Customer journal no. 76 – II/2015

DQS IN DIALOG

The changing understanding of Quality

The German Institute for Standardization (DIN) is the gateway to global standardization. DIN's goal is to develop standards that have validity worldwide. These help remove technical barriers to trade and add to the exporting strength of German industry. DIN represents German national interests in Europe and throughout the world. Participation in standards work at DIN gives German experts access to decision-making processes in supranational standards committees. DIN is also founding shareholder of DQS. On occasion of the 30th anniversary of DQS, the DQS editorial staff asked Dr. Torsten Bahke (Ph.D, Eng.), Chairman of the Board of DIN and former Chairman of the DQS Shareholders Committee, a few questions.

DQS: Why did DIN support the founding of DQS in 1985?

Dr. Bahke: The original purpose of founding DQS in 1985 was to promote the German economy. In order to export goods internationally, it required particular focus on the subject of Quality Assurance (QA).

ISO, the International Organization for Standardization published their very first standard for Quality Assurance ISO 9001 in 1987. But much work had been done in this field in the years before already. In 1979 in Great Britain the standard BS 5750 was published, which is considered the forerunner of ISO 9001. In Switzerland and Great Britain, to mention just a few, organizations already existed that issued certificates about the quality assurance systems of companies.

DQS was founded as the first certification body for management systems in Germany by DIN and the German Association for Quality (DGQ), along with two large industry associations, with the objective of ensuring independent confirmation of the fulfillment of quality assurance standards irrespective of business sector.

DIN contributed their know-how of standardization, while DGQ added their training expertise to the new company, which was originally intended to be a self-governing institution of the German economy. A certified „Quality Assurance System“ increased the confidence of customer both domestic and international into the quality ability of German compa-

Dr. Torsten Bahke (Ph.D, Eng.)
Chairman of the Board of DIN

HIGHLIGHTS

nies. At the same time, it ensured further dissemination of the idea of standardization and promoted their application. Today, the ISO 9000 series is one of the most popular series of standards in the world. In 2014, a total of 1 138 155 certificates have been issued worldwide*.

DQS: What does DQS stand for today, 30 years after its founding?

Dr. Bahke: The understanding of quality has changed, not only in Germany but all over the world. There is a need for holistic quality management systems that guarantee reliable performance in international supply chains. That is why DQS is active and recognized as a global player these days, one of the ten largest certification bodies for management systems. While in 1985, DQS was totally focused on the subject of quality, 30 years later DQS also conducts audits and certifies comprehensive management systems for environmental protection, occupational health and safety, and information security. To do this, DQS operates offices in 60 countries, employs 2,500 competent auditors worldwide, and has certified more than 57,000 sites.

* *Source: ISO Survey*

Principles of International Standardization

Voluntary nature

Compliance with ISO Standards is voluntary, but they may become a market requirement, as has happened in the case of ISO 9000 on quality management systems, or of dimensions of freight containers and bank cards.

Market relevance

ISO develops only those standards for which there is market demand. The work is carried out by experts from the industrial, technical and business sectors which have asked for the standards, and which subsequently put them to use. These experts may be joined by others with relevant knowledge, such as representatives of government agencies, testing laboratories, consumer organizations, environmental agencies and academia, for instance.

Consensus

Although compliance with ISO Standards is voluntary, the fact that they are developed in response to market demand, and are based on consensus among the interest parties, ensures widespread applicability of the standards. It has been agreed that evolving technology and evolving interests need to be taken into account by a regular (five-yearly) review of the standards, when it is decided whether a standard should be maintained, updated or withdrawn. In this way, ISO standards retain their position as the state of the art, as agreed by an international cross section of experts in the field.

One vote per country

Each full ISO member is entitled to participate in the preparation of standards it deems of importance for the economy of its country. Each ISO member has a single vote, irrespective of the economic significance of the country. ISO work is thus carried out within a democratic framework which gives each country the strategic means to influence the direction the work is to take and the technical content of individual standards.

Globality

ISO Standards are technical specifications providing the framework for compatible technology worldwide. About 50,000 experts in all participate in approximately 3,000 ISO committees (technical committees, subcommittees, working groups, etc.).

Source: www.din.de

DQS: What relationships do you see between standardization and certification?

Dr. Bahke: Standardization and certification are closely connected; standards are the approved evaluation basis for a certification. They are created in a transparent and moderated process that involves stakeholders from such areas as business, science, public administration, consumers and testing institutes. Those expert circles that will be using the standard later, determine its contents themselves. That is why standards serve as tools of deregulation. Laws and regulations only provide the legal framework, while the design is handled by the users themselves – moderated by standardization bodies such as DIN.
DQS is also involved in national and international standardization councils, in order to contribute their experience with management systems back into the standardization processes.

DQS: What is your wish for the future development of DQS?

Dr. Bahke: It is my wish that DQS continues to support the German and international economy through quality on the highest level, and to keep their sights on new and innovative areas.

EDITORIAL

It was the year 1985 and ISO 9001 was not even published yet – only a draft version was available when the first DQS customer received their certificate. 30 years and many standards, customers and auditors later, DQS ranks among the 10 major global players in the field of management system certification.
Customers actually were the reason DQS came into existence at all; it was to fulfill their expectations of conformity assessment that several German non-profit associations came together to found DQS in 1985 in the first place. And customer expectations have continued to drive DQS ever since; today's customers expect their certification body to deliver specific input and feedback that can be used to further develop their management system. Now more than ever, a certificate is not just a certificate; for our customers it is the start of a partnership designed for their benefit and growth.

Audits are at the heart of these expectations, and they have also developed. Certified organizations no longer see audits as the "price to pay for the certificate". In today's volatile and innovation-focused markets, audits have become a valuable management tool for the analysis and optimization of business processes. And with the latest revision of ISO 9001:2015 and its emphasis on the context of an organization, audits are essential for the identification and management of strategic risks and opportunities.

In this issue of our customer journal, you will read from one of our founders: the German Institute for Standardization. Their Chairman of the Board encourages us to "continue to support through quality on the highest level, and to keep our sights on new and innovative areas."

We will gladly pledge to this.

Martina Meinefeld
Manager, International Business Development
martina.meinefeld@dqs.de

CUSTOMER PROFILES

Drink safely – DQS Ethiopia certifies PepsiCo plants to HACCP

MOHA, Ethiopia's sole supplier of Pepsi Cola and other PepsiCo International brands such as Mirinda Orange, 7-Up, Mirinda Tonic and Mirinda Apple as well as bottled water products, is now certified by DQS Group to HACCP. MOHA is one of the leading producers of carbonated soft drinks in Ethiopia, currently operating eight Pepsi Cola Plants across Ethiopia (3 plants in the capital city Addis Ababa and 5 plants up-country). With a total sales revenue of more than 150 million USD in 2014, the plants created job opportunities for over 4000 persons.

PepsiCo and MOHA were impressed with the competence of the DQS Ethiopia team during first contact already, and when invited to present DQS Group and its approach to assessment and certification. The reputation and growth of DQS in the Ethiopian market was as much a factor in their decision as the fact that with DQS Group, they would enter into a relationship with world class global partners. This was further emphasized by the referral from DQS Ethiopia clients like the Ethiopian Standards Agency (also certified by DQS Ethiopia), the speed of certificate issuance (within three weeks after completion the certification audit), and the ability to pay the certification fee in local currency.

Both companies judged the DQS audits at all five plants, which were all conducted by local auditors to have been absolutely value adding. The comprehensive audits covered all areas and all food safety requirements; the auditors were focused, managed their time well and their overall approach to auditing was very positive. The audits were accompanied by fruitful discussions, a lot of sharing of experience and identification of opportunities for improvement.

The cooperation with DQS resulted in a variety of concrete improvements, among them the identification of additional applicable regulatory requirements, which were effectively implemented after the audit.

"Quality and Safety are crucial in our business and we have committed ourselves to these two words. DQS as our preferred certification partner knows exactly the strengths and the requirements of our market. For me personally, this is very reassuring". Says Mr. Getachew Birbo, CEO of MOHA Soft Drinks Share Company, sole producer and supplier of Pepsi Cola and other PepsiCo International brands in Ethiopia

Also, the employee health check has now been more effectively managed by way of an analysis done to evaluate the trending and prevalence of any communicable disease. At least as important, however, is the enhanced understanding gained that audits are a value-adding tool that leads to improvements.

Considering that the main reasons to become certified was to manage food safety risks in a scientific way based on international standards, which is also a requirement of PepsiCo international ("all plants shall be assessed at least once every year for HACCP & GMP audits"), PepsiCo and MOHA are well satisfied with the audits and the results. They now intend to continue with DQS Group in other management system standards such as Environmental Management System (ISO 14001 already under implementation in the plants in Ethiopia) and FSSC 22000.

For the time being, the upcoming new plants will also join the annual certification audit programme shortly, and the possibility of outsourcing supplier audits to DQS Group is also being considered.

Article by
Tadesse Solomon
Deputy Manager, DQS Ethiopia

DQS Management Services Plc.
info@dqsethiopia.com

MOHA SOFT DRINKS INDUSTRY SC
moha@ethionet.et

Introducing MIDROC

MOHA Soft Drinks Industry Share Company, established in 1996, is a subsidiary of MIDROC Ethiopia Investment Group, which is a member of the MIDROC Group of companies owned by the prominent global business tycoon, H.E Sheikh Mohammed Hussein Ali Al-Amoudi and his family.

These Group companies are operating in Africa, Europe, the Middle East and the United States of America. MIDROC Ethiopia, with about 70 group and affiliate companies, is engaged in multifaceted business sectors across the country including agriculture, agro - industry, hospitality (Sheraton Addis), construction, mining, leather, soft drinks, healthcare and properties.

ISO 50001 Certification at G & W Mineral Resources

Wadeville, South Africa

As part of its on-going efforts to improve plant efficiencies, throughput and cost reductions to its customer base, G & W recently embarked on a quest to acquire international certification to the energy standard ISO 50001. G & W is already a holder of an Integrated Management System (IMS) certification of ISO 9001, ISO 14001 and OHSAS 18001 by DQS.

On occasion of the certificate presentation, G & W Managing Director Coenraad Calitz welcomed an assembled audience of personnel and guests at the company's training centre in Wadeville to overview the background behind the successful metamorphosis that had occurred at the plant. Coenraad demonstrated that a number of key processes had been achieved and implanted in the business operation to turn around the plant in terms of on -going improvements, lean materials management and safety. Their use of Kanban, to mention just one example, had resulted in faster turn-around times in order fulfilment and thus happier customers, as their on-time and in-full delivery record has become entrenched over the last 40 months.

These, Coenraad explained, were the results of successful handover and daily operation to the shop-floor personnel. "Particularly", said Coenraad, "of our 'daily conscience' and 'finger on the pulse culture' of kaizen change. Everything we do in these initiatives is largely a success thanks to the 'buy-in' by line supervisors – some of whom are here today with us, and of course, the teams operating in each section of the plant."

For its journey to ISO 50001, it engaged the services of the National Cleaner Production Centre (NCPC) to provide its training courses in energy management systems (EnMS) and energy systems optimisation (ESO) which were developed in partnership with UNIDO as part of the Industrial Energy Efficiency (IEE) suite. Francois Labuschagne, the CEO of DQS South Africa, said that "this is indeed a notable occasion for us and we at DQS are delighted to present the certificate to G & W Mineral Resources, as the first company in Africa to have achieved this standard through DQS". "This is such an occasion that we've had a special presentation certificate made to honour the achievement". This makes G & W one of only 8 organizations in Southern Africa who have achieved or are working towards ISO 50001.

Francois asked the auditor, Henry Kruger, the Lead Auditor who conducted the audit of the ISO 50001 compliance to comment. "I was very impressed", Henry commented, "On the degree of preparation made by G & W in ensuring that the audit went smoothly and successfully with no major compliance issues and a real focus on the projects achieved in making the certification a success".

Speaking on behalf of all those who contributed to achieving the certification,

Presenting the DQS ISO 50001 certificate.
(L to R) Coenraad Calitz (MD – G & W); Henry Kruger (Lead Auditor DQS)

Coenraad expressed the point that "This is a significant milestone of success for us, but we've committed to a course of continuous improvement, motivated by the PDCA process inherent in all ISO standards and will continue to drive this sentiment and approach in G & W."

"I appreciate the commitment made by all the personnel at G & W plus the support given us by the NCPC and DQS South Africa. The goal was ISO 50001 certification, but it is the learning and improvements on the journey that matters in the end."

G & W Mineral Resources is part of the Zimco group of companies in South Africa, itself a wholly-owned subsidiary of the Ecobat Technologies group in the UK, giving G & W Mineral Resources access to global technology and resources.

G & W operates 6 mines, producing Bentonite, Kaolin and various other minerals. The production is consolidated in Wadeville where the minerals are milled, bagged and distributed sub Saharan wide in either paper-bags, bulk bags or tankers.

Sustainable development is a key element of all decision making to ensure continued economic, environmental and social value and reputation.

For information or to inquire after certification, please contact:

DQS German Association for Certification of
Management Systems (Pty) Ltd.
Mr. Francois Labuschagne
279 Kent Avenue
Randburg 2125 – South Africa

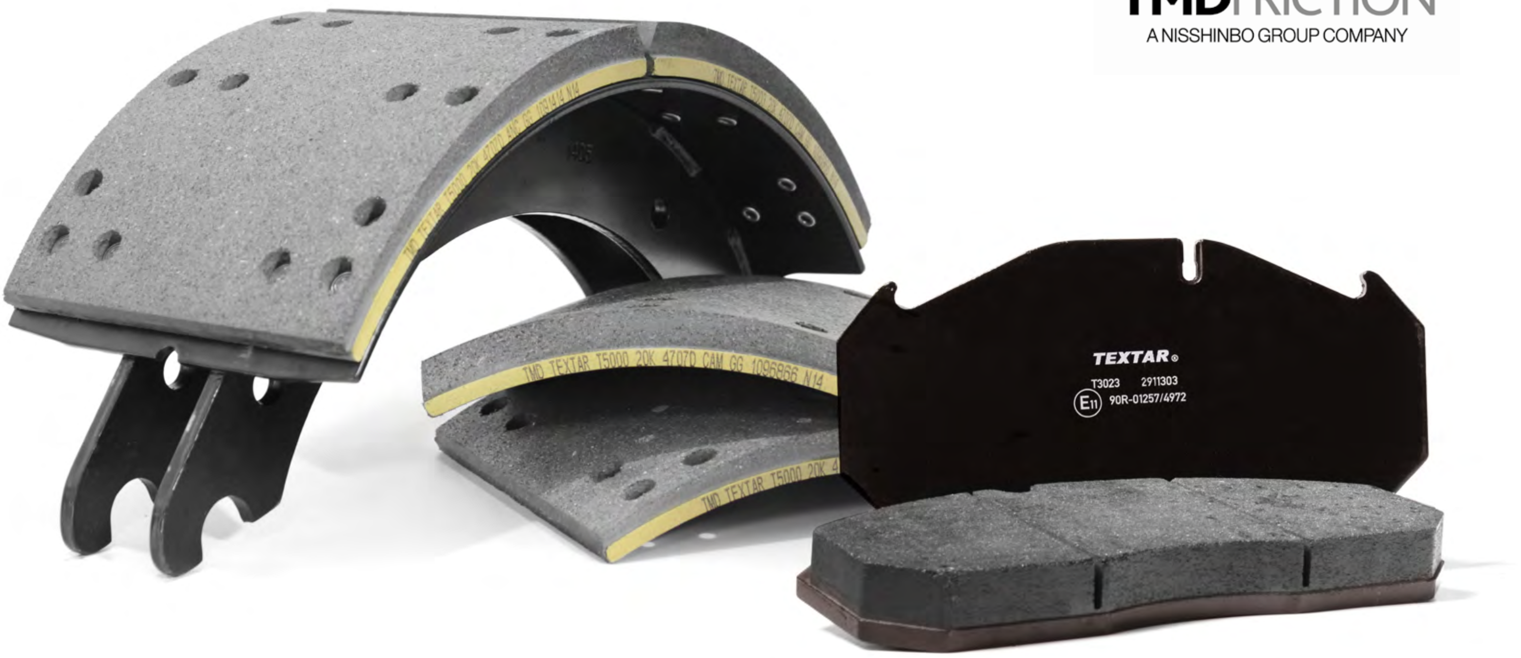
Tel. +27 11 7870060
Fax +27 11 7870115
E-mail: dqs@dqs.co.za
www.dqs.co.za

All pictures credit: Kaimara/CSIR

TMD Friction is now certified in energy management system ISO 50001

At TMD Friction, we are constantly looking for better ways of preserving the environment, and to demonstrate our strong social & environmental commitment. As market leaders, we are always looking for new technologies which allow us to help preserve the environment and reduce energy costs. Those were just two of the main reasons for our plant in Querétaro, Mexico to have become certified according to ISO 50001 for Energy Management Systems.

TMDFRICTION
A NISSHINBO GROUP COMPANY



"This certification represents TMD's commitment to continuous improvement. As the global leaders in brake friction technology, we are always looking for ways to make our products better and more efficient while respecting the environment and conserving resources", says Fabio Jurchaks, Sales & Engineering Director NAFTA.

Using energy efficiently helps organizations save money as well as helping to conserve resources and tackle climate change. ISO 50001 supports organizations in all sectors to use energy more efficiently, through the development of an energy management system (EnMS). As result of this certification, we have also been able to make our personnel aware of the importance of energy usage during their daily work. In addition, our energy and operational costs have been reduced considerably.

At TMD we understand quality not only as a defined production procedure, but as an overall belief and behavior. Because of this, the continual improvement needs to be a daily process, not only inside the organization but also to the environment and society. In this constant improvement process, TMD is now producing the highest quality friction materials with the least ecological impact.

ISO 50001 is based on the management system model of continual improvement also used for other well-known standards such as ISO 9001 or ISO 14001. The key requirements we have to fulfill to be ISO 50001:2011 certified include:

- Develop a policy for more efficient use of energy
- Fix targets and objectives to meet the policy
- Use data to better understand and make decisions about energy use
- Measure the results
- Review how well the policy works, and
- Continually improve energy management

This overall process has been supported by DQS in a very positive way. They have provided us with the support and guidance for the process implementation. We look forward to working with DQS in order to continuously improve our processes. As of 2014, this certification has only been obtained by 6,778 companies globally from all sectors, and only 85 companies in North America. Today, TMD is proudly part of this group.

This article was brought to you by:

Karina Arce
Marketing Coordinator & Customer Service NAFTA
www.tmdfriction.us

and
DQS de México S.A. de C.V.
www.mx.dqs-ul.com

ISO 50001 Certification: Why companies (should) want it

The careful handling of energy resources is one of the most important responsibilities of any organization today. Suitable measures will focus on the continuous improvement of energy efficiency, as well as the entire energy-related performance of the organization. International energy management standard ISO 50001 supplies an organization with an ideal framework to achieve this.

1. **Improving the Corporate Image – be a Green Company**
   Companies are increasingly being measured by their care for the world, whether this relates to environmental impact, occupational health and safety, or social responsibility in general. ISO 50001 certification shows that a company is actively reducing energy consumption and thus working towards a greener planet.
2. **Financial gains**
   The implementation of an energy management system often allows for simple organizational changes to result in significant savings, without any major investments. Companies which have implemented ISO 50001 have reported energy savings from 11 to 25%.
3. **Laws and regulations; Government incentives**
   Many governments around the world have committed themselves to reducing CO2 emission and energy consumption significantly within the next 5-15 years. Please visit the website of your Environment Ministry to see what incentives your government gives for the implementation or certification of ISO 50001!

Specifically for countries within the EU, the EU energy efficiency directive provides enormous opportunities. The directive includes the obligation for large enterprises to carry out an energy audit at least every four years, with a first energy audit at the latest by 5 December 2015. Companies with an active ISO 50001 certificate are exempted from this obligation. Also, there are incentives for SMEs to undergo energy audits to help them identify the potential for reduced energy consumption.

To find out about further benefits, please contact your local DQS office. Their contact data is available via www.dqs-holding.com/international.

If you want to know more about ISO 50001 and the benefits of a certified energy management system in your company, please contact your local DQS office. Links to all offices can be found on the group website at www.dqs-holding.com.

It is time for Excellence in Education

ISO 29990 is a relatively new globally applicable standard for learning service providers. In this short series, we present the experiences of customers from various countries with its implementation, and the benefits gained – starting with FEPADE in El Salvador.

LA PRIMERA INSTITUCIÓN EN LATINOAMÉRICA EN RECIBIR LA CERTIFICACIÓN ISO 29990
Certificación ISO 29990
ISO 29990
"Proveedor de Servicios de Aprendizaje"
Certificación ISO 9001
ISO 9001
"Satisfacción del Cliente"

Lic. Castrillo, Executive Director, FEPADE El Salvador talks about their first experiences with ISO 29990

Fundación Empresarial para el Desarrollo Educativo (FEPADE) was the first company in Latin America to receive certification according to ISO 9001 and ISO 29990. Since then, the impact of these certifications has awakened much curiosity and also expectations in their environment. Companies that employ the services of FEPADE want to know how they did it and why. Together with DQS, FEPADE are working to raise awareness in the country that there is a specific standard for learning service providers. As Mrs. Castrillo said *"From the moment we implemented both ISO 29990 and ISO 9001 we realized that we are pioneers now, and that we have made a qualitative jump."*

Founded 28 years ago, FEPADE is a non-profit educational organization whose mission is to contribute to the development of education in El Salvador at all levels through the implementation of various programs and projects. Their vision is to be the best providers of learning services in Latin America, and to guarantee quality in their service with a focus on customer satisfaction.

The ISO 29990 standard defines a specific management system for institutions involved in offering training and education. *"At first we were afraid to make a dual certification," said Mrs. Castrillo, "because that requires a higher level of commitment. But, why not take the chance when we have already gone half the way? After all, when you work with a company like DQS that is known for being the best on the market, you know it is worth the effort and you can bet on the good results. So we chose DQS, as I saw it had the reputation of being the best in the world."*

Certificate handover by the Managing Director of DQS El Salvador, Mr. Guenter Schranz, to the team of FEPADE

During the preparations already, FEPADE learned many important things, such as the importance of teamwork, strengthening of emotional tools and working to convince people. Big changes cost money and effort, and their benefits are not always tangible. But as the preparations moved forward, the staff was able to see that they were defining the path together where they want to go and to make that positive change. Mrs. Castrillo explained: *"Our staff thought of this in terms of improving the car we were driving when we do our work, and the improvement was like moving from a simple but roadworthy vehicle to a Mercedes-Benz."*

The certification resulted in improved operational tools and manual processes in daily operations. FEPADE now operates in a more organized atmosphere that is better structured and where results are visible. Internal and external customers are seeing improvements in the quality of service that FEPADE is providing. Mrs. Castrillo: *"Making future plans for education is the biggest TO DO for us, our mission and FEPADE's permanent service line. We make a plan every year, review it, and then adapt and re-adapt it to keep up with our quality development. The fact that FEPADE is certified influences the promotion of non-formal education and apprentice training in our country. Many universities and other education institutions see FEPADE as an ally and have an interest in doing business with us now, due to our certifications".*

At the official certificate presentation, the President of FEPADE, Ing. Ricardo Freund, stated that *"we decided to go for a double certification in order to exceed the expectations of our customers, and to ensure a positive and significant impact on the educational environment. We worked hard to meet all the requirements and opted for the global certification of DQS to validate and verify the excellence of FEPADE globally."*

The requirements of ISO 29990 are very high and the standard demands much more from a learning service provider than any other. To ensure the educational development and progress of their country, some governments have begun to require implementation of ISO 29990 as a requirement for receiving government subsidies.

Lic. Castrillo
Directora Ejecutiva
FEPADE El Salvador
www.fepade.org.sv

Interview conducted by
Daniella Torres,
DQS El Salvador

For more information on ISO 29990 in El Salvador, please contact:

DQS El Salvador
Ca 2 Pje 6 #64, Lomas de San Francisco
San Salvador, El Salvador
Tel. +503 2265 3300
E-mail: cert@dqs-elsalvador.com
www.dqs-elsalvador.com

For all other countries, please visit
www.dqs-holding.com
for an overview of local offices in your area.

Nigeria's oldest and largest development bank achieves international ISO 9001 certification for their Quality Management System

BANK OF INDUSTRY
...transforming Nigeria's industrial sector.

from left: Head Strategy and Transformation/Management Representative, Mrs. Betsy Obaseki; Managing Director/CEO, Bank of Industry, Mr. Rasheed Olaoluwa; DQS Nigeria Country Director, Mr. Lawrence Ogudu; Divisional Head, Large Scale Industry, Bank of Industry, Mr. Joseph Babatunde; CEO, DQS, South Africa, Mr. Francois Labuschagne and Divisional Head, Small and Medium Enterprises, Mr. Abdulganiyu Mohammed, at the official presentation of ISO certificate to Bank of Industry in Lagos

The Bank of Industry, Nigeria's foremost and most successful development financing institution, has become one of the few organizations in the financial service sector to achieve the international ISO certification for Quality Management System in Nigeria.

This stringent standard according to which DQS certifies, which is maintained by the international Organization for Standardization (ISO) and administered by Accreditation Bodies, recognizes the BOI world class structure, processes, maintenance of systems and ongoing initiative for continual improvement in the pursuit of the bank's vision. "To be Africa's leading development financing institution operation under global best practice".

"This is a great achievement for the bank of Industry" states Mr. Rasheed Olaoluwa, Managing Director and Chief Executive Officer of the bank.

The certification came after a lengthy and detailed audit of the bank's processes conducted by the bank internally. "We performed regular internal audits and monitoring and measured the activities of our processes in order to ensure that we not only keep up with the ISO standard requirements, but meet our vision and promise to our stakeholders of running our business under global best practices," explained Mrs. Betsy Obaseki, the Head of Strategy and Transformation /Management Representative.

A comprehensive system wide audit was carried out by a team from DQS Nigeria as part of the final audit and certification exercise. During the audit several key strengths were noted by the team of visibly impressed DQS auditors, as well as opportunities for improvement.

The Bank was commended for having a highly visionary, committed and transformational leadership, structures and process driving the business and highly competent and committed staffs at all levels and traceable evidence of movement towards its clearly defined mandate:

"To transform Nigeria industrial sector by providing financial and business support services to enterprise".

"I am impressed and very proud of BOI's achievement, and with what I have seen, BOI have stepped up to be the organization that cannot be ignored in the industry, as well as having prepared the structure for sustainability of this certification", said Francois Labuschagne, Chief Executive Officer at DQS South Africa who represented DQS Group at the event of the official certificate presentation ceremony held in Lagos, Nigeria, along with Lawrence Ogudu, local Managing Director in Nigeria.

For more information, please contact:

***DQS Management Systems Nigeria Ltd.
Mr. Lawrence Ogudu
2, Montgomery Road
P.O Box 271
Yaba – Lagos – Nigeria
Tel. +234 7034141755
Tel. +234 8023216994
E-Mail: Ogudul@dqsnigeria.com
www.dqs-holding.com***

***DQS German Association for Certification of Management Systems (Pty) Ltd.
Mr. Francois Labuschagne
279 Kent Avenue
Randburg 2125 – South Africa
Tel. +27 11 7870060
Fax +27 11 7870115
E-Mail: dqs@dqs.co.za
www.dqs.co.za***

UPDATES TO STANDARDS

ISO 9001:2015 now published!

The revision of the quality management standard ISO 9001 is now finally concluded: ISO 9001:2015 was now published.
After the FDIS of the standard was published in July, the ISO member countries had two months to vote on this final draft before the deadline of 9 September. Not a single country voted against the FDIS.

For reasons of efficiency, ISO decided to make the official publication date 15th of September 2015 – the same publication date as for ISO 14001:2015. The transition rules and deadlines for both standards are thus the same.

ISO 9001:2015 and ISO 14001:2015 – The Next Generation

Join us to be up to date:
www.dqs-holding.com

In comparison with ISO 9001:2008, the main changes to the standard are:

- High level structure and core text from ”Annex SL“
- Increased emphasis on achieving value for the organization and its customers (“output matters”)
- Increased leadership requirements for top management commitment and involvement (Top management is accountable for the system and its performance).
- The need to understand the context of the organization and the needs and expectations of interested parties
- Emphasis on risk-based thinking
- Increased flexibility regarding the use of documentation

Certified companies will have a three-year period to transition to the revised standard. Detailed information on the standard can be found on the website of ISO TC/176/SC2. The standard is available from the ISO store at ww.iso.org.

DQS supports their clients with information, trainings, workshops and gap assessments. Please contact your local DQS office to receive further information; their contact data can always be found on our website at www.dqs-holding.com.

Leadership and commitment in ISO 9001:2015

If we compare the current ISO 9001:2008 with ISO 9001:2015, the first thing we notice in chapter 5, the subject of this article, is the new headline: what used to be "Management responsibility" has now become simply "Leadership". And that makes a world of difference; the size of the chapter alone has increased by about half. What is noticeable is the high degree of detail when it comes to top management requirements. The first sub-chapter alone describes ten separate key areas for specific action. Overall, the new standard specifies the tasks of top management much more specifically than before.

According to the standard's definition, top management is the person or group of people who directs and controls an organization at the highest level. This is the level where decisions are made about resources, and where responsibility may be delegated. In most organizations, these characteristics are synonymous with the function of a managing director, and the corresponding authority to act.

One of the first new requirements is called "accountability": top management shall take accountability for the effectiveness of the quality management system. You will notice here the distinct difference between "responsibility" and "accountability". Other staff members or supervisors may be responsible for the conduct of activities. However, top management is always accountable in the sense that they have to answer for the results of the quality management system, and bear the entrepreneurial responsibility for their effectiveness. The awareness of this and the resulting imperatives for Top Management are not always pleasant – I speak from experience here – but they are effective.

In order to achieve this, all of the quality management system requirements have to be integrated into the organization's business processes, and the use of process approach and risk-based thinking needs to be promoted. A look at ISO 9004:2009 helps to make these expectations more tangible. Maturity level 2 (of 5) already calls for the definition of key processes, their systematic measuring and clear process responsibilities. What would be even better, for example, is the integration of interested parties during process design. And when it comes to risks and opportunities, regular evaluation, anticipatory risk analyses and emergency preparedness would constitute an excellent example for the implementation of risk-based thinking.

But be careful: plans, ideas and concepts are not enough – it is results that matter. This governing principle of ISO 9001:2015 is also reflected in the requirements for top management. They have to ensure that the quality management system achieves its intended results. Achieving only some of the expected results and systematically conducting corrective action would fulfill only the very basic requirements. Characteristic of a mature organization would be consistently excellent results with sustainable trends, ideally above the sector average; both in respect of the entire system as well as the key processes.

So what does DQS as a certification body expect of top management when conducting an audit? "Leadership" in the sense of ISO 9001:2015 requires personal, pro-active participation of top management in the management system. Evidence of this can be found in meaningful Management Reviews based on facts, in minutes, personal messages, decisions and last but not least in a permanently high level of product and service quality. If you make your own commitment to quality noticeable in so many different ways, you will be well prepared for certification.

Götz Blechschmidt
Managing Director
DQS GmbH, Germany

POINT OF VIEW

Risk-based thinking and action

Revision of ISO 9001:2015

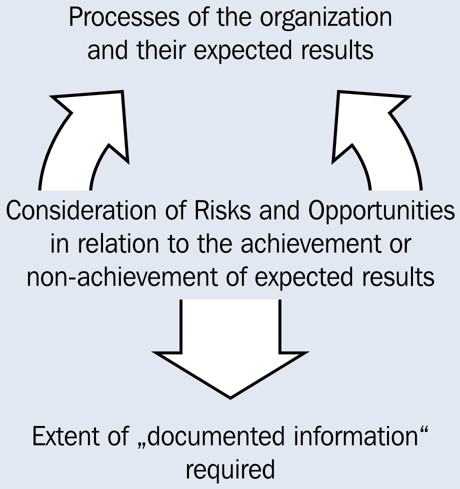
One of the most essential changes that the revision of ISO 9001 has in store for us is certainly the risk-based thinking approach. Of course the subject of "risk" is not completely new to ISO 9001; until now, however, it had been part of the requirements for preventive measures. These have been done away with in the revised version, and have been replaced by the consideration of Risks and Opportunities.

The consideration of Risks and Opportunities starts with ISO 9001:2015's increased focus on the achievement of "intended results", with respect to both the quality management system itself as well as the processes required for this. These "intended results", on the other hand, are directly derived from the system's scope of applicability, which is aimed at creating products and services that fulfill customer expectations, legal or regulatory requirements or the organization's own definitions. We are therefore not talking about a comprehensive risk management system based on e.g. ISO 31000, and there is no requirement for a formalized risk management process. And nobody is required to employ specific methods for the identification or appraisal of risk, either.

In this context, it is really advisable to refer to two documents published by the respective ISO committee, both of which explain in very short and concise form what the risk-based approach is all about. One of them is a presentation on "Risk Based Thinking" and the other a very vivid, practical example for crossing a busy street. Both articles can be downloaded free of charge from the link below. For additional, good explanations one can also refer to chapter 0.3.3 of the revised edition. Among other things this chapter explains how indispensable risk-based thinking really is for an effective quality management system, and how it should be applied to achieve improved results and to avoid negative effects.

When defining an organization's processes, ISO 9001:2015 requires a risk-based approach.

The inner logic of ISO 9001:2015


Processes of the organization and their expected results
Consideration of Risks and Opportunities in relation to the achievement or non-achievement of expected results
Extent of „documented information" required

ISO 9001:2015 defines risk as the effect of uncertainty on an expected result.

Specific requirements of ISO 9001:2015

- Identification of Risks and Opportunities, in order to ensure the achievement of intended results, enhancing desired effects (those are Opportunities) and preventing or reducing undesired effects (those are Risks), and to achieve improvement
- Evaluation of identified and recognized Risks and Opportunities. No mandatory methods have been listed. Well-known and established tools such as (process) FMEA, SWOT analyses, ABC analyses or risk matrix can certainly be recommended.
- Deriving measures from the Risks and Opportunities identified. These may relate to eliminating/avoiding the risk or the source of risk, to reduce the risk by way of changing its probability of occurrence or its effect/impact. It may also mean an acceptance of risk, e.g. to take advantage of an opportunity.
- Evaluation of the effectiveness of measures, e.g. when identified risks do not occur or where the probability of occurrence has been lowered. Also consider the mitigation of impact (e.g. through insurance or contractual provisions in customer contracts, etc.)

As far as the question of “in what form and to which extent “documented information” (in new ISO 9001:2015 lingo) is required, what we can say is that there is no explicit, precise requirement in the relevant chapters of the standard. Instead, Annex A4 (which is very interesting to read in and of itself) states that: “…the organization is responsible for its application of risk-based thinking and the actions it takes to address risk, including whether or not to retain documented information as evidence of its determination of risks.” To put it simply: each organization defines their own requirements – not the standard, not the CB, and not their auditors.

Interested parties and their relevant requirements regarding Risks and Opportunities

An aspect that should not be overlooked is the examination of relevant requirements raised by parties that are relevant to the quality management system. Relevant, in this case, needs to be interpreted as having an effect on the organization’s ability to continuously provide products and services conforming to customer expectations and legal or regulatory requirements. Therefore, these requirements need to be included in the context of examining Risks and Opportunities.

Often overlooked: Opportunities

Even though ISO 9001:2015 always balances Risks with Opportunities, many people are looking to see exactly what opportunities those may be. This does not refer to the achievement of intended results, because that is a basic requirement of the quality management system and its processes. But once again we can find sound advice in chapter 0.3.3 of ISO 9001:2015, where the following possible opportunities are listed:

- Attract customers
- Develop new products and services
- Reduce waste
- Improve productivity.

More advice can be found in the comments to chapter 6.1.2, such as:

- Adoption of new practices and use of new technologies
- Introducing new products to the market
- Opening up new markets
- Building partnerships

To sum this all up, what we recommend is to identify and appraise Opportunities with the same intensity that is being used to identify and appraise Risks, and to derive actions in the same way, in order to take advantage of them.

Frank Graichen
Managing Director, DQS Medizinprodukte GmbH
frank.graichen@dqs.de

Recommended reading material from the ISO Committee

The presentation on “Risk Based Thinking” and document N1222 “Risk in ISO 9001:2015” can be downloaded free of charge from http://isotc.iso.org/livelink/livelink/open/tc176SC2public

For more information and a deeper look inside Risk Management, this series will be continued in the next issue of DiD, the Customer Journal of DQS Group.

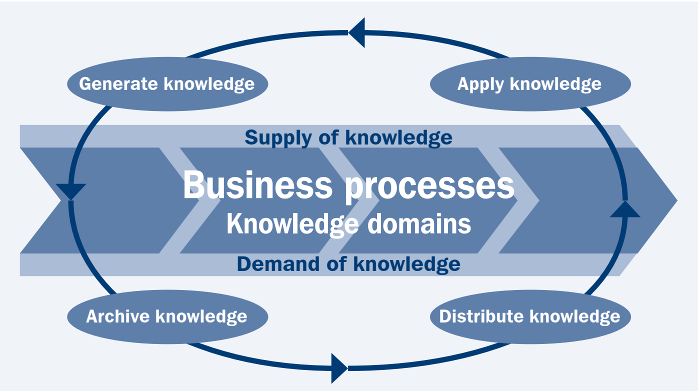
ISO 9001:2015 – Organizational Knowledge

We live and we work in an "Information and Knowledge Economy", and most organizations will not argue the real-life significance of knowledge as an asset and success factor anymore. But how do we manage to integrate the resource "Knowledge" systematically into a management system?

ISO 9001:2015 states that: "The organization shall determine the knowledge necessary for the operation of its processes and to achieve conformity of products and services. This knowledge shall be maintained and be made available to the extent necessary. When addressing changing needs and trends, the organization shall consider its current knowledge and determine how to acquire or access any necessary additional knowledge and required updates."

Breaking this down into actual requirements means that:

- For each of their identified processes, the organization also needs to specify the exact pertinent knowledge. → Process knowledge needs to be included in the process description.
- There are two issues at stake: one is process execution, the other quality achieved. → Process knowledge refers to the execution of individual partial processes and activities (e.g. regarding the control of methods and technologies, the handling of machines) and the implementation of conformity requirements (regarding laws, normative and other requirements, customer demand, etc.)
- Knowledge needs to be maintained in concrete organizational forms, i.e. regarding processes, products, and the development of customer expectations. Modern information technology holds very effective tools for this. → Maintenance also implies availability and practical use of knowledge as an objective.
- "to the extent necessary" is a step towards competence management. In the context of the standards, knowledge is not an abstract value in and of itself, but focused functionally on its effective application in processes by competent users. → For that we need methods of learning and transfer on how to turn knowledge into competencies of single users or working groups.
- How much of the knowledge required is already available, and what requirements for knowledge need to be considered in the future? On the other hand, which knowledge needs to be "disposed of", because outdated knowledge may be anything from unnecessary ballast to actually posing a danger to the effectiveness and efficiency of processes. → One way of implementation can be found in "learning processes" and "learning organizations".
- What is the knowledge we in our organization fall back on, and what kind of "additional knowledge" do we continuously or in special cases draw from external sources? → What kind of organization and safety features are in place for this? And how do we avoid unwanted "loss" of knowledge?



What is Knowledge Management all about?

The ISO draft refers to knowledge as "available collection of information being a justified belief and having a high certainty to be true", thus creating a connection between information and knowledge.

Authors:
Karsten Koitz, Ph.D., DQS Auditor, together with Prof. Dr.-Ing. Holger Kohl and Ronald Orth, both Fraunhofer IPK, Germany
karsten.koitz@dqs.de

Methods and tools for the systematic knowledge management in organizations

	Methods and tools, e.g.
Generate knowledge	Customer satisfaction surveys
Archive knowledge	Technical methods to document knowledge, i.e. standardized directory structures, wikis, document server
Distribute knowledge	Expert de-briefings with retiring staff members – "knowledge transfer between generations"
Apply knowledge	Checklists or process instructions that ensure quality of results in recurring tasks

ISO 45001 achieves Committee Draft status

The new international standard for Health and Safety, ISO 45001, officially reached Committee Draft (CD) stage

Inspired by the well-known BS OHSAS 18001, ISO 45001 is designed to provide the requirements and guidance to implement a system and structure to help organizations around the world ensure a safer and healthier working environment for their employees.

The committee draft (CD) of ISO 45001 has been approved (with comment) in June 2015, taking a big leap towards its publication. It achieved more than 75 percent approval by the members involved in its development. Following a consultation period, it is expected to be finalized as the draft international standard (DIS) for public voting later this year.

We asked David Smith, Chairman of the committee developing the standard, to tell us more.

Can you tell us about some of the major differences between OHSAS 18001 and the new ISO 45001?

Well, obviously, the overall aim of the standard remains the same and those familiar with OHSAS 18001 will recognize many of the themes in the new ISO standard. However, there have been some very interesting developments related to the new rules for developing International Management System Standards (for more information, see Annex SL of the ISO Directives). For example, there is now a much stronger focus on the "context" of an organization as well as a stronger role for top management and leadership.

What do you mean by the "context" of an organization?

In the new standard, an organization has to look beyond its immediate health and safety issues and take into account what the wider society expects of it. Organizations have to think about their contractors and suppliers as well as, for example, how their work might affect their neighbours in the surrounding area. This is much wider than just focusing on the conditions for internal employees and means organizations cannot just contract out risk.

And how is the role of the organization's leadership different?

Well, ISO 45001 insists that these occupational health and safety aspects now be embodied in the overall management system of the organization, requiring a much stronger buy-in from its management and leadership. This will be a big change for users who may currently delegate responsibility to a safety manager rather than integrate this entirely into the organization's operations. ISO 45001 requires health and safety aspects to be part of an overall management system and no longer just an added extra.

OHSAS 18001 is a widely adopted standard and has been very successful. Why are we developing an ISO standard?

There are a number of reasons for looking at this topic using the ISO system. Firstly, many organizations are already using a number of ISO management system standards, so an occupational health and safety tool that can be easily integrated into this makes things a lot easier. In particular, we have focused on easy integration with ISO 14001 as many organizations, especially small businesses, have one person that looks after both safety and environmental concerns. In addition, we hope that the ISO name and recognition will give further credibility to the standard and drive wider adoption.

However, one of the really fantastic things about this ISO project has been the involvement of a really wide variety of organizations and countries. I was involved in the first meeting leading to OHSAS 18001 over 20 years ago, and so it is personally really exciting for me to see today the sheer number of countries actively involved in the standard's development. Involvement from countries across the globe, from Europe and America, but also Africa, Asia and South America, will help us to create a tool that will work for everyone. We have also had strong involvement from the International Labour Organization (ILO), who are experts on the topic and have some very valuable insights to bring to the table.

Of course, with this many stakeholders, the development work isn't always easy and there are disagreements. But to have so many people involved has been wonderful and gives me hope that we are on track to providing a tool that can be used by any organization, within any regulatory framework, in any country.

So for any new users out there, can you tell us more about the major benefits of using this standard?

If you implement the system and structure we suggest, and do it properly, you can reduce the risk of causing harm to the people working for you. According to ILO statistics published this year, around 2.3 million died as a result of work-related accidents or diseases (ill health) in 2013. These are shocking statistics and a heavy burden for society. Implementing a strong occupational health and safety management system helps organizations reduce accidents and ill health, avoid costly prosecutions, perhaps even reduce insurance costs, as well as create a culture of positivity in the organization when its people see that their needs are being taken into account.

Want a sneak preview of ISO 45001?

The committee draft version of ISO 45001 is now published and may be made available by your ISO member, giving you the opportunity to find out more about the contents of the new standard before the final publication date, set for late 2016.

Credits: www.iso.org/iso/news.htm?refid=Ref1874

David Smith, Chairman of project committee ISO/PC 283, Occupational health and safety management systems.

ISO 14001:2015 published

The revision of Environmental Management Standard ISO 14001 is concluded: ISO 14001:2015 was published on September 15. On that day, the three-year transition period started, after which all certificates according to the old standard will cease to be valid.

A comparison shows that quite opposed to ISO 9001, there were indeed further changes to content.

- Clause 5.2 “Environmental policy” now relates to the suitability of both the purpose and the context of the organization
- The duty to notify “persons doing work under the organization’s control” (subcontractors) about env. policy has been deleted
- The title of Chapter 6.1 was changed from “6.1 Actions to address risk associated with threats and opportunities” to 6.1 Actions to address risks and opportunities”, to correspond with the wording of ISO 9001
- The contents of clause 6.1.4 “Risk associated with threats and opportunities” have been moved into sub-clause 6.1.1 “General”
- The sub-clause “Planning action” now has its own number: 6.1.4
- Increased requirements in clause 7.2 “Competence” now also include the employees’ ability to fulfil their compliance obligations. Also new is the requirement to determine training needs associated with environmental aspects and the environmental management system.
- The change of wording in clause 7.4 “Communication” from “the organization shall establish, implement and maintain a process” to “shall plan and implement a process” is of no real consequence.
- The note to clause 7.5.1 “Documented information” regarding the extent of documented information was supplemented by “the need to demonstrate fulfilment of its compliance obligations”.
- Clause 8.1 „Operational planning and control“now includes a provision to the effect that environmental requirements be addressed in the design and development process for the product or service, considering each stage of its life cycle.
- The provisions of clause 8.2 “Emergency preparedness and response” have been expanded. The organization is now required to provide relevant information and training related to emergency preparedness and response, as appropriate, to relevant interested parties. Further to this, corresponding documented information shall be maintained on emergency preparedness and response.
- Clause 9.1 “Monitoring, measurement, analysis and evaluation” now includes environmental performance.
- The Management review as per clause 9.3. shall now include the needs and expectations of interested parties. What is also new is that the outputs of the management review shall include opportunities to improve integration of the environmental management system with other business processes.

Certified companies will have a three year period to transition to the revised standard. DQS supports their clients with information, trainings, workshops and gap assessments.
Please contact your local DQS office to receive further information.

Robert Bernacik
DQS Product Manager, ISO 14001
robert.bernacik@dqs.de
Member of NAGUS, the German DIN council responsible for the German position in the international consensus.

Credibility and process thinking in environmental communication

New requirements of ISO 14001:2015

ISO 14001:2015 has now been published. Management representatives and auditors, as well as supervisors and employees need to start thinking about how to interpret the changes for their own organization now. One subject that the revision focuses on is internal and external communication. Some consider this to be a Soft Fact, but depending on your business sector, risks, or levels and conflicts of interest this may become a very Hard Fact very quickly. Once the credibility of environmental communication has been compromised, it is extremely difficult to regain the trust of customers, partners and the public. There have been many examples of this in the past. ISO 14001:2015 now includes a stronger focus on this.

The increased importance of environmental communication is being fed from many sources. On the one hand, interested parties have been given more emphasis. Once the relevant parties have been identified, we need to ask which information needs to be forwarded. Customers may also increasingly inquire after your environmental performance: they may need this for their own life cycle planning of products and within their supply chain. Environmental reporting, on the other hand, has become common practice. Many organizations already participate in the voluntary, European eco-audit directive EMAS, or the internationally recognized Global Reporting Initiative (GRI), among others. Starting 2016 in the European Union, 25,000 organizations with more than 500 employees will have to publish a sustainability report with non-financial information (EU Directive 2014/95). There is a noticeable trend among ca. 2,500 large European companies to integrate their reporting about economic, social and ecological aspects and results. The International Integrated Reporting Council (IIRC) is currently working on a framework for integrated reporting.

www.dqs-holding.com

What exactly does ISO 14001:2015 require?

7.4.1 General

In which the organization shall establish and implement a process for internal and external communications relevant to the environmental management system. This process shall include with whom to communicate, when, on what, and how. What is new here is that a process is now required, while previously it was just a method or procedure for communication. In planning the communication process, the organization is now also required to take into account its compliance obligations. Those may derive from reporting constraints for permits, or data deliveries to the supply chain or external presentations. One of the major changes is that the organization shall ensure that information communicated is correct and credible.

What has not changed is that the organization still has to react to communications regarding its environmental management system, but now this also includes relevant internal communication, such as reports issued by environmental assessors, whether voluntarily assigned or mandated by law. External communications still enjoy the privilege of being input for management review. This has not changed. The term “communications” generally includes relevant inquiries, suggestions for improvement, complaints or news. The organization shall retain documented information as evidence of its communications, as appropriate.

1. Which are your organization’s environmental objectives? **2. Which strategies does your organization pursue?**	Legal certainty	Risk mitigation	Conservative efficiency	Opportunity focus	External legitimation	External credibility	Competitive advantage	Comprehensive env. protection	Improved env. performance	…
Fulfill legal and other external env. requirements, also for reporting if appl.	X	X			X	X		X	X	
Reduce env. cost			X							
Include interested parties in the improvement of env. performance		X		X	X	X	X	X	X	
Invest in env. friendly technologies and env. competence				X	X	X		X	X	
Invest in env. friendly product development				X	X	X	X	X	X	
Communicate env. self-declarations and env. reporting externally					X	X	X	X	X	
Promote corporate ecological sustainability in all areas				X	X	X	X	X	X	
…										

An organization’s objectives and strategies

7.4.2 Internal communication

Communication between the various levels and functions of the organization continues to be a requirement. What is new is that this now includes changes to the environmental management system.

7.4.3. External communication

This is basically a repeat of the general requirements regarding the external communication of relevant information as established by the organization’s communication process(es) and its compliance obligations.

What is the purpose of environmental communication?

As a rule, all strategies and objectives are tied in with internal and/or external communication. This is what makes it so important to recognize why environmentally relevant information needs to be communicated. And that is why an organization’s top management should agree on strategies and objectives and be aware of the values associated with them. That is the basis upon which to define the required environmental policies and objectives, and to align them with the strategic focus and context of the organization. This is where you need to determine the importance of environmental dialogue with interested parties, such as employees, suppliers or neighbors.

Relevance matters

A stringent approach allows for an effective and credibly designed communication process. What is important here is to focus on relevant, environmental information. Avoid all types of formalism, perfectionism and aimless activism in order to keep the process slim. Also avoid greenwashing. This happens whenever environmental subjects are pushed to the front even though interested parties consider them irrelevant to the organization's actual environmental impact. Credibility is also endangered whenever employees or supervisors only pay lip service to the communicated environmental standards and values. By the same token, correctness in environmental communication does not happen on its own. Errors may occur when e environmental data is communicated without being reviewed for correctness and up-to-dateness first. The requirement to establish and implement a process that ensures credibility and correctness is therefore the perfect choice.

What does process-driven environmental communication include?

According to clause 3.3.5, ISO 14001:2015 defines a process as a set of interrelated or interacting activities which transforms inputs into outputs. A process may, but is not required to be documented. That is the framework for the various requirements of ISO 14001:2015 as below.

The communication process

Input	Activities	Result
Internal and external issues from the organization's context, especially env. relevant influences on the organization Relevant expectations and needs of interested parties Management objectives and strategies Significant env. aspects and performance, to include product life cycle Legal and other (self) env. commitments Relevant risks and opportunities relevante interne/externe Äußerungen Resources for env.-related communications (personnel, technology, media) …	**WHO with WHOM** Internal/external Authorized and entitled **ABOUT WHAT** Relevant Confidential Suitable **WHEN** Regularly Case-by-case **HOW** Understandable True Factual and reliable Consistent and complete Written/oral Formal/informal	Scope of applicability of the EMS Environmental policy Management review Information and reports – documented (print, IT, video, etc.) or not Legally conformant reporting Documented communication evidence, if applicable …

Opportunities for communication can be individual cases, project cases, regular cases or routine cases. This is subject to how complex the process steps are, how well they can be planned or structured, how similar they are and how repeatable. To an increasing degree, environmental communication is also integrated in existent processes, e.g. in purchasing, production, R&D, waste disposal, hazardous material handling, laboratories, claims processing, management or public relations. An environment-related emergency will usually be notified immediately. Instructions on how to handle hazardous materials is usually carried out verbally during a demonstration; during an Open House, a presentation may be shown. Environmental information is varied and communications must be designed in accordance with their significance. By now you have probably realized that communications cannot be defined as one central process. However, the credibility, correctness and suitability of communicated environmental information must be ensured at all times.

Claudia Nauta
DGQ Weiterbildung GmbH, Germany
Product Manager for Environmental, Energy and OHS
NC@dgq.de

New ISO 27001 Standard Can Reduce Security Breaches

We have witnessed some high profile security breaches in in the past few years. It started with massive data breach of Target reported in December 2013, followed by Home Depot, JP Morgan Chase, Sony Pictures, and the list goes on. The Care First BlueCross Blue Shield group reported massive data breach in May 2015; 1.1 million insurance subscribers' personal data have been stolen. Other BlueCross entities hacked were Anthem Inc., 78 million individual records, and Premera Blue Cross, 11 million records compromised. Most recently, hackers accessed data for 4 million current and former federal employees. The hard question we have to ask is are we learning from these incidents.

Let us go back a couple of years to 2011. Lockheed Martin reported that hackers were able to get into their network. This is the time when Lockheed and the Pentagon were working on their top secret project to develop the F22 and F35 fighter jets. Both the Pentagon and Lockheed denied losing any classified information in that hacking. Everything seemed fine until China released their latest fighter jet J31 in December 2014. Defense analysts were stunned by the striking similarities between the Chinese J31 and the U.S. F35. The Pentagon and Lockheed spent upward of 800 billion dollars to develop the F35. A simple Google search will give you even more information on this subject, but it is just one example of loss of intellectual property through cybercrime. How much is the U.S. economy losing every year? Dr. Ron Ross, head of the Federal Information Security Act (FISMA) implementation project, estimated it to be around a trillion dollars per year.

Let us try to understand root causes of these high profile breaches

Lockheed Martin is known for its robust security protocols due to their involvement in a number of top secret defense projects. Why were the hackers able to succeed? Investigation revealed that hackers first penetrated RSA token database of EMC (a third party vendor) to steal secure user credentials of one of the vendors of Lockheed. Then they logged into the Lockheed system as one of their trusted vendors. It was an eye opener for the security professionals. It showed securing your own network is not enough, but supply chain security is as important as your own security. This case also showed a classic syndrome of "denial." It is very difficult for a premiere institute to accept the fact that they have been outsmarted by some "bad guys."

Let us move on to 2013. Target had outsourced its network security monitoring to a third party organization. That vendor started reporting suspicious activities in Target network several months before the whole incident went out of control. Target had just gone through PCI audits, and their systems were certified. So there was reason to believe "we are safe." Later investigation revealed that hackers penetrated one of the HVAC vendors of Target and got access to Target network. Once again the hackers exploited the weakness of a supply chain partner, and Target senior management's initial reaction was "denial."

Not long after the Target incident, Home Depot declared a massive data breach. Once again, hackers stole credentials of one the vendors of Home Depot to get access to the Home Depot network.

The Sony Pictures hacking topped the list of 2014 security breaches. One of the many things leaked by the hacker in public file sharing sites was a confidential email from the General Counsel of

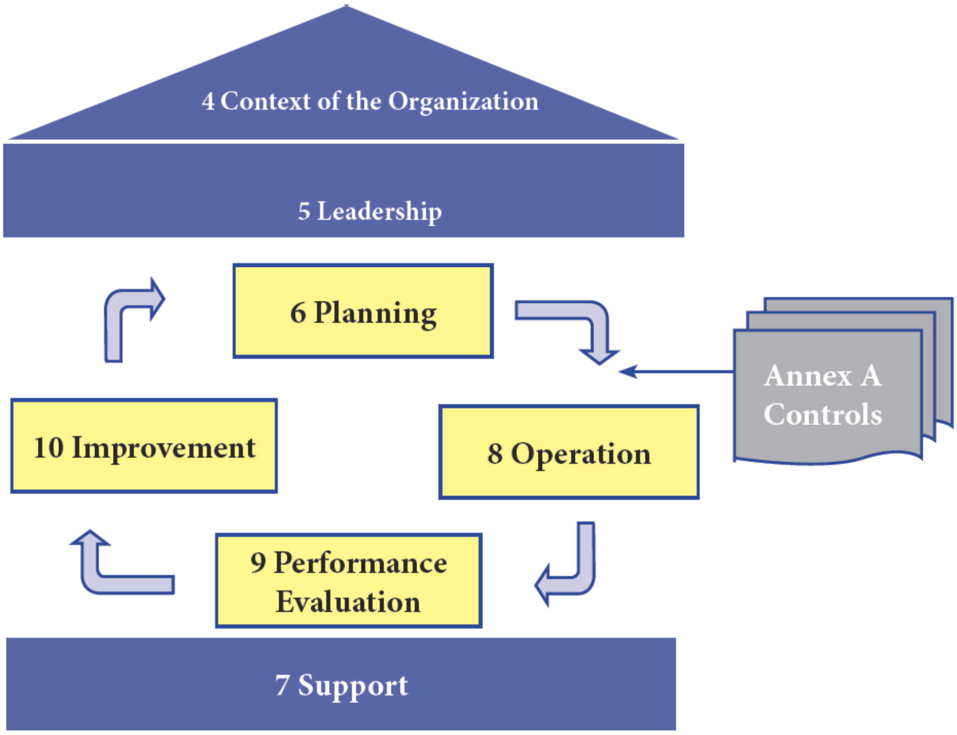
Sony Pictures to the senior management urging them to act on the security gaps reported by an audit firm. That audit was conducted in August of 2014. Senior management of Sony Pictures was aware of the security gaps and chose not to act.

Let us review the new ISO/IEC 27001 standard in these contexts

One of the major changes in the standard is to shift focus of incident management to event management. Security events are symptoms or early indications of a potential problem. Early detection minimizes impact of an incident. Sometimes organizations are aware of some known weaknesses but don't take timely action, as in the case of Sony Pictures. Target management was alerted about these events, but those were ignored. The CareFirst group reported the security incident in April 2015. Their report says hackers had been stealing information from June of 2014. This shows their event management process was not effective.

Another major change is in the area of supplier security.
The new standard has provided additional controls to ensure supply chain security.

The figure below illustrates how an Information Management System works.



Section 4 requires organization to understand its business context, threats and opportunities, stakeholders and their expectations, and determine the scope and boundaries of the security management system. Section 5 requires the leadership team of the organization to establish the security management system that includes establishing policies, defining roles and responsibilities, providing resources etc. Section 6 requires organization to develop objectives and plan for the ISMS. Section 8 addresses implementation of the ISMS plan where main activity is risk assessment and developing risk mitigation plan. Annex A provides a list of security controls. Organizations implement the controls as means of mitigating risks. Section 9 requires organizations to establish a performance measurement system to monitor the effectiveness of the ISMS. One of monitoring process steps is management review, where senior management is required to review performance of the ISMS. Section 10 addresses the corrective action system to address any deviations found in section 9. Section 10 also provides requirements for improvements. Sections 6, 8, 9 and 10 drive a continuous improvement cycle. Section 7 provides requirements for the support functions like resource management, training, and document management.

Please remember that no security certification guarantees protection from hacking. All the cases discussed clearly show that security controls are not effective without management support. ISO 27001 is the only standard on information security that provides a management system framework in addition to the security controls.

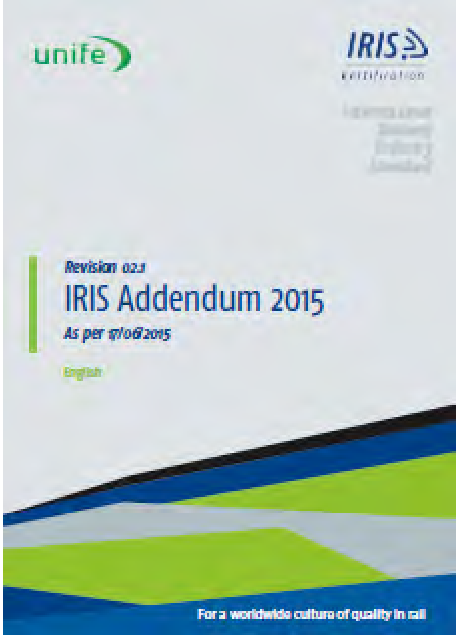
Subrata Guha
Director, IT Services
DQS Inc., USA

New developments for the International Railway Standard IRIS

Interesting news from Brussels: the board of Union des Industries Ferroviaires Européennes (UNIFE), the European railway industry's umbrella organization, has decided to elevate IRIS to an ISO standard.

Mark Manly, Chairman of the IRIS steering committee, announced that the development will be speeded up by applying the ISO "fast-track" procedure. The objective is to move the publication of an ISO railway standard forward similar to the transition period for the upcoming ISO 9001:2015, and to be ready by the fourth quarter, 2018.

In further news, the IRIS Management Centre has launched the IRIS Addendum 2015. It will simplify the evaluation process by introducing an assessment sheet as the new mandatory tool for auditors to be used during the evaluation of a company instead of the current questionnaire. This assessment sheet will also be useful for the audited company as well, offering much clearer feedback and more concrete examples of good practices to implement. Moreover, the IRIS Addendum 2015 creates a complete product scope for infrastructure companies by enlarging the existing scope 19.



unife

IRIS Certification

[illegible]

Revision 02.1

IRIS Addendum 2015

As per 17/06/2015

English

For a worldwide culture of quality in rail

You can find the IRIS Addendum 2015 in the Download Area, on the home page of the IRIS website www.iris-rail.org.

Following this IRIS Addendum 2015, the IRIS Audit-Tool (available for IRIS members only) has been updated as well. The version 4.2.0.00 manages all changes provided by the IRIS Addendum 2015, thus it contains now the entire set of requirements including the ISO 9001:2008 one.

The upgrade of the current IRIS Audit-Tool to V 4.2.0.00 has to be done via the current version. By opening the Audit-Tool a message for upgrade will appear. By downloading and installing this upgrade, the client accepts the payment conditions.

Starting in 2016, the "IRIS Revision 03 – Working Group" will then start to work on Revision No. 3, which will see the implementation of the new requirements of ISO 9001:2015, and which is planned for publication in 2017. Until then, Revision 02.1 with Addendum 2015 will be applicable for certification purposes.
This news was added to the IRIS Portal.
To find more information and related material (documents for download) please visit the IRIS portal: www.iris-rail.org
To inquire about certification to IRIS, please contact your local DQS office, a complete list of which can be found at www.dqs-holding.com.

Hans Jahn
DQS Product Manager, IRIS
hans.jahn@dqs.de

BRC Packaging Issue 5: An Overview of the Main Changes

On July 1st 2015, the British Retail Consortium published the latest issue of its Global Standard for Packaging and Packaging Materials. The standard, which has been updated to reflect the changing requirements and expectations of the various stakeholders, will be valid from January 1st, 2016 onwards. To help you prepare for certification, we have compiled an overview of the main changes in Issue 5.

Structure & Fundamentals

Like before, the BRC Packaging Standard distinguishes two main categories, with separate requirements. Whether a product falls in one category or the other depends on the intended use of the product. To reflect the fact that the intended use rather than the level of risk is the determining factor, the names of these categories have been changed: „high hygiene risk“ is now called „high hygiene“, „low hygiene risk“ becomes the category „basic hygiene“. High Hygiene relates to those items that are intended to come into direct contact with food or other hygiene sensitive product, while Basic Hygiene is intended for all other items, such as labels applied to other packaging materials through to the manufacture of tertiary (transit) packaging.

Except for changes in the numbering, the eight so called Fundamentals remain unchanged.

Evaluation System

An excellence level has been introduced to foster continuous improvement. The new classification “AA” is geared towards sites that have already reached the Grade A. Sites with less than 5 minor nonconformities can achieve the excellence level. The maximum possible number of minors of the previous category A remains unchanged.

Unannounced Audits & Additional Modules

The audit protocol now provides the opportunity to conduct unannounced audits. This is entirely optional. There is also the option to include additional modules in the audit. At the moment, there are two optional modules available: Traded Goods (also known as factored goods) and the Environmental Awareness Module (EAM).

Time Plan

After the publication of the new BRC Packaging Standard on July 1st, 2015, there is a transition period of six months. The use of Issue 5 is compulsory for all certification audits taking place from January 1st, 2016 onwards. Prior to that date, it is not possible to be certified according to the new version.
For more detail re. the changes per chapter, please visit www.dqs-cfs.com. The standard can be downloaded from the BRC Bookshop free of charge, but a quick registration is necessary.

Dr. Thijs Willaert
Communications Manager
DQS CFS GmbH

BRC Storage & Distribution

Certification according to BRC Food standards, BRC Packaging and Consumer Products have been part of the service spectrum of DQS since quite some time. Now, certification according to BRC Storage & Distribution was added to the service portfolio of DQS CFS. This means that DQS is now able to make offers and do audits against this standard according to BRC016.

We would also like to inform you that a new version of BRC Storage & Distribution will be developed. The release of version 3 is planned for spring 2016. It is expected that the first certification audits according to the new version will be carried out in autumn 2016.

The Global Standard for Storage and Distribution provides the essential certification link between the range of BRC manufacturing Standards and the end user, the retailer and the food service company. The Standard ensures best practice in handling storage and distribution of products and promotes continuous improvement in operating practices.

To read more visit: www.dqs-cfs.com

Reminder: BRC Food Version 7 now applicable

In case you missed this: Version 7 was published on 7 January 2015 and has been required for audits since 1 July, 2015. If you want to know more about the changes, visit www.dqs-cfs.com

To find out more about the services and certifications by DQS Group, please contact the office nearest you.
The list of international offices can always be found at

published by

DQS Holding GmbH
August-Schanz-Str. 21
60433 Frankfurt am Main
Germany
Tel. +49 69 95427-0
Fax +49 69 95427-111
www.dqs-holding.com

responsible for content
Martina Meinefeld and Ilona Korall
Tel. +49 69 95427-339
martina.meinefeld@dqs.de

compiled and translated by
Petra Träm

editorial dept. and layout
kompri, Triefenstein

The customer journal of DQS Group is published several times per year. Reprinting of articles, partially or in full, permitted after consultation with the editorial dept. and when stating the source.

october/2015