The International Organization for Standardization (ISO) produces thousands of standards every year covering multiple topics and disciplines. A certain group of those standards known as management system standards are designed to support organizations in delivering products and services which are higher in quality, safer, more secure, more resilient, and environmentally friendly.

These standards are well known such as ISO 9001 (Quality Management), ISO 27001 (Information Security), ISO 14001 (Environmental), ISO 22301 (Business Continuity) and the soon to be launched ISO 45001 (Health and Safety).

Some organizations are required to implement these standards and some others to demonstrate their compliance to them. Within the industry there is a lot of “noise” about compliance, certification and accreditation, and the difference between these terms. So what do they actually indicate in reality?

**Compliance**

Any organization can choose to implement a management system standard and use the standard to drive improvement and manage risk. They can choose to meet the requirements and perform internal audits as part of their overall management system. When an organization implements such standards there are no mandatory requirements (demanded by the standards themselves) to undergo an external audit. Essentially any organization can implement the standard and claim to be compliant.

Customers of such organizations may ask that their suppliers meet certain standards and in some cases suppliers may simply state that they are compliant, however, some customers may go one step further and ask for evidence or choose to audit their supplier. For organizations with multiple customers this could certainly be a large burden having to handle multiple customer audits through the year. This costs time, resources, and often coinage to produce the same evidence time after time.

**Certification**

Certification to ISO standards for an organization is simply a way of proving that an organization does indeed comply with the relevant standard(s). It does not involve implementing extra requirements or controls, and if an organization has already become truly compliant, certification should be a simple next step.

Certification involves an audit being performed by an independent organization known as a certification body. A certification body will usually perform an audit over two stages. Stage one is a high level review of the management system, whereas stage two is used to look at the management system in much closer details to provide evidence of compliance in various areas.

A good certification body and their auditors will approach the audit from a positive perspective, attempting to find evidence of conformity and are not in the business looking to “catch people out” or to deceive people. In the event that non-conformities are found (by failing to fulfil requirements of the standard), then agreements can be made on how this will be addressed, which in some cases may need a re-visit and in others it may be acceptable to correct the non-conformity over a longer period of time.

If an organization meets the requirements and is recommended for certification, then the certification is awarded for a period of three years. During that time the organization must undergo annual surveillance audits. Surveillance audits are much smaller than the original audit and are designed to check whether the organization is maintaining and improving its management system.

**What are the benefits of being certified?**

If an organization has taken the time to become compliant then getting certified can have the following benefits:

- The organization can easily prove compliance to customers and interested parties
- The organization is independently recognised for its efforts
The level of auditing from customers can often be significantly reduced as independent certification can increase assurance.

Many organizations are now demanding that their suppliers are certified to ISO standards.

How do we choose a good certification body?

There are many factors to take into consideration but first we should describe an important matter. There are no rules or laws preventing anyone from setting up a company and calling it a “certification body” and awarding certificates. So how can we be sure that a certification that has been awarded by a “certification body” is credible and reliable?

One response is accreditation. In order to demonstrate that their certification processes are fair, credible, and trustworthy, certification bodies should follow a standard known as ISO 17201. ISO 17021 lays out how a certification body should operate in order to provide confidence in the certifications they award.

When a certification body is compliant to ISO 17021, they can be audited and accredited by an accreditation authority. Most countries around the globe have a national accreditation authority (sometimes more than one) which accredits certification bodies. These bodies are all members of the International Accreditation Forum (IAF).

So when selecting a certification body, always check whether they are accredited by a member of the IAF. There are some “certification bodies” which are not accredited or are accredited by organizations which are not members of the IAF. This does not by default mean that their service is poor; however, it is much harder to prove credibility without such recognition.

The following graphic shows the role of accreditation authorities and certification bodies:
Does my certification body have to be accredited by the accreditation authority in my country?

The IAF has a simple motto “one accreditation international recognition”. Some certification bodies such as PECB work globally and undergoing accreditation audits in every single country in which they operate in would not make sense. So all IAF members recognize each other. Indeed it is a requirement for accreditation authorities to do so “Accreditation body members must declare their common intention to join the IAF Multilateral Recognition Agreement (MLA) recognising the equivalence of other members’ accreditations to their own.”

So as long as your certification body is accredited by a member of the IAF then this is the major point.

What else to look for?

Other factors in selecting a certification body would include, their credibility, their geographic presence, the price (of course) their knowledge of your industry and competence of their auditors. The latter is extremely important. Ensuring the audit team has the right skills, experience, and knowledge is fundamental to have a positive audit experience.

That is why we at PECB, are continually involved in educating and certifying individuals and companies against ISO standards, as a way to show their commitment towards excellence, credibility, and international recognition. For more, please visit www.pecb.com.

About the author

Graeme Parker is an experienced professional in Cyber Security, Business Continuity, Risk Management and Governance fields with proven experience in implementing and developing effective management systems against various ISO standards. He is the Managing Director of Parker Solutions Group, the PECB representative in the United Kingdom.

If you have any questions, please contact him at: graeme@parkersolutionsgroup.co.uk