The ISO standards are periodically reviewed and revised. That is why the date at the end of the title is significant. For example, in the list above ISO/IEC 27001:2013 is quite new and supersedes ISO/IEC 27001:2005. Any organisation that is certified against ISO/IEC 27001:2005 must 'transition' to ISO/IEC 27001:2013 before October 2015 – two years after its publication. Two or three years are allowed for businesses to revise their management systems to bring them into line with the new version. The 'transition' occurs at the next ISO audit and a new certificate is issued. Failure to transition and comply in time will result in the certificate being revoked.

The following standards will be superseded with new versions in the next two years:-

- ISO 22301:2012 has recently been superseded by ISO 22301:2014
- ISO 9001:2008 will be superseded by ISO 9001:2015 later this year
- ISO 14001:2004 will be superseded by ISO 14001:2015 later this year
- OHSAS 18001:2007 will be superseded by ISO 45001:2016 next year

If you are currently working towards gaining ISO 9001:2008 certification you should continue with that version until the ISO 9001:2015 version is finalised and published, which is scheduled for release towards the end of 2015. You will then have three years to transition to the new version.

ISO standards are published by the International Organization for Standardization (ISO): www.iso.org
Their web site provides information about the standards and what is changing.

In general, all new ISO standards are being brought into line with something called 'Annex SL'. This simply means that when they are next revised the ISO standards will have the same structure, clause numbering, and have some standard wording regardless of the subject of the standard. This makes it a lot easier for businesses to comply with multiple ISO standards using a common or integrated management system. Once you have gained certification against one ISO standard it is just an incremental amount of effort to comply with another one, not double the effort.

Common themes run through all these ISO standards. They are increasingly becoming risk-based management systems, e.g. managing the risk of an information security breach, managing the risk of not being able to fulfil obligations to customers and managing the risk of a crisis preventing your businesses from operating. Managing risk, as recommended in ISO 31000, is sometimes referred to as Enterprise Risk Management, which underpins compliance with numerous other ISO standards. Another common theme across all these ISO standards is Legal and Regulatory Compliance and compliance with 'other' obligations such as customer contracts, landlord leases and local authority planning consent.

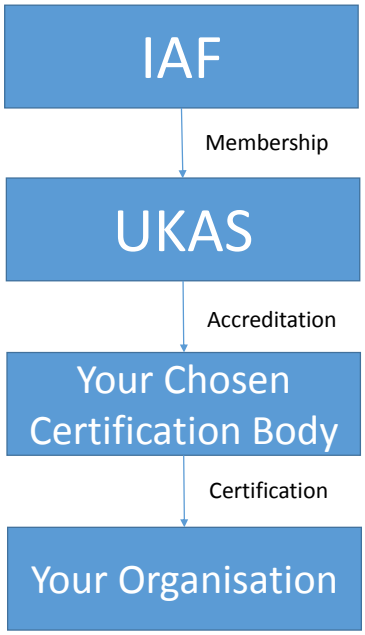
The ISO standards require ISO certified businesses to have a process for ensuring they are aware of and comply with applicable legislation and their other obligations. Relying on a professional law firm to keep you informed about every change to UK legislation is costly so a more cost-effective approach is required. A properly implemented ISO compliant management system helps you remain legal and compliant. Applied Risk Management Ltd provides an 'applicable legislation update service. For further information go to: www.appliedriskmanagement.co.uk

The British Standards Institute (BSI) is the organisation which publishes and sells ISO standards within the UK. BS and ISO standards can be purchased from their online shop: http://shop.bsigroup.com/

Note that if you wish to purchase a number of standards within a year, consider registering as a member of BSI in order to get member discounts. You could recoup the membership fee in the savings made on the purchase price when buying more than (typically) three standards in a year. Note that you don't have to buy the standard to become certified.

If you choose to gain formal certification against an ISO standard, either through choice or to meet a customer contractual requirement, you should use an **accredited certification body** (ACB). There are many companies that offer ISO certification services but only accredited certifications are worth having. If you are offered a very low cost for ISO certification, compared to the big reputable certification bodies, beware as they may not be supplying accredited certifications!

Accreditation is the term used to indicate that an ISO certification body has been audited and 'approved' (hence accredited) to issue ISO certificates. For example, in the UK it is the United Kingdom Accreditation Service (UKAS) that audits the ISO certification bodies and approves them to issue ISO certificates – UKAS audits them against ISO 17021-1:2011 which defines how ISO certification audits are to be conducted. i.e. UKAS audits the auditors, like a regulator.



On a global basis it is the International Accreditation Forum (IAF) that is the overall authority for accreditation. This body ensures standards are implemented consistently on a global basis thus supporting global trade. An accredited certification in one country is just as valuable as an accredited certification any other.

UKAS is a member of the IAF. UKAS is the main body for accrediting (approving) ISO certification bodies to issue ISO certificates in the UK, empowered by law. There are other reputable accreditation bodies in the UK, such as APMG (for ISO/IEC 20000), and there are accreditation bodies based in other countries which are equally reputable.

So if you are looking for a reputable organisation to issue you with an ISO certification you should look at the credentials of the certification bodies you are considering using to check they are accredited. Check they are accredited by an organisation that is a member of the IAF, such as UKAS.

As mentioned above, increasingly, Government departments require their suppliers to be ISO certified by a UKAS accredited certification body. For more information about accreditation and what it means for ISO certification, go to the UKAS web site: www.ukas.com

The UKAS web site lists the names of the ISO certification bodies that are UKAS accredited. It also lists the bodies that have lost their accreditation for various reasons!
So if you want to choose a reputable and respected organisation to audit your business and issue your ISO certifications, which your customers will accept and respect, begin by looking at the list of accredited certification bodies (ACBs) on the UKAS web site.
Note that there are other reputable accreditation bodies in addition to UKAS.

Beware of certification bodies offering unaccredited ISO certifications. You may be wasting your money.

Assuming you have chosen which ISO standard(s) are of interest to you, your business and your customers, and you have chosen a reputable accredited certification body (ACB) to audit your business and issue your ISO certificates, the next step is to get your business ready for ISO certification.

Note that one of the golden rules is that the accredited certification body you use to audit your business and issue your ISO certificates is not allowed to advise or assist you in getting ready for certification. Beware of organisations offering to provide both consultancy and certification!

To get your organisation or business ready for certification you can either read the ISO standard(s) and attempt to make your business compliant yourself, or you can seek assistance from an independent ISO management systems consultant who has experience of defining and implementing ISO compliant management systems. If you have a certification deadline to meet you'll want to get it right first time. ISO 10019 provides guidance on selecting a consultant to help you become certified. As mentioned above, you can read this standard via the Manchester Library's web site.

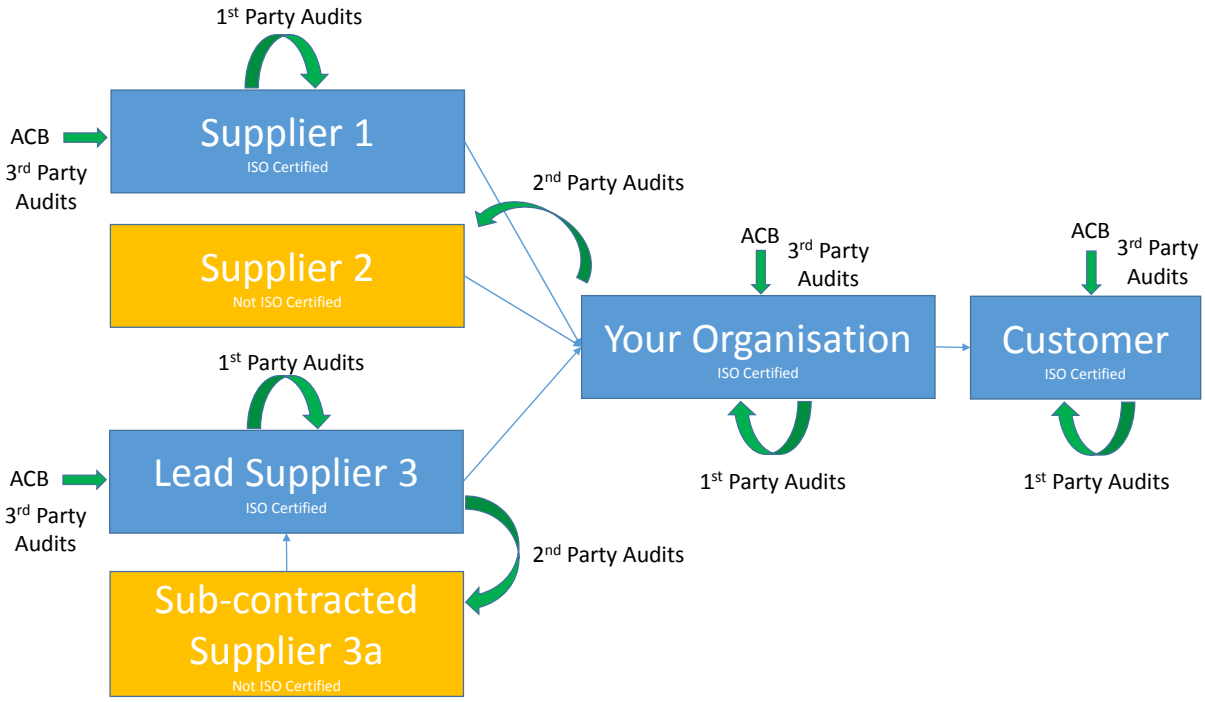
Choosing a reputable consultant to help you define and implement your ISO compliant management system is tricky unless you know what to look for. The International Register of Certificated Auditors (IRCA) was established as a way of registering and approving ISO auditors. The IRCA web site lists the IRCA registered auditors and lets you search for auditors and verify their credentials: www.irca.org
Auditors who are registered by IRCA are bound by the IRCA 'Code of Conduct' which is also available via the IRCA web site.

A mandatory part of gaining and maintaining an ISO certification is Internal Auditing, or 1st party auditing. This is where the ISO certified business checks itself for continued compliance and self-improvement. The ISO standards do not allow a person to audit their own work, so the business needs to have enough people to achieve that, or they can outsource internal auditing to an independent auditor.

Similarly, an ISO certified business has an obligation to manage its suppliers. If the supplier is also ISO certified you could trust that. If they aren't certified you could audit your suppliers but you may prefer to use an independent auditor, particularly for high value supply contracts where an independent view is more likely to be trusted and respected by both parties. Supplier auditing is also called 2nd party auditing.

ISO certification audits by an accredited certification body are usually called external audits or 3rd party audits.

The following diagram shows a typical supply-chain auditing regime:



If you wish to find out more about reputable Accredited Certification Bodies, ISO standards, ISO certifications, ISO auditing (1st, 2nd or 3rd party), Governance, Risk, Compliance, Applicable Legislation Update Services or just need some help defining and implementing effective policies, processes and management systems without going as far as formal ISO certification, contact:

Andrew Mills BSc CEng MIET MBCI IRCA
Applied Risk Management Limited
c/o Ross Building
Adastral Park
Martlesham Heath
Ipswich
IP5 3RE

Mobile: 07773 402952
E-mail: andy.mills@appliedriskmanagement.co.uk
Web: www.appliedriskmanagement.co.uk

Applied Risk Management Ltd can provide ISO standards and management systems consultancy on half-day or daily rates. Contact us now for a no-obligation quote.

An electronic copy of this article, in PDF format, is available free from Applied Risk Management Ltd.

Ask about our Applicable Legislation Update service too!

End