APPLIED RISK MANAGEMENT

ISO Standards & Certification

White Paper

Issue: 6

Date: 19th January 2017

Contents

Company Number: 09299432 Registered in England & Wales
Registered Address: Cardinal House, 46 St Nicholas Street, Ipswich, IP1 1TT
VAT Number: 203 1806 56

0 Document Version Control

Author	Version	Date	Comments
Andy Mills	1.0	20th April 2015	First Issued
Andy Mills	2.0	3rd March 2016	Second issue – updated text
Andy Mills	3.0	4th March 2016	Third issue – context & interested parties
Andy Mills	4.0	15th June 2016	Fourth Issue – link updated
Andy Mills	5.0	26th November 2016	Fifth Issue – link & text updated
Andy Mills	6.0	19th January 2017	Sixth Issue – link & font updated

1 ISO Standards Overview

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

Some discerning customers such as Government departments, local authorities, utility companies, 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, especially when competing globally.

1.1 Where Can I Buy ISO Standards

Firstly - It is not necessary to purchase standards in order to read or learn about them. The Manchester Library allows you to view most ISO and British standards online free of charge.

Go to:
Manchester Library

Click on 'Search British Standards'. 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.

If you wish to purchase your own registered copy of a standard you can buy it as either a hard-copy you receive through the post or a PDF copy you can download.

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. The cost of BSI membership varies depending on the size of your organisation.

Note that you don't have to buy the standard to become certified.

2 What Are ISO Standards

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

- ISO 9001:2015 – Quality Management System
- ISO/IEC 27001:2013 – Information Security Management System
- ISO/IEC 20000-1:2011 – IT Service Management System
- ISO 22301:2014 – 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. Some of the relevant ISO standards are:-

- ISO 14001:2015 – Environmental Management System
- OHSAS 18001:2007 – Occupational Health & Safety Management System
- ISO 50001:2011 – Energy Management System

Note that OHSAS 18001 is about to be superseded by:-

- ISO 45001:2017 – Health & Safety Management System

An organisation can gain certifications against any or all the above standards.

Other popular BS and ISO standards include:-

- ISO 22313:2014 – Business Continuity Management System Guidance
- ISO 31000:2009 – Enterprise Risk Management Guidance
- ISO 26000:2010 – Corporate Social Responsibility Guidance
- ISO/IEC 27002:2013 – Information Security Management System Guidance
- ISO/IEC 20000-2:2011 – IT Service Management System Guidance
- OHSAS 18002:2008 – Occupational Health & Safety Management System Guidance
- BS 8543:2015 – Complaint Handling
- BS 7858:2012 – Security Screening

These 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 compliant management system. e.g. ISO 22313:2014 is the guidance document for the ISO 22301:2014 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 9001:2015 is quite new and supersedes ISO 9001:2008. Any organisation that is certified against ISO 9001:2008 must ‘transition’ to ISO 9001:2015 before September 2018 – three years after its publication. Two or three years are allowed for businesses to revise their management systems to bring them into line with a new version. The ‘transition’ usually occurs at the next ISO audit and a new certificate is issued. Failure to transition and comply in time will result in the ISO certificate being revoked. Similarly, ISO 14001:2004 has been superseded by ISO 14001:2015.

2.1 International Organization for Standardization

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.

All new and revised 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 high level structure, clause numbering, and have some common 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 with your obligations.

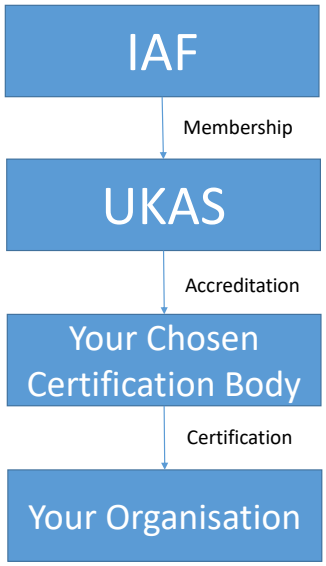
Applied Risk Management Ltd provides an 'applicable legislation' update service for a nominal annual fee.
For further information go to: www.appliedriskmanagement.co.uk

2.2 Accreditation

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 is the only Government appointed authority that audits the ISO certification bodies and approves them to issue ISO certificates – UKAS audits them against ISO 17021-1:2015 which defines how ISO certification audits are to be conducted.
i.e. UKAS audits the auditors and grants/revokes accreditations, a bit like a regulator.

Choosing an ISO certification body is like choosing which University to go to. You want one that is globally respected so your certificate is recognised and means something, globally.



On a global basis it is the International Accreditation Forum (IAF) that is the overall authority for standards accreditation. This body ensures standards are implemented consistently on a global basis thus supporting global trade. Their aim is for an accredited certification in one country to be just as respected as an accredited certification in any other. Each country has only one Government-appointed accreditation body.

UKAS is a member of the IAF and empowered by UK Law for accrediting (approving) ISO certification bodies to issue ISO certificates in the UK.

Note: There are other reputable accreditation bodies in the UK, such as APMG (for ISO/IEC 20000-1), and there are accreditation bodies in other countries which are equally reputable, such as ANAB in USA.

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 body 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 and blue-chip companies 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

Also see the GOV.UK article on un-accredited certification:
BIS policy on unaccredited certification

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 (name and shame)!

So if you want to choose a reputable and globally respected organisation to audit your business and issue your ISO certifications, which all 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 but it is a 'buyer beware' market because some are not as well respected. Also be aware of certification bodies offering unaccredited ISO certifications – so-called 'independent' certification bodies. You may be wasting your money if your customers don't accept or recognise your certification.

2.3 Getting Ready for Certification

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, other than doing one gap-analysis (pre-assessment) visit. An ISO auditor must declare any conflicts of interest.

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 free of charge 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 globally. 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.

ISO standards are deliberately generic to allow any type of organisation to be compliant. They tell you what to do, not how to do it. This is where an experienced ISO consultant can help. Knowing 'what good looks like', knowing the ISO terminology and having relevant industry experience are key elements of effective implementation. A consultant can advise you on what works and what doesn't based on experience. ISO standard use a particular set of terminology which a good consultant can interpret for you.

If you wish to be certified against multiple ISO standards you could integrate your management systems, thus achieving administrative efficiencies. PAS99 refers. ISO standards based on Annex SL are easier to integrate into an Integrated Management System (IMS).

The starting point for management systems complying with Annex SL is determining the Context of your organisation and identifying the Interested Parties. The Context is the 'market' and 'countries' you operate in, what you do and the issues you need to address. The Interested Parties are your customers, suppliers, staff, investors, landlord, etc. These Interested Parties have needs and expectations which your management system is required to address, be it quality, security, safety, etc. This is the foundation upon which to build your management system and identify the risks that need to be addressed.

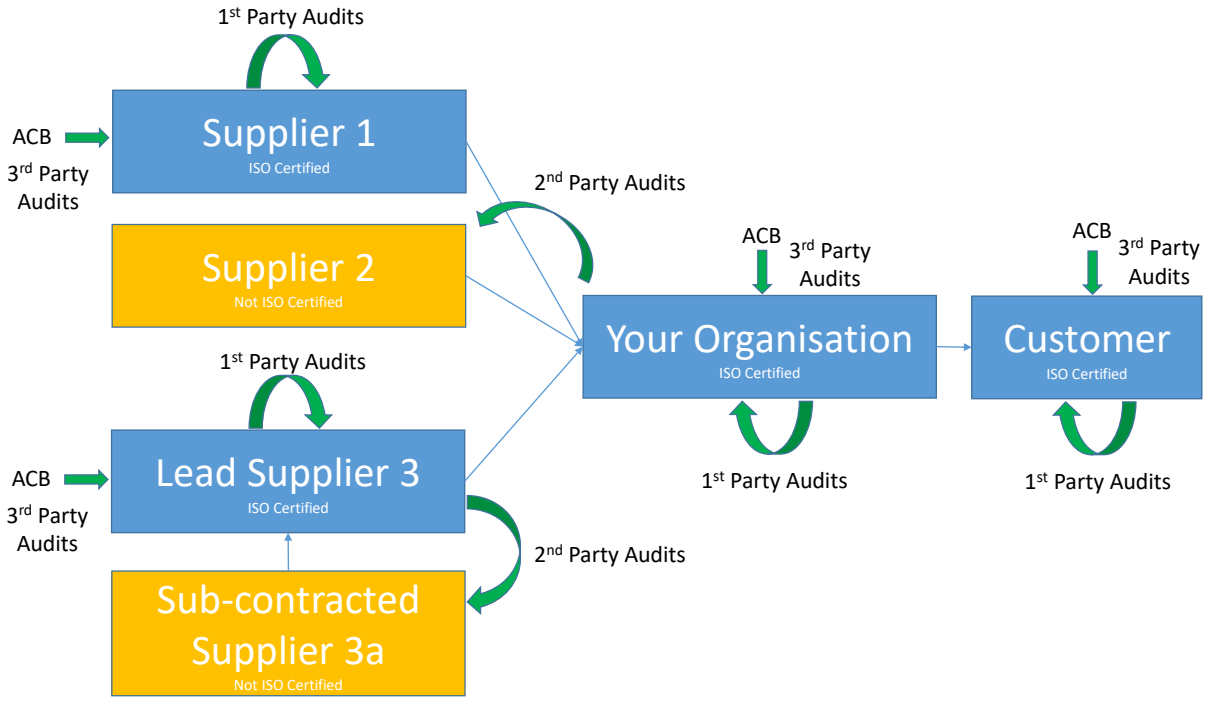
2.4 Audit

A mandatory part of gaining and maintaining an ISO certification is Internal Auditing (1st party auditing). This is where the ISO certified business checks itself for continued compliance and self-improvement. Internal auditors need to be impartial, objective and not audit their own work, so your business needs to have enough people to achieve that, or you can outsource internal auditing to an independent auditor i.e. a consultant.

Similarly, an ISO certified business has an obligation to manage its suppliers. If the supplier is also ISO certified you could trust that, so long as it is an accredited certification. 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. (2nd party audits).

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

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



If the customer is an ISO certified organisation they will require their supplier's organisations to be managed effectively to minimise risk to the supply-chain. This can be achieved by due-diligence checks and/or ISO certification. They may insist on their supplier being certified against one or more ISO standards and write that into the supply contract.

If you are faced with that situation you could do likewise and place contractual obligations upon your suppliers to be ISO certified too. If you are unable or unwilling to do that you could use non-certified suppliers and ensure their integrity by other means, such as 2nd party auditing. If you wish you could conduct 2nd party audits on your supplier's supplier if they are not ISO certified.

A systematic regime as described above ensures supply-chain integrity via effective governance, risk and compliance.

2.5 Certification Cycle

To gain and maintain an ISO certification the organisation must go through regular 3rd party audits.

The starting point is usually a 'gap-analysis' (pre-certification) audit. This helps you determine whether all the requirements of the ISO management system are in place. It is usually an informal audit used to determine the state of readiness for certification. Your ACB is only allowed to perform one gap-analysis (pre-certification audit) otherwise it could be regarded as consultancy.

The first stage of the formal ISO certification audits is the document review. This is known as the Stage 1 audit. An auditor from your chosen accredited certification body (ACB) will visit your site(s) to review your management system policies and processes to confirm they cover all the requirements of the ISO standard. The auditor will also determine whether you are ready for the Stage 2 certification audit, or believes you will be ready by the date of the Stage 2 audit. You need to aim to have three months of operational records available by the date of the Stage 2 audit. You must also have made some progress towards your objectives, conducted at least one internal audit and a management review. Note: ISO standards define what an internal audit and management review are.

The Stage 2 audit is where the auditor sees your management system in operation. The auditor will be looking at your operational records, objectives, management review records, internal audit reports, etc. You must have these in place before the Stage 2 audit, therefore you need to have been running your management system for a while before you undergo the Stage 2 audit.

If the auditor is satisfied you are compliant with the ISO standard and are operating an effective management system you will be issued with an ISO certificate a few weeks after the Stage 2 audit. The Stage 1 and Stage 2 audits assess your intent, implementation and management system effectiveness.

If the auditor finds non-conformities during the Stage 1 audit you will have until the date of the Stage 2 audit to correct those. They will be reviewed and hopefully closed-out during the Stage 2 audit.

If the auditor finds non-conformities during the Stage 2 audit there will be either of two outcomes:-

- If the non-conformity is classed as 'minor' you may still be recommended for certification
- If there is a 'major' non-conformity or there are multiple 'minor' non-conformities you will be required to correct those before being recommended for certification. A further audit may be required to allow the auditor to check that the non-conformities have been addressed before recommending your organisation for ISO certification

Note: These requirements differ slightly between ACBs.

An accredited ISO certificate is granted for three years, subject to maintaining your compliance. The scope of certification and renewal date are stated on the certificate.

Once you have gained your ISO certification, your ACB is required to conduct regular surveillance visits. For a newly certified organisation the surveillance visits may be six-monthly, to begin with. Once your ISO compliant management system is proven to be 'self-improving' your ACB may be happy to reduce the frequency of the surveillance to annual visits.

At the end of the three years you will be required to go through a re-certification audit. This is equivalent to the Stage 1 document review and the Stage 2 certification audit combined, so is more thorough than the surveillance visits, but the time allowed is typically 2/3rds that allocated for the combined Stage 1 and 2. On successful completion you will be issued with a new ISO certificate stating the next renewal date. For some standards the re-certification could be done by Strategic Review. You ACB will advise you if this is relevant for your organisation.

Failure to maintain ISO compliance could result in your ACB withdrawing your ISO certification at any time during the three year cycle. For example, your auditor could find a major non-conformity during a surveillance visit. If you fail to correct that non-conformity within an agreed timescale (typically 3 months) your certification could be withdrawn. If your customer(s) complains to your ACB, your ACB may need to conduct an additional audit to determine whether there is a non-conformity.

"It is not enough to do your best; you must know what to do, then do your best"
W. Edwards Deming

3 Getting Further Information

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:

Andy Mills BSc CEng MIET MBCI
Applied Risk Management Limited
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 and/or 1st and 2nd party auditing. Contact us now for a no-obligation quote.

Ask about our Applicable Legislation Update service too!