Vol. 9, No. 1 January-February 2009

ISO Management Systems

When Results Count. ISO Standards.

ISSN 1680-8096

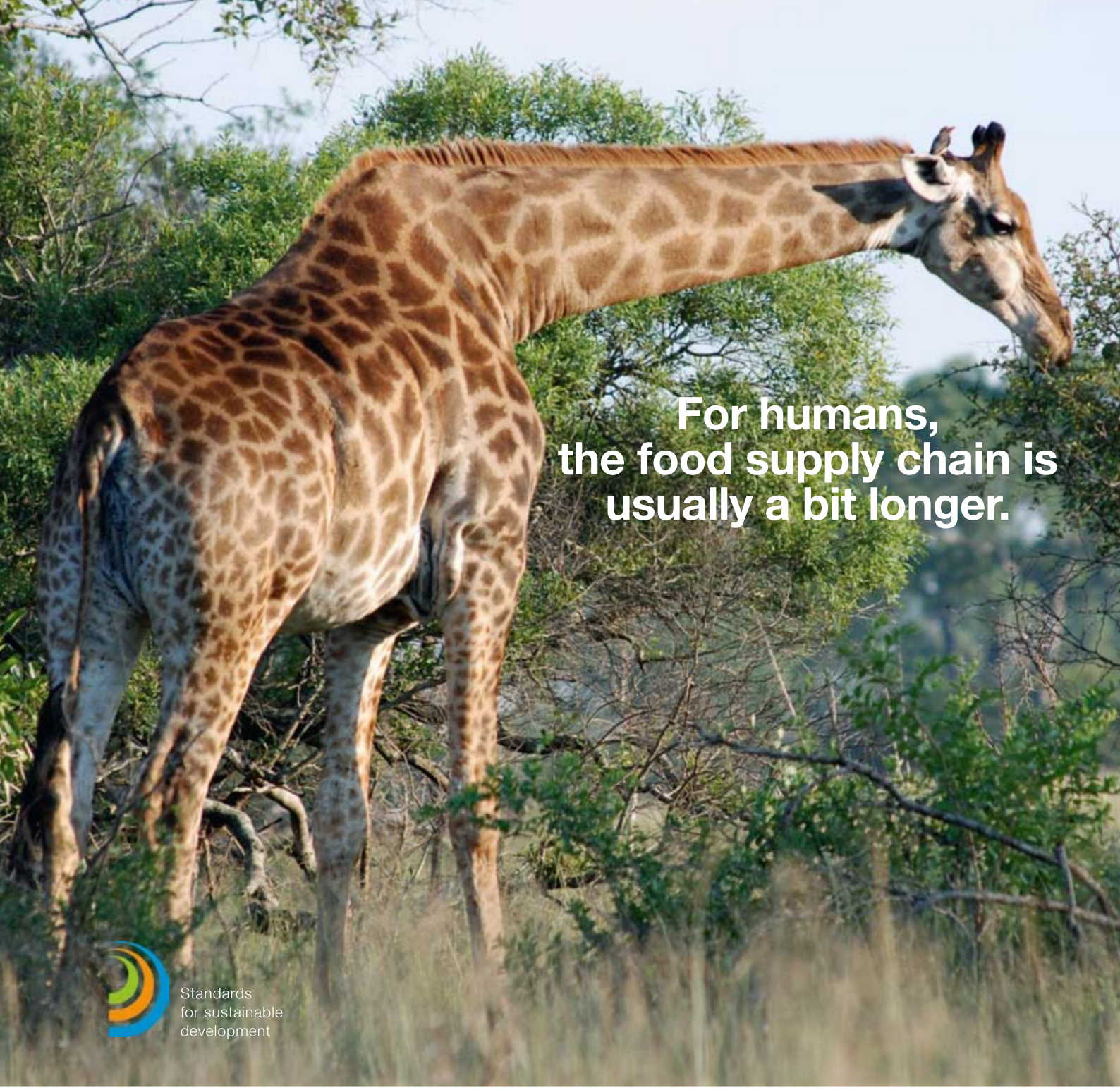
- ISO 9000 video
- ISO 50001 and energy
- Standards and sustainability

ISO/IEC 27001 for SMEs

"Big D" becomes "Green D"

ISO 22000 and a million daily meals

Ship registry and ISO 9001



The ISO Pack on Food Safety Management Systems on CD.

The supply chain that puts food from the farm on to our table is a bit longer than in nature. It can stretch across continents and include producers, processors, transport and storage operators, and retail outlets. **The ISO 22000 family of standards** helps all types of operator in the supply chain to implement management systems that ensure the food we eat is safe. **The ISO Pack on Food Safety Management Systems** includes on one CD the entire ISO 22000 family of standards, in **English** and in **French**. It costs just 379 Swiss francs (about USD 340 – EUR 231).

Available from ISO national member institutes (listed with contact details on the ISO Web site at **www.iso.org**) and from the ISO Central Secretariat Webstore at **www.iso.org/isostore** or e-mail to **sales@iso.org**.

ISBN 978-92-67-01166-0

International Organization for Standardization

Central Secretariat
1, ch. de la Voie-Creuse
Case postale 56
CH-1211 Geneva 20

by Roger Frost

You can count on ISO standards

You may have noticed that there is a slogan under the ISO Management Systems *title on the cover page of the magazine. The slogan reads: "When Results Count. ISO Standards."*

Given our emphasis on ISO's management system standards and the results they deliver for users – as reported by the users themselves – it's easy to forget that ISO has more than 17 400 "other" International Standards and related documents to offer.

The sheer scale of the implementation of some of them, for example, the metric system, makes it rather difficult, if not impossible, to come up with precise, totally accurate data on the results they help to achieve.

Another complication is that a number of standards, such as for freight container dimensions and many information technology standards, provide benefits not only for specific users like the transport and IT sectors, but potentially for all sectors. Indeed, it could be argued that some standards like these provide spin-off benefits for much of the world's population.

Some standards provide **spin-off benefits for much of the world's population**

It is relatively simple for individual users of ISO management system standards to calculate the benefits that they bring their organizations. For the reasons given above, it is often necessary to have recourse to estimations and projections to convey an idea of the results delivered by other standards.

The following examples, large and small, cover both management systems and "other standards" – and include a striking negative example.

• MPEG-2

The MPEG-2 coding standard has facilitated the worldwide growth of the digital television and DVD industries, including the diffusion of some 3.5 billion DVD machines and 40 billion DVDs. an estimated market of USD 2.5 trillion.

• Product data exchange

The ISO Standard for Exchange of Product Data (STEP), which addresses the exchange of digital product information, has been calculated as having the potential to save USD 928 million a year by reducing interoperability problems in the automotive, aerospace and shipbuilding industries alone.

• Freight containers

It is estimated that more than 90 % of the world trade in non-bulk goods is transported in freight containers conforming to ISO specifications. Containerization has reduced the time and cost of moving goods across the oceans to market by 84 % and 35 % respectively.

• Space

The failure to adhere to the international metric system of measurement (now the ISO 80000 series) cost US taxpayers USD 125 million at the end of September 1999 when NASA's Mars Climate Orbiter was lost in space because engineers had failed to make the conversion from Imperial units to metric, a costly mistake that sent the spacecraft fatally close to the surface of Mars.

Counting on ISO standards

• Oil and gas

A multinational company calculated that if the systematic use of ISO standards could be expected to save 1 % of the industry's annual expenditure, then the saving would amount to USD 180 million and represent a return on investment of 25 to 1.

• Concrete

It is estimated that the world trade in concrete is USD 13-14 trillion and that implementing ISO standards could increase this by 1-2 % over a decade. With an annual production of concrete estimated to be 15 billion tons and about 1 % of the world's population having jobs that directly relate to the concrete construction industry, the value of ISO standards impacting the world trade in concrete, the quality and longevity of concrete and the environmental impact of concrete production is potentially enormous.

• Cranes

Maintenance programmes based on International Standards of the millions of cranes in use around the world are estimated to save USD 3 billion annually.

• Petroleum company

Average benefits of ISO 9000 implementation were some nine times the costs over the first year.

• International development bank

An ISO 14001-based resource conservation programme helped save over USD 250 000 through electricity, water, paper, and solid waste reduction at its HQ from 2003 to 2006.

• City council

As a result of a combined ISO 9000 and risk management programme implemented by a city council, its insurer waived an 8 % increase in its premium.

CONTENTS

ISO MANAGEMENT SYSTEMS is published six times a year by the Central Secretariat of ISO (International Organization for Standardization) and is available in English, French and Spanish editions.

Publisher: ISO Central Secretariat, 1, ch. de la Voie-Creuse, Case postale 56, CH-1211 Geneva 20, Switzerland.
Tel. + 41 22 749 01 11.
Fax + 41 22 733 34 30.
E-mail central@iso.org
Web **www.iso.org**

Editor in Chief: Roger Frost.
Contributing Editor: Garry Lambert.

Artwork: Pascal Krieger and Pierre Granier.

A one-year subscription (six issues) to *ISO MANAGEMENT SYSTEMS* costs 128 Swiss francs.

Subscription enquiries: Sonia Rosas-Friot, ISO Central Secretariat.
Tel. + 41 22 749 03 36.
Fax + 41 22 749 09 47.
E-mail sales@iso.org

Advertising enquiries:
ISO Central Secretariat,
Case postale 56, CH-1211 Geneva 20, Switzerland.
Contact: Régis Brinster.
Tel. + 41 22 749 02 44.
E-mail brinster@iso.org

ISSN 1680-8096

Cover photo: Montage ISO

by **Robert Page**

ISO/TC 207 can get even better

Dr. Robert Page has succeeded Mr. Daniel Gagnier as the new Chair of ISO/TC 207. Dr. Page is currently the TransAlta Professor of Environmental Management and Sustainability, Energy and Environmental Systems Group, Institute for Sustainable Energy, Environment, & Economy, University of Calgary, Canada, where he is also an Adjunct Professor in the Haskayne School of Business. He is also the acting Chair of the Government of Canada's National Round Table on the Environment and the Economy (NRTEE).

He is known nationally and internationally for his work on energy and the environment in areas such as climate change, emissions trading, biodiversity and protected spaces, environmental impact assessment, and policy and regulation.

Dr. Page has served for the Government of Canada in international negotiations on the Conference of the Parties for the Kyoto Protocol, the North American Free Trade negotiations, and trade and the environment.

It was a great honour for me to accept the nomination as the Chair of ISO technical committee ISO/TC 207, *Environmental management*. I have had the pleasure to know several past Chairs of this eminent committee, such as George Connell and Daniel Gagnier, and will work to build on their important legacy.

It has been over 20 years since Ms. Gro Harlem Brundtland authored *Our Common Future*, the seminal report of the United Nations Commission on Environment and Development. This report introduced the concept of sustainable development to the world as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs".

Ms. Bruntland's report recognized that sustainable development in practice required the integration, or a systems view, of economy, society and environment. It recognized the needs of the world's poor and the inherent limitations on what the Earth's environment can support. Organizations large and small, governmental, business or non-governmental, have been trying to operationalize the concept of sustainable development ever since.

Since 1996, ISO/TC 207 standards have made a significant and important contribution to sustainable development. Born out of the 1991 Rio Earth Summit, ISO/TC 207 has epitomized that Summit's Agenda 21 and its focus on how governments, enterprises and non-governmental organisations could co-operate to achieve sustainable development.

While a success against any measure, ISO/TC 207 and its ISO 14000 family of standards now compete in a more crowded market-place addressing a myriad of environmental and sustainability issues.

Integrative thinking

New challenges include the "fragmentation" of environmental issues and analysis – which needs to be balanced with integrative thinking that recognizes inter-relationships and cause-effect relationships.

The need for public credibility and market relevance has never been greater, but must be balanced against the rigour and decentralized participation inherent in the ISO process. The role of developing countries, and their active participation, in ISO and ISO/TC 207 remains critical not only our credibility, but also to finding consensus on global environmental issues.

ISO/TC 207 is built on incredible foundations – its institutional strength, global reach and collective will to develop standards that matter. It is against this backdrop that ISO/TC 207 can get even better, to address calls for greater market relevance and more effective tools.

Continuity and **change** should not be viewed as competing visions

Continuity and change should not be viewed as competing visions, but as a necessary and powerful reality in today's world. In ISO/TC 207, the axiom "things must change so they can remain the same" is an operating principle.

Within this context, it is my sincere belief that the collective expertise, ability and commitment of our standards experts – from all walks of life and corners of the world – can and will increase the "sustainability footprint" of ISO standards. •

Contact: ISO/TC 207 Secretary, Kevin Boehmer.

E-mail kevin.boehmer@csa.ca

Web www.tc207.org

Web www.csa.ca

Information security management systems for small and medium-sized enteprises

Although many large organizations have been quick to see the benefits of ISO/IEC 27001:2005 – the information security management system standard – many SMEs have been slow adopters because of a lack of basic advice in its implementation. This will change with development of a new ISO handbook to demystify the process, due for publication in 2009.

by **Edward Humphreys**

Visiting Professor ***Edward Humphreys*** *(FH University of Applied Science, Hagenberg, Upper Austria), is Convenor of ISO/IEC JTC 1,* Information technology, *subcommittee SC 27,* IT security techniques, *working group WG 1,* Information security management systems.

E-mail edwardj7@msn.com

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements,* is one of a family of information security management systems (ISMS) standards (**see box**) for use by all organizations regardless of size and sector.

Well over 5000 organizations have already certified their ISMS in conformity with ISO/IEC 27001, and many more are in process of doing so – testimony to its broad applicability in helping protect business assets and information, and the reason why the ISMS strandard has become the common information security language within and between many different types of enterprise.

However, while many large organizations have been quick to see the benefits, many small to medium sized enterprises (SMEs) are still slow to adopt the standard because of a lack of basic advice on its implementation.

Help will shortly be at hand following the development of a new ISO handbook designed to provide much needed guidance on ISO/IEC 27001 implementation for SMEs from all sectors, due for publication in 2009. This article provides a preview.

Two approaches

The handbook will offer a "step-by-step" or "all-at-once" approach to implementation depending on the SME resources available. It explains that, irrespective of the size and nature of the SME , ISO/IEC 27001 implementation does not need to be costly or resource intensive.

Step-by-step ISMS implementation enables the SME to be able to achieve a basic level of cost-effective protection without much effort. And by following two to three more steps, the organization can achieve a fully ISO/IEC 27001-conforming ISMS when appropriate to the business.

Basic protection

All organizations need a baseline of security to provide a minimum level of protection. For example, virus attacks can threaten any organization, including SMEs. They should have back-up systems in place to protect against information loss or destruction, and ensure physical protection of personnel data and equipment.

SMEs are still slow to adopt ISO/IEC 27001

ISO/IEC 27002:2005 provides a code of practice that describes the necessary controls for basic protection, including:

- a policy for high level information security management;
- user awareness;
- antivirus software;
- backup;
- access controls;
- physical protection of premises and commercially sensitive paper-based files and documents;
- protection of personnel data and company records.

ISO/IEC 27002 Control Questions	Yes	Partial	No	Comments
Do you have software implemented in your computers to detect, prevent and recover from a malicious code attack (e.g. from a virus attack)?		4		Not all the computers in the business have this software installed.
Do all your staff know about the dangers of malicious code attack (e.g. from a virus attack) and are they trained in the use of the software used to detect, prevent and recover from such attacks?		4		
Do you regularly update the software used to detect, prevent and recover from a malicious code attack (e.g. from a virus attack)?	4			

Figure 1 – *Example of a typical information security gap analysis.*

Implementing a basic level of protection is an appropriate starting point for any SME, beginning with a simple gap analysis to identify the protection already in place, and what it lacks. Above is a typical gap analysis checklist using the controls listed in ISO/IEC 27002 (see **Figure 1**).

ISMS policy

An information security policy statement can be a one-page document from senior management listing policy objectives and commitment, displayed in the organization's premises. This is a simple but effective daily reminder to employees of the importance of information security.

Risk assessment

The objective of a risk assessment is to identify the risks confronting an SME so that an appropriate set of information security controls can be implemented to reduce those risks to an acceptable level.

Yet risk assessment is seen by many SMEs as a formidable and time-consuming task requiring substantial resources. It does not need to be so. To extend SME information protection beyond the baseline level requires a risk assessment exercise. However, the steps involved are quite straightforward as explained in the forthcoming ISO handbook.

The baseline controls mentioned are designed to reduce specific risks – such as antivirus software to reduce the

The ISO/IEC 27000 family

The ISO/IEC 2700 family of information security management standards currently comprises four publications:

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*

ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management*

ISO/IEC 27006:2007, *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems*

The principal standard, ISO/IEC 27001:2005, covers all types of organizations (e.g. commercial enterprises, government agencies, not-for-profit organizations), and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's overall business risks.

It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties, and is intended to be suitable for several different types of use, including the following:

- use within organizations to formulate security requirements and objectives
- use within organizations as a way to ensure that security risks are cost effectively managed
- use within organizations to ensure compliance with laws and regulations
- use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met
- definition of new information security management processes
- identification and clarification of existing information security management processes
- use by the management of organizations to determine the status of information security management activities
- use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization
- use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons
- implementation of business-enabling information security
- use by organizations to provide relevant information about information security to customers.

risk of a virus attack, back-ups to minimize the risk of data loss through system failures, physical protection to lower the risk of equipment and documentation theft.

ISO/IEC 27001 implementation **does not need** to be costly

Typical vulnerabilities identified by risk assessment can include:

- *On-line information theft and fraud*

This inclues on-line auction frauds, "phishing" (e-mail disguised as official bank communication), "419" scam letters, and numerous other deceptions designed to lure users to part with personal information, bank and credit card details, social security numbers or passwords.

- *System failures*

These can can shut down an SME's IT system and disrupt normal business activity for days with possibly serious effects on revenue and competitiveness.

- *Software problems*

These includes bugs, viruses, out of date programs and unauthorised access which can compromise information security.

- *Misuse of company resources*

These can done by external users or SME staff, whether accidental or intentional, and

can result in breaches of information security.

- *Delayed response to security incidents*

Immediate reporting of any potential security risks should be routine with measures taken to correct the problem before it can have a negative impact on the organization.

The risk assessment should only focus on those areas requiring protection to avoid unnecessary expenditure on information security solutions covering less risky areas of the business.

Regardless of the measures taken, it is impossible to reduce information security risks to zero. The SME should implement the necessary controls to reduce the risks to an acceptable residual level without overspending on information security measures. There is a point at which the benefits gained are outweighed by the cost of implementing more and more security.

The new handbook will **demystify** ISO/IEC 27001

Maintaining an ISMS

Implementing the controls set out in ISO/IEC 27001 is an important aspect of protecting information, but just as important is maintaining the day-to-day effectiveness of the ISMS. If the system is not regularly managed then the investment in security can be wasted.

It is impossible to reduce information security risks to **zero**

Managing its information security enables an SME to make system improvements and upgrades when necessary to protect its investment in security. This involves regular monitoring, and reviewing any changes in operations that might affect the level of protection that has been implemented.

If changes in business conditions are significant enough to increase information security risks, then the SME will have to consider changing the set of ISMS controls to counter the new risks. Regular reviews not only ensure the continuing effectiveness of the system, but can be far more cost effective than more substantial periodic system upgrades.

Better protection

In this article, I have highlighted some of the advice given in the forthcoming ISO handbook. It will also include checklists, scorecards and case studies to help SMEs focus on the key aspects of protecting their business information using ISO/IEC 27001 as the ISMS tool. In essencethe new handbook will help to simplify and demystify ISO/IEC 27001 requirements and give SMEs a clearer understanding of how best to protect their businesses. •

ISO publishes new edition of ISO 9001

by **Roger Frost**

ISO has published ISO 9001: 2008, the latest edition of the International Standard used by organizations in 175 countries as the framework for their quality management systems (QMS).

ISO 9001:2008, *Quality management system – Requirements,* is the fourth edition of the standard first published in 1987 and which has become the global benchmark for providing assurance about the ability to satisfy quality requirements and to enhance customer satisfaction in supplier-customer relationships.

ISO 9001:2008 contains no new requirements compared to the 2000 edition, which it replaces. It provides clarifications to the existing requirements of ISO 9001:2000 based on eight years' experience of implementing the standard worldwide and introduces changes intended to improve consistency with the environmental management system standard, ISO 14001:2$004.

All ISO standards – currently more than 17400 – are periodically reviewed. Several factors combine to render a standard out of date, such as technological evolution, new methods and materials, new quality and safety requirements, or questions of interpretation and application. To take account of such factors and to ensure that ISO standards are maintained at the state of the art, ISO has a rule requiring them to be periodically reviewed and a decision taken to confirm, withdraw or revise the documents.

ISO/TC 176, which is responsible for the ISO 9000 family, unites expertise from 80 participating countries and 19 international or regional organizations, plus other technical committees. The review of ISO 9001 resulting in the 2008 edition was carried out by subcommittee SC 2 of ISO/TC 176.

User survey

This review has benefited from a number of inputs, including the following: a justification study against the criteria of ISO Guide 72:2001, *Guidelines for the justification and development of management system standards*; feedback from the ISO/TC 176 interpretations process; a two-year systematic review of ISO 9001:2000 within ISO/TC 176/SC2; a worldwide user survey carried out by ISO/TC 176/SC 2, and further data from national surveys.

ISO Secretary-General Alan Bryden commented: "The revised ISO 9001 results from a structured process giving weight to the needs of users and to the likely impacts and benefits of the revisions. ISO 9001:2008 is therefore the outcome of a rigorous examination confirming its fitness for use as the international benchmark for quality management.

ISO/TC 176/SC 2 has also developed an introduction and support package of documents explaining what the differences are between ISO 9001:2008 and the year 2000 version, why and what they mean for users. These documents are available on the ISO Web site.

Although certification of conformity to ISO 9001 is not a requirement of the standard, it is frequently used in both public and private sectors to increase confidence in the products and services provided by certified organizations, between partners in business-to-business relations, in the selection of suppliers in supply chains and in the right to tender for procurement contracts. Up to the end of December 2007, at least 951486 ISO 9001:2000 certificates had been issued in 175 countries and economies.

ISO has also developed **an introduction and support package**

ISO (which does not itself carry out certification) and the International Accreditation Forum (IAF) have agreed on an implementation plan to ensure a smooth transition of accredited certification to ISO 9001:2008. The details of the plan are given in a joint communiqué by the two organizations which is available on the ISO Web site.

ISO 9001:2008, *Quality management system – Requirements*, costs 114 Swiss francs and is available from ISO national member institutes (listed with contact details on the ISO Web site **www.iso.org**) and from ISO Central Secretariat (**sales@iso.org**).

ISO launches video clip: "The ISO 9000 family – Global management standards"

by **Roger Frost**

ISO has just launched a video clip in which users share their perspectives of earlier ISO 9001 editions and other standards in the ISO 9000 family which has become the global benchmark for qualtiy management systems.

The ISO 9000 family – Global management standards takes the form of a fictional television business news report on ISO 9000 in which real users speak from their personal experience in the varied contexts of multinational industry, a humanitarian aid organization and a police department, which ISO says underlines the combination of flexibility, efficiency and effectiveness of the ISO 9000 approach.

ISO Secretary-General Alan Bryden comments: "Whenever the ISO 9000 family is evoked, the emphasis is usually on ISO 9001 certification. This video is refreshing because the users emphasize the importance and benefits of ISO 9000 aspects such as management commitment, metrics, customer focus, continual improvement, knowledge transfer, cost savings and the eight quality management principles."

Users emphasize the **importance and benefits** of ISO 9000 aspects

The video includes interviews with ISO 9000 users from: the international oil and gas industry; the Cambodia Trust, a humanitarian aid organization with headquarters in the United Kingdom, and the Phoenix Police Department, Arizona, USA.

The ISO 9000 family is developed and maintained by ISO technical committee ISO/TC 176, *Quality management and quality assurance.*

The video concept was created by Communication Services, ISO Central Secretariat (ISO/CS). Post-production by Communication and Information services (ISO/CS) and Taurus Studio (sound). Geneva, Switzerland **www.taurus-studio.com**. Production input by Trueworld Communications, United Kingdom, **www.trueworld**.media.officelive.com

The ISO 9000 family – Global management standards can be downloaded free of charge from ISO's Web site. It is also available (English only) in high resolution on DVD in PAL (ISBN 978-92-67-10485-0) and NTSC (ISBN 978-92-67-10486-7) versions for being shown in conference settings. The DVD version is also free, although postage and handling will be charged. It is available from ISO national member institutes (listed with contact details on the ISO Web site **www.iso.org**) and from ISO Central Secretariat (**sales@iso.org**). •

50001 – future management system standard for energy

by **Edwin Pinero** and **Jason Knopes**

ISO has identified energy management as one of the top five fields[1] meriting the development and promotion of International Standards. Effective energy management is a priority focus because of the significant potential to save energy and reduce greenhouse gas (GHG) emissions worldwide.

1) Priorities also include calculation methods, biofuels, retrofitting and refurbishing, and buildings as determined by the ISO Council Standing Committee on Strategies Energy Task Force in 2007.

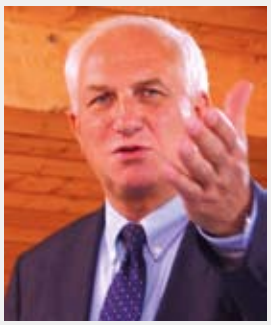
Existing ISO standards for quality management systems (ISO 9000 series) and environmental management systems (ISO 14000 series) have successfully stimulated substantial, continual efficiency improvements within organizations around the globe. An energy management standard is expected to similarly achieve major, long-term increases in energy efficiency – 20 % or more in industrial facilities[2].

ISO 50001 will provide strategies to **increase** energy efficiency, **reduce** costs, and **improve** environmental performance

Early on, the United Nations Industrial Development Organization (UNIDO) recognized industry's need to mount an effective response to climate change and to the proliferation of national energy management standards.

In March 2007, UNIDO hosted a meeting of experts, including representatives from the ISO Central Secretariat and nations that have adopted energy management standards. That meeting led to submission of a UNIDO communication to the ISO Central Secretariat requesting that ISO consider undertaking work on an international energy management standard.

A pressing need



"The urgency to reduce GHG emissions, the reality of higher prices from reduced availability of fossil fuels, and the need to promote efficiency and the use of renewable energy sources provide a strong rationale for developing this new standard, building on the most advanced good practices and existing national or regional standards."

Alan Bryden
ISO Secretary-General
2003-2008

Discussions between US experts and ISO's US member, the American National Standards Institute (ANSI) led to a formal proposal for ISO to establish a committee on this subject. In February 2008, the ISO Technical Management Board (TMB) approved the establishment of a new project committee, ISO/PC 242, *Energy management,* to develop the future ISO 50001 management system standard for energy.

ANSI is serving as the committee Secretariat in partnership with ISO's national member for Brazil, *Associação Brasileira de Normas Técnicas* (ABNT).

International framework

The future ISO 50001 will establish an international framework for industrial and commercial facilities, or entire companies, to manage all aspects of energy, including procurement and use. The standard will provide organizations and companies with technical and management strategies to increase energy efficiency, reduce costs, and improve environmental performance.

Based on broad applicability across national economic sectors, the standard could influence up to 60 % of the world's energy demand[3]. Corporations, supply chain partnerships, utilities, energy service companies, and others are expected to use ISO 50001 as a tool to reduce energy use and carbon emissions in their own facilities (as well as those belonging to their customers or suppliers) and to benchmark their achievements.

As part of the standard development process, ISO/PC 242 will define relevant terms and develop management system requirements along with providing guidance for use, implementation, measurement, and metrics associated with the standard.

To provide compatibility and integration opportunities with other management systems, it is anticipated that the standard will foster the same management system principles of continual improvement and use the Plan-Do-Check-Act cycle employed in ISO 9001 and ISO 14001.

The authors

Edwin Pinero is Chair of ISO/PC 242.

Jason Knopes is Secretary of ISO/PC 242.

It is envisioned that the future standard will provide organizations and companies with a recognized framework for integrating energy efficiency into their management practices. Multi-national organizations will have access to a single, harmonized standard for implementation across the organization with a logical and consistent methodology for identifying and implementing energy efficiency improvements. The standard will also:

- assist organizations in making better use of their existing energy-consuming assets;
- offer guidance on benchmarking, measuring, documenting, and reporting energy intensity improvements and their projected impact on reductions in GHG emissions;

2) McKane, et al, 2007 in UNIDO publication, *Policies for Promoting Industrial Energy Efficiency in Developing Countries and Transition Economies,* V.08-52434-April 2008.

3) *International Energy Agency International Energy Outlook 2007,* industrial and commercial world energy use

- create transparency and facilitate communication on the management of energy resources;
- promote energy management best practice and reinforce good energy management behaviour;
- assist facilities in evaluating and prioritizing the implementation of new energy-efficient technologies;
- provide a framework for promoting energy efficiency throughout the supply chain;
- facilitate energy management improvements in the context of GHG emission reduction projects.

The first meeting of ISO/PC 242 was held on 8-10 September 2008 near Washington D.C. The meeting was attended by more than 80 delegates from 25 ISO national member bodies from all regions of the world, as well as representation from UNIDO, which has liaison status with ISO/PC 242.

Excellent progress was made in the technical discussions and a first working draft has already been circulated for comment. A major point of discussion is the need to ensure compatibility with the existing suite of ISO management system standards. The committee therefore took the key decision to base the draft on the common elements found in all of ISO's management system standards. The 2nd ISO/PC 242 meeting will take place in Rio de Janeiro, Brazil in March 2009.

Energy leaders are encouraged to participate in their country's national mirror committee which will coordinate the country's participation in developing the standard. Contact information for ISO members in each country is available on ISO's Web site **www.iso.org**.

Countries wishing to actively participate and send representatives to ISO/PC 242 meetings should confirm their participation status with the ISO Central Secretariat (contact Trevor Vyze – **vyze@iso.org**) and should also inform the ISO/PC 242 Secretary, Jason Knopes, of ANSI (**JKnopes@ansi.org**) and Co-Secretary Felipe Viera, of ABNT, (**Felipe.Vieira@abnt.org.br**). •

How ISO contributes to a sustainable world

by **Roger Frost**

ISO has just published a new brochure providing a concise overview of how ISO's technical programme, which has so far produced more than 17 400 International Standards, contribute to a sustainable world.

ISO – a multi-sector, multi-stakeholder international organization – is the leader for the production of consensus-based International Standards. ISO's membership comprises the national standards bodies of 157 countries. This network is complemented by more than 600 international and regional partners and the participation of close to 100 000 experts.

The brochure is entitled *How ISO's technical programme and standards contribute to a sustainable world*. It explains how International Standards of the type developed by ISO, based on a double level of consensus, between stakeholders and between countries, contribute to the three dimensions of sustainable development – economic, environmental and social. They:

- support the facilitation of global trade, the dissemination of new technologies, good business practices and the relations between economic actors;

- support good environmental practice and information, energy efficiency and the dissemination of new, eco-friendly and energy performance technologies;
- contribute to consumer protection, safety at work, healthcare, security and other social interests which may require technical or management standards for the related products and services.

ISO Secretary-General Alan Bryden commented: "While the content of the majority of ISO standards is technical, their implementation goes beyond solving technical problems to delivering positive results in economic, environmental and societal spheres."

Survey

The new brochure is based on a survey launched in 2007 by the ISO Technical Management Board (TMB) of the technical committees that development ISO standards.

They were asked how they felt their standards contributed to sustainable development. The brochure gives a selection of examples provided by committees developing standards for energy, food, water, the environment, health, fire safety, building, transport, nanotechnologies, social responsibility and people with disabilities.

It also describes how ISO's standardization work benefits from strategic management and policy inputs that also contribute to sustainability. These inputs come from the TMB and ISO policy development committees for consumer affairs, developing countries and conformity assessment.

How ISO's technical programme and standards contribute to a sustainable world, 20 pages, A5 landscape format, is available in English (ISBN 978-92-67-10484-3) and French (ISBN 978-92-67-20484-0) editions, free of charge, from ISO national member institutes (listed with contact details on the ISO Web site **www.iso.org**) and from ISO Central Secretariat (**sales@iso.org**). It can also be downloaded as a PDF file from the ISO Web site. •

ISO Guide will help reduce environmental impacts of products

by **Sandrine Tranchard**,
Communication Officer, ISO Central Secretariat

ISO has published an updated edition of its guide to reducing the potential environmental impact of products by taking environmental aspects into account in product standards.

Every product has an impact on the environment during all stages of its life-cycle, from extraction of resources to end-of-life treatment and the need to reduce the potential adverse impacts on the environment of a product is recognized around the world.

The newly published ISO Guide 64:2008, *Guide for addressing environmental issues in product standards,* is a practical tool for addressing these issues, as well as a contribution to sustainable international trade.

This Guide is intended for use by all those involved in the drafting of product standards. Standards writers are not expected to become environmental experts but, by using this Guide, they are encouraged to:

- identify and understand basic environmental aspects and impacts related to the product under consideration; and
- determine when it is possible and when it is not possible to deal with an environmental issue through a product standard.

However, the identification of these aspects and the prediction of their impacts is a complex process. When writing a product standard, it is

important to ensure that an evaluation as to how products can affect the environment at different stages of their life-cycle is carried out as early as possible in the process of developing the standard.

Step-by-step

ISO Guide 64:2008 proposes a step-by-step approach, based on the principle of life-cycle analysis, in order to promote a reduction of potential adverse environmental impacts caused by products.

The implementation of ISO Guide 64:2008 will help to make standards writers aware of how it is possible to make an effective contribution to environmental improvement through a product standard, and how to reduce potential adverse environmental impacts of products.

Through a helpful tool (the environmental checklist), the writer of product standards can assess the relevant product environmental aspects, based on the availability of environmental information, product and environmental knowledge and the application of life-cycle analysis.

Primarily intended for product standards writers, the objectives of ISO Guide 64:2008 are to:

- outline the relationship between the provisions in product standards and the environmental aspects and impacts of the product;
- assist in drafting or revising provisions in product standards in order to reduce potential adverse environmental impacts at different stages of the entire product life-cycle;
- emphasize that taking into account environmental issues in product standards is a complex process and requires balancing competing priorities;
- recommend the use of life-cycle analysis when defining environmental provisions for a product for which a standard is being drafted; and
- to promote the future development of relevant sector guides for addressing environmental issues in product standards by standards writers, consistent with the principles and approaches of this Guide.

Taking into account **environmental issues in product standards** is complex

ISO Guide 64: 2008, *Guide for addressing environmental issues in product standards*, was developed by the Working Group, *Inclusion of environmental aspects in product standards*, ISO/TC 207, *Environmental management*. It costs 132 Swiss francs and is available from ISO national member institutes (listed with contact details on the ISO Web site **www.iso.org**) and from ISO Central Secretariat (**sales@iso.org**).

Material flow cost accounting with ISO 14051

by **Katsuhiko Kokubu, Marcelo Kos Silveira Campos, Yoshikuni Furukawa,** and **Hiroshi Tachikawa**

Material flow cost accounting (MFCA), an environmental management accounting developed in Germany in the late 1990s and since adopted widely in Japan, focuses on tracing waste, emissions and non-products, and can help boost an organization's economic and environmental performance.

To standardize MFCA practices, working group (WG) 8 of ISO technical committee ISO/TC 207, *Environmental management*, is currently working on the development of ISO 14051, *Environmental management – Material flow cost accounting – General framework*, targeted for publication early in 2011.

ISO 14051 will be complementary to the ISO 14000 family of environmental management system standards (EMS), including life cycle assessment (ISO 14040, ISO 14044), environmental performance evaluation (ISO 14031), and the

greenhouse gas management standards (ISO 14064-1-3, ISO 14065).

In this article, the basic concept and application of MFCA, and development of the new International Standard are explained.

A vital social issue

Climate change, environmental legislation, and the global economy are in the headlines more than ever, highlighting the fact that effective management of environmental and economic affairs has become a vital social issue. In response, manufacturers and other businesses are under pressure to increase productivity while reducing environmental impact.

MFCA can help organizations to achieve such objectives by identifying emissions and waste within a process in cost and physical terms. Such precise data can motivate managers to enhance material productivity and significantly reduce waste far more effectively than relying only on conventional production and cost accounting information.

The original concept of MFCA was developed in Germany by Professor Bernd Wagner and colleagues at IMU (Institute für Management und Umwelt) in Augsburg, Germany, and introduced in Japan around 2000.

Many Japanese companies have since adopted MFCA, supported by the Japanese Ministry of Economy, Trade and Industry. In 2008, the Japanese Industrial Standards Committee (JISC) submitted an MFCA proposal to ISO/TC 207, resulting in the creation of a new working group, WG 8, in March 2008, to develop ISO 14051.

MFCA explained

MFCA is a management information system that traces all input materials flowing through production processes, and measures output in finished products and waste.

For example, where 100 kg of materials is input into a production process and 70 kg of finished products is obtained, 30 kg of waste has also been produced. An equivalent cost evaluation of the finished product and waste can then be made.

The authors

Katsuhiko Kokubu *is Convenor of ISO/TC 207/WG 8 and Professor, Graduate School of Business Administration, Kobe University.*

E-mail kokubu@kobe-u.ac.jp

Marcelo Kos Silveira Campos *is Co-convenor of ISO/TC 207/WG 8 and Director, Industrial Affairs, Brazilian Chemical Industry Association.*

E-mail marcelo@abiquim.org.br

Yoshikuni Furukawa *is Secretary of ISO/TC 207/WG 8 and General Manager, Sustainable Management, Government Relations Department, Nitto Denko Corporation.*

E-mail yoshikuni_furukawa@gg.nitto.co.jp

Hiroshi Tachikawa *is Assistant Secretary of ISO/TC 207/WG 8 and Managing Director, Propharm Japan Co. Ltd.*

E-mail hiroshi.tachikawa@propharm.jp

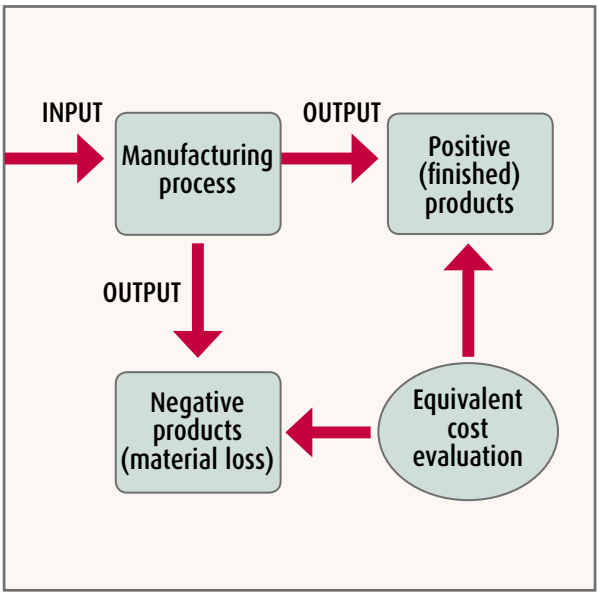


Figure 1 – *The concept of material flow cost accounting.*

MFCA can boost economic and environmental performance

In MFCA, finished products and waste are respectively termed positive and negative products. The essential point of MFCA is to recognize waste as non-marketable (second) products in the sense that materials are consumed and manufacturing facilities are used (see **Figure 1**).

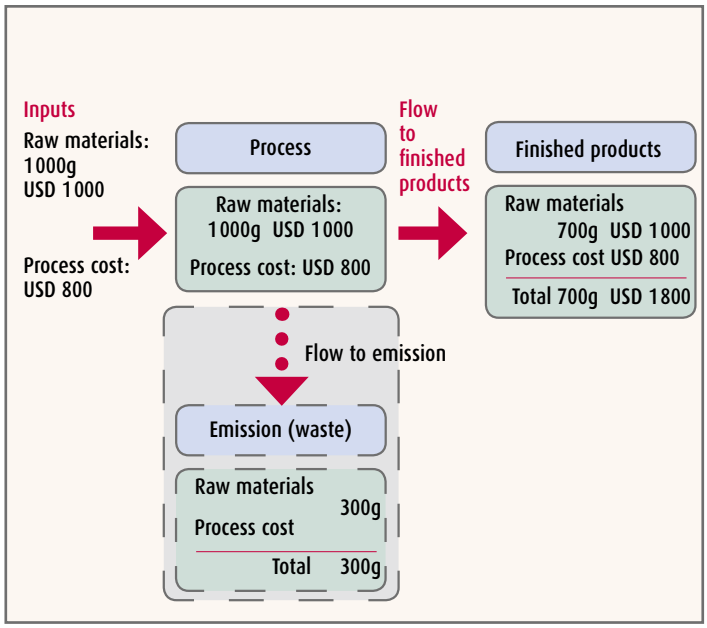


Figure 2 – *An example of conventional cost accounting.*

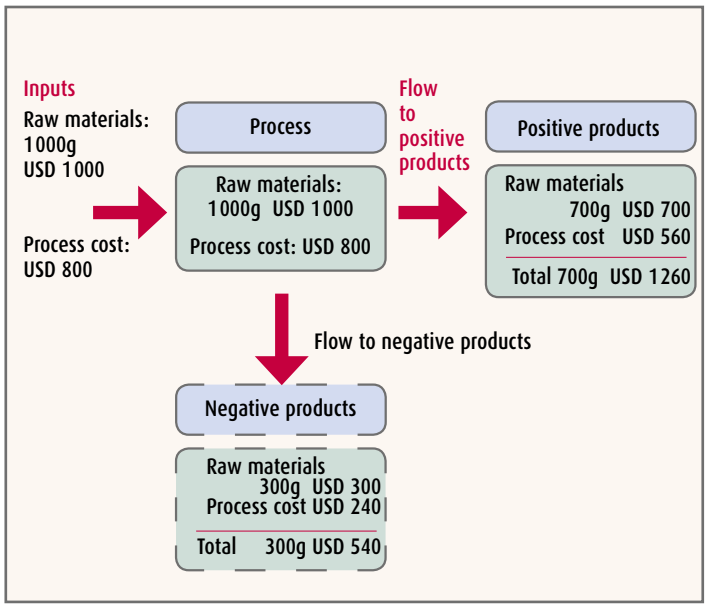


Figure 3 – *An example of material flow cost accounting.*

MFCA calculations differ from conventional cost accounting, as illustrated in **Figures 2** and **3**. In the examples, each production process yields a single product from 1000 g of material at a cost of USD 1000, plus the processing cost at USD 800. The costs are calculated using conventional cost accounting in **Figure 2** and MFCA in **Figure 3**.

Even if waste is visible in the factory, the cost of that waste is usually ignored in conventional cost accounting, as shown. This amount is automatically included in the cost of output (finished products).

However, in MFCA, waste is considered to be another product (negative product), and hence has cost allocated to it based on certain criteria, which in example **Figure 3** is weight. Therefore, the cost of the waste, as a negative product of 300 g, is calculated as USD 540. This is a new information generated by MFCA that provides an incentive to management to reduce that cost, achievable by reducing waste.

MFCA in action

MFCA can provide internal and external benefits, enabling an organization to make a greater profit with less environmental impact. A typical internal benefit is the strengthening of an organization's competitiveness, since MFCA delivers both increased profits and material productivity.

A good example of how MFCA enabled a company to improve productivity is shown in a case study of Nitto Denko, a major Japanese manufacturer of chemical, electronic and healthcare products (see **Figure 4**). The company significantly increased the ratio of positive versus negative products during the period 2001 to 2004, using MFCA.

MFCA can also bring external environmental benefits by enabling organizations to manufacture the same amount of finished product with less input. As a result, they can reduce environmental impacts such as CO_2 emissions and consumption of natural resources, as exemplified in the case of the Sanden Corporation, a Japanese manufacturer and supplier of automotive, commercial cooling and heating products (see **Figure 5**).

	2001	2004	2009 (Target)
Positive products (ratio)	68%	78%	90%
Negative products (ratio)	32%	22%	10%
Total (ratio)	**100%**	**100%**	**100%**

Figure 4 – *Improvement in material productivity at Nitto Denko through MFCA.*

	Current amount	Target amount	Amount of reduction	Rate of reduction
Input Materials	119t	109t	10t	-8%
Emissions (waste) Negative products	41t	31t	10t	-24%
CO_2 emissions	1,234t- CO_2	1,151t- CO_2	83t- CO_2	-7%

Figure 5 – *Reduction in CO_2 emissions at Sanden Corporation through MFCA.*

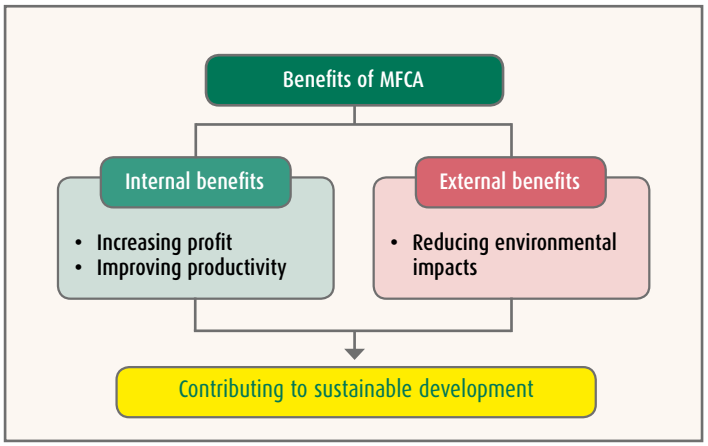


Figure 6 – *Benefits of MFCA.*

By applying MFCA to its manufacturing processes, Sanden found it could reduce the amount of input materials and CO_2 emissions, and thus contribute to sustainable development.

Balancing environmental and economic factors are vital issues confronting many organizations wishing to achieve sustainable development. MFCA can be of great assistance in this endeavour. It has become recognized as a valuable management tool because it links the environment to economics, as shown in **Figure 6** *(preceding page)*.

MFCA offers the potential for:

- increased production efficiency through capital investment, based on appropriate and accurate evaluation of investment projects;
- cost reduction through changes in product design and raw materials based on precise evaluation of manufacturing cost;
- revitalizing on-site improvement activities (e.g. environmental and quality management systems) by providing specific targets;
- possible extension to the supply chain and social cost management;
- applicability to any organization, regardless of type, size, activity and location, and in developing as well as developed countries.

MFCA implementation need not involve advanced computer-based information databases since simple spreadsheet calculations and the use of a calculator are often sufficient – an advantage for small and medium-sized enterprises.

Standardizing MFCA

ISO/TC 207/WG 8 is currently progressing from working draft to committee draft stage in the development of ISO 14051, *Environmental management – Material flow cost accounting – General framework*. The International Standard will comprise:

1. Scope
2. Normative reference
3. Terms and Definitions
4. Objectives of MFCA
5. Framework and Elements of MFCA
6. Approach for MFCA

Annex: Calculation Methods and Case Studies

While the objective of ISO 14051 is to standardize the general principles and framework of MFCA, it does not cover detailed procedures for accounting calculation but rather the steps required to introduce MFCA, and as such is expected to benefit a wide range of industries.

ISO 14051 can be considered as a standard for sustainable development. However, implementation of the cost accounting method is not within its scope at this stage, nor is it intended for the purpose of third-party certification.

Integration with ISO 14000

MFCA can be integrated into the ISO 14000 family of EMS standards and is complementary to life cycle assessment (LCA), environmental performance evaluation (EPE) and greenhouse gas management standards.

With regard to EMS integration, MFCA can provide significant information to an organization in the Plan-Do-Check-Act (PDCA) cycle. LCA generally regards the lifecycle of a product and service as a system, and analyses the environmental influence in the lifecycle but does not currently include economic aspects of an organization. MFCA supports this point.

- MFCA focuses on emissions (waste)
- Profit is hidden in emissions (waste)
- MFCA finds out the hidden profit

Figure 7 – *Spotlighting the benefits of MFCA.*

Concerning EPE – the PDCA continual improvement process – ISO 14031 in principle sets the outline necessary to monitor material flows within organizations, but does not relate this information to financial information systems and business decisions regarding costs and the setting of product prices. However, MFCA provides this link.

MFCA can provide significant information to an organization

In addition, the assessment of CO_2 emissions in many sectors is based on the evaluation of the material input of energy carriers, which need to be thoroughly registered in technical as well as monetary information systems. MFCA, again, provides this link.

ISO/TC 207/WG 8 proceedings

ISO/TC 207/WG 8 has already held workshops and meetings twice, first in Bogota, Colombia, in June 2008 and second in Tokyo, Japan, in November 2008. A Committee Draft is planned to be circulated in March 2009. Currently some 42 experts from 24 countries are participating in the development of the standard, with publication expected in 2011. •

The "Big D" becomes the "Green D"

Dallas is largely known across the globe for being big…big money, big business, and big hair (the hair styles made famous by the Dallas TV series)…and is appropriately nicknamed, "Big D". However, the "Big D" is now known as "Green D" as a result of a three-year ISO 14001 implementation and certification programme across all major city departments, a first in any US municipal organization.

by **Laura W. Fiffick**

Dallas skyline, Texas.

City Hall, Dallas, Texas.

With more than 1.2 million residents covering 384.7 square miles, Dallas is the ninth largest city in the US. The city is in the heart of the fourth largest metroplex in the US, and one of the fastest growing areas in the nation.

Municipal activities involve some 13 000 employees and a vast number of operations ranging from Love Field Airport and the Dallas Convention Center, to the McCommas Bluff Landfill and two wastewater treatment plants. In charge is a City Manager, with 14 council members serving two-year terms and a Mayor serving a four-year term.

EMS implementation

The City began its consideration of an environmental management system (EMS) as far back as 2002. Assistant City Manager, Jill Jordan, decided that Dallas needed an EMS to manage its many sustainability programmes ranging from the purchase of natural gas vehicles to the construction of green buildings.

The Office of Environmental Quality conducts an ISO 14001 audit at a City facility.

Each department **was given two years for EMS implementation**

After attending a conference for cities on EMS sponsored by the Texas Municipal League, Ms. Jordan created a position within the Environmental Health Services (EHS) Department to start working on the City's EMS. Initially, other priorities in the department and the City took precedent, and the EMS made little progress other than creating a few draft documents.

However, in December 2003, following negative media reports regarding its environmental practices, the City of Dallas received a notice of enforcement (NOE) for environmental compliance practices at its service centre facilities.

These facilities house a variety of operations relating to building, park, street, and vehicle maintenance. The NOE primarily focused on storm water and US Resource Conservation and Recovery Act (RCRA) concerns.

The City sprang into action and created the Office of Environmental Quality (OEQ) with 10 staff members reporting to the City Manager's Office. OEQ was staffed with environmental professionals with experience ranging from EMS implementation to air quality consulting and waste management.

While the NOE was being negotiated only for the service centre facilities, the City Manager's Office decided, with the assistance of OEQ, to implement an EMS based on ISO 14001 across all departments with operations affecting the environment.

It was also decided the system would be certified in order to ensure the EMS was implemented according to the standard and to have an unbiased third party auditor conduct the certification.

Educating school children about the importance of storm water protection at the annual Earthfest celebration in downtown Dallas.

The departments included were as follows: Streets, Park and Recreation, Equipment and Building Services, Aviation, Sanitation, Police, Fire, Convention and Event Services, Public Works and Transportation, Code Compliance, and Dallas Water Utilities. Three other facilities were included as a result of the NOE (Marshal's Office, Building Inspection, and the Radio Shop).

Each department was given two years – by April 2007 – to

complete implementation of the EMS. An environmental management representative (EMR) was assigned in each of these departments to implement the EMS. OEQ developed the schedule and deliverables, as well as provided the training and coaching necessary to implement the EMS. Frequent updates were given to the City Manager's Office and each department Director on the progress.

The EMS was divided into 10 elements for implementation: pre-planning, policy, aspects, legal, objectives and targets, training, documents, EMS auditing, corrective action, and management review. OEQ and the EMRs met each month for one hour and every six months for one day.

Each meeting included training as well as discussion and feedback on the EMS. Problems were discussed, and information was shared among all EMRs.

Certification

The City of Dallas' EMS was certified across 11 departments, plus three additional facilities, encompassing some 11 000 of the City's 13 000 employees and 450 facilities.

Stage I of the ISO 14001 certification audit was conducted in only one day; however Stage II lasted approximately seven weeks and included an average of three separate audit teams working simultaneously.

In one week, there were seven audit teams working across six different departments. Each audit team included at a minimum one auditor from the certification body, the department's EMR, and one member of OEQ. Some EMRs included one or more members of their EMS core team on the audit team.

A training discussion on environmental aspects and impacts during City operations.

Inspection of spill materials at a City fuelling facility.

Nonconformities received were first addressed by the individual department, and then reviewed by OEQ to determine if it was a system-wide issue. After all nonconformities were closed, the certification was received in June 2008.

The City of Dallas will have semi-annual follow-up surveillance audits for the first year following certification, and then will move to an annual surveillance audit schedule.

Resources

Initially, each departmental EMR was directed to dedicate 50 % of their time to implementation of the EMS. However, some larger departments, such as Dallas Water Utilities, ended up with a full time EMR as well as an additional assistant staff member.

Many of the departments divided EMR responsibilities among two or three staff members. Additionally, each department developed a cross-functional EMS core team.

These core teams met at least once a month for at least one hour over the three years of the EMS implementation and certification process. OEQ was originally staffed with 10 positions; however over the implementation of the EMS and associated successes, OEQ now has 22 members. Of these 22 staff members, four are dedicated full time to the EMS.

Introduction of the "Earth Day Everyday" EMS logo to City employees.

Benefits

The primary benefit achieved as a result of the EMS is environmental compliance across the City of Dallas. Departments now have the tools they need to assess and comply with environmental legal requirements.

Turning compost material at Dallas Zoo for use in exhibits.

These tools include regulatory notifications, ongoing training, environmental documentation systems, compliance auditing, and monitoring of corrective action. OEQ conducts over 100 compliance audits per year and reports the results to City Management.

As of the writing of this article, no notices of violation have been received by the City of Dallas (11 notices of violation were received by the City of Dallas in the first year of EMS implementation), and each facility with a compliance

audit averages two minor nonconformities per audit. These nonconformities identified are generally minor paperwork issues or are related to drum labelling.

This achievement is not only important for the financial and legal benefits, but if a City is going to ask its residents and businesses to exceed environmental requirements through water and waste programmes, then the City should be doing it as well.

Monitoring stormwater treatment devices at the Dallas Police Auto Impound.

The second benefit achieved has been improved environmental quality. These improvements have been achieved in the form of reduced water use (1 % reduction per year), energy conservation (5 % reduction per year), renewable energy purchase (40 % of total enegy purchase per year), and increased recycling rates in City departments.

Additionally, many new environmental initiatives are on the horizon. For example, the Streets Department is now recycling trash collected overnight from downtown Dallas streets, and the Fire Department is recycling used cooking oil from its fire stations.

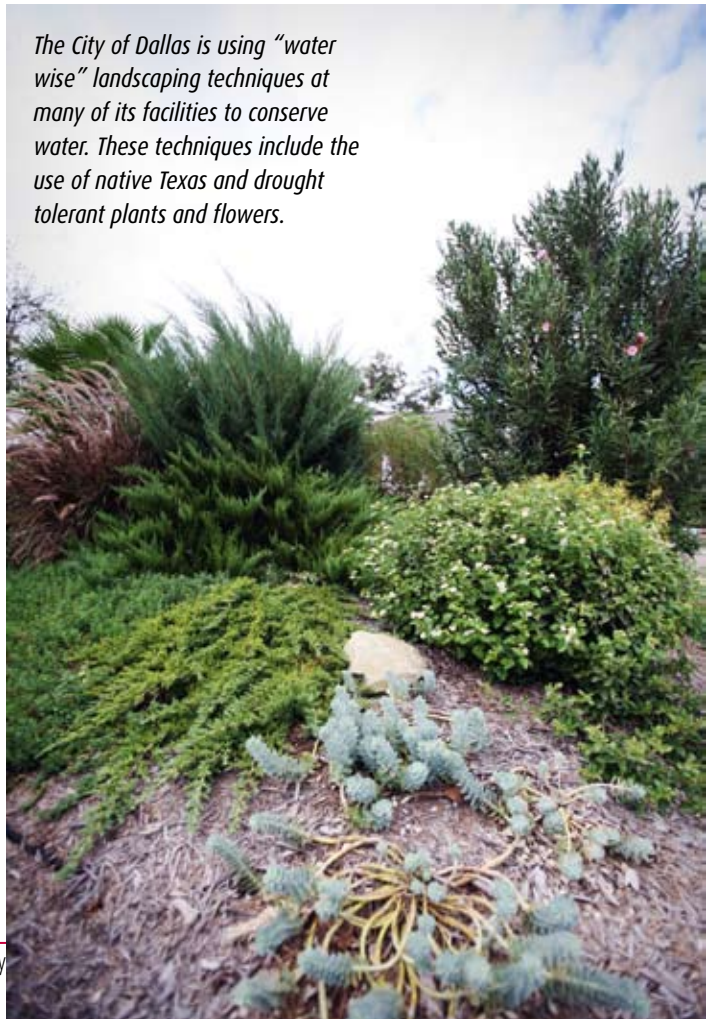
A third benefit is increased communication on environmental issues across the EMS Departments. Before implementing the EMS, even if departments had an environmental representative, there was no discussion or sharing of information between them. Now, each department has an EMR that meets regularly with other EMRs to discuss not only the EMS, but also ongoing environmental projects. This has not only led to enhanced efficiency and cost savings to the City, but also to improved environmental and safety practices.

For example, during one meeting on washing parts by maintenance staff, a mechanic from Equipment and Building Services discussed a new water-based parts washer that steams the parts clean. Not only did the water-based parts washer eliminate the use of hazardous chemicals, but it also allowed him to conduct other tasks while the parts were being cleaned.

Lessons learned

While the City received many unexpected environmental benefits of the EMS, there were also unexpected obstacles. One of these obstacles included staff turnover in both OEQ and with the EMRs. One department had five different EMRs before certification and has already had an additional change post-certification.

The departments with even one change in the EMR had difficulty keeping up with the pace of the EMS implementation due to the lack of understanding of environmental regulations and EMS terminology, as well as due to some desire to change the components of the EMS that were already in place.



The City of Dallas is using "water wise" landscaping techniques at many of its facilities to conserve water. These techniques include the use of native Texas and drought tolerant plants and flowers.

The City's green fleet includes a total of 2,006 alternative fuel vehicles –175 of those are hybrid (electric and gasoline).

The City of Dallas was certified across **11 departments**

Another lesson learned was varying levels of commitment across City facilities. While a Department Director may be very engaged in the overall implementation of the EMS, OEQ had some difficulty assessing if the entire department, including all facilities, were on track.

In a few cases, facility managers were not engaged in the EMS and had not implemented all components as scheduled. This would only be discovered during a conversation with the

facility manager or an EMS or compliance audit.

A third difficulty was the actual certification process with the third party registrar. Understanding the differences between operations of a municipality as compared to those of a typical industrial facility was a large hurdle for the registrar to overcome.

One benefit is **increased communication** on environmental issues

In addition, communication between the various audit teams working simultaneously was difficult. Municipal operations are not affected by environmental legal requirements in some instances in the same way as industrial facilities. This caused some confusion and disagreement during the registration audit.

Additionally, the nonconformities identified in the field by auditors were not consistently communicated during the various closing meetings either to OEQ or to the registrar's lead auditor.

Two specific areas of concern were the requirements in the ISO 14001 standard for evaluation of compliance and contractor requirements. While the City of Dallas had documented its interpretation of the ISO standard and associated requirements, not all of the auditors had reviewed this documentation, and many of the auditors had their own separate interpretation.

Future plans

With the success of the ISO 14001 programme at the City of Dallas, the City Manager and City Council have decided to also implement ISO 9001 (quality management) as well as OHSAS 18000 (health and safety management) across City departments. These programmes will be implemented in departments one-by-one, instead of across all departments at the same time.

To date, the Streets Department has received ISO 9001:2000 certification. Ultimately, the requirements of the three standards (quality, EMS and health and safety) will be integrated across City Departments. •

The author

Laura W. Fiffick is a Senior Environmental Scientist working with Gresham, Smith and Partners, a planning, engineering, architecture and interior design firm in Dallas, Texas. She was the Director of the Office of Enviornmental Quality at the City of Dallas when the City's environmental management system was implemented. Laura Fiffick would like to acknowledge the assistance of Frank Camp at the City of Dallas in preparing this article.

E-mail laura_fiffick@gspnet.com
Web http www.gspnet.com

The author would like to acknowledge the assistance in preparing this article of Frank Camp, Senior Environmental Coordinator, Office of Environmental Quality, City of Dallas.

E-mail
frank.camp@dallascityhall.com
Web www.dallascityhall.com

"Big Blue" refuse containers used in a single stream recycling programme implemented by the City of Dallas for the residential sector.

Isle of Man Ship Registry – anchored to ISO 9001

Certified to ISO 9001 since 1996, it was the arrival of ISO 9001:2000 that really turned the Isle of Man Ship Registry into a "fan", explaining: "ISO 9001 works because of its common sense approach and its eight core quality principals are clearly obvious steps for any business to pursue whether they are seeking certification or not."

by **Ray Ferguson**

***Ray Ferguson** is Quality Manager with the Isle of Man Ship Registry.*

E-mail ray.ferguson@gov.im
Website www.iomshipregistry.com

The Isle of Man ensign.

The Isle of Man, situated in the Irish Sea midway between England and Ireland, registered its first ships over two centuries ago and has been operating a modern International Ship Registry since 1984.

It boasts some of the worlds most highly respected shipping companies such as BP, Maersk and Shell amongst its clients. About 90% of the world's trade by volume is sea borne and shipping remains one of the most economical forms of transportation.

As part of the Manx (Isle of Man) Government attached to the Department of Trade and Industry, our business involves the registration of ships and yachts, the technical regulation and jurisdiction for those vessels on the register and the development of merchant shipping legislation.

With a dedicated team of only 32 employees, we service a current fleet of over 440 ships with a combined tonnage of around 9.4 million gross tons. In addition, we have an order book with a further 72 ships and 57 yachts (including "super yachts") under construction that are due for delivery under the Isle of Man flag in the next 2-3 years.

ISO 9004:2000 offers many helpful ways to **grow beyond customer expectations**

Our surveyors carry out vessel surveys and audits for compliance with national and international maritime codes visiting ships at ports around the world, fitting in as much as possible with the vessels' schedules to ensure minimum disruption to any portside activities and operations that may be taking place.

Shipping company offices are also visited and their internal management systems audited on a regular basis to ensure compliance with the international safety management (ISM) systems code.

The Registry team provides a "user friendly" and speedy process throughout the registration procedure and are available 24/7 enabling clients to register their vessels at any time from anywhere in the world.

In a highly competitive global marketplace, customer focus and quality of service is paramount – particularly when the only "product" that we offer is ourselves.

Registry surveyors carry out vessel surveys and audits for compliance with national and international maritime codes.

Inspections are carried out to fit in with vessels' schedules to ensure minimum disruption to any portside activities.

Mandatory

In the late 80s and early 90s, international shipping suffered a number of maritime disasters that cost many lives and investigations revealed major errors on the part of ship management. The International Maritime Organization (IMO) developed and made mandatory for certain ship sizes the International Safety Management Code which contained many of the elements of ISO 9001:1994.

As a government department with the responsibility to approve and audit ships and companies for compliance with the ISM Code, it was decided that we needed to invest in our own quality management system.

So although we had been an ISO 9001:1994 registered organization since 1996, certified through Lloyd's Register Quality Assurance (LRQA), it was the introduction of the generic ISO 9001:2000 standard that provided the emphasis on the two key features of customer satisfaction and customer focus which, together with the change of approach from individual elements to a "process-based" approach, opened up the opportunity to develop a quality management system that could be fully integrated into our normal business operations.

The lament about the perceived bias of the old ISO 9001:1994 standard towards the manufacturing industry and engineered product quality can still be heard in some service industry sectors today and I believe this impression was a leading reason for the relatively slow uptake of the 2000 standard within many public sector and service organizations.

The eight quality principals are obvious steps for any business to pursue

The Ship Registry's clients include 57 yachts – including "super yachts" like the one pictured here – under construction that are due for delivery under the Isle of Man flag in the next 2-3 years.

Fortunately, recent surveys indicate a positive swing with an increasing number of public and service organizations adopting quality standards and tools.

It was recognised quite early by the Ship Registry that, with the 2000 standard, we could create a management system specific to our business objectives and in line with our existing scope of certification which states:

The provision of a shipping register and marine administration including the registry, survey and inspection of ships, issue of seafarer's certification and developing merchant shipping legislation.

Working with LRQA, the transition took about 24 months during which time our quality manual was completely revised, internal auditors retrained and staff made aware of the change of focus. After several discussions our policy – or mission – statement was agreed as the following:

It is the policy of the Isle of Man Ship Registry to provide a high quality service dedicated to the principles of quality assurance, in order to promote both the expansion and diversification of the shipping sector and the creation of employment opportunities by registering quality ships and facilitating the establishment of marine enterprises in the island.

It as also agreed that we would achieve this via three steps:

1. maintain and develop a first-class ship registry;
2. continuously seek improvements in our performance;
3. encourage new shipping business.

We received our final assessment and certification in late 2003 coinciding with our "new" management system having just been used to help develop the procedures and processes required to meet forthcoming International Ship and Port Security Code requirements.

Greater focus

The benefits of having a greater focus, clear objectives and improved communication have kept the Isle of Man Ship Registry highly placed on the Paris and Tokyo Memorandum of Understanding on "White Lists" for port state control. This is the industry performance standard, and has contributed to us being placed No. 1 on the Flag State Performance table issued by a round table of shipping associations.

Many of the companies we visit are also certified to ISO

9001:2000 so a common bond exists that helps towards a good working relationship. Our ISO 9001:2000 certification, which we actively promote, sends out the signal that we are serious about quality and that is an important message to the shipping world. The competitive advantage of being one of only a few registries holding ISO 9001:2000 certification is a major consideration in our marketing.

By far the greatest impact of our ISO 9001:2001 involvement has been in our combined approach to customer needs, analysis of data and the impetus of continual improvement. The ISO 9004:2000 guidelines for performance improvements is a useful guide that is often overlooked, but which actually offers many helpful ways to grow beyond customer expectations.

A successful system **cannot remain static**

Although we had been collecting a vast amount of data it was not really being analysed into any useful information. So two years ago, we created several key performance indicators so vital areas of interest could be monitored on a monthly basis giving an early warning to the management team if anything was slipping to plan and providing the opportunity for preventive measures to be taken if required. This data now also provides a year-by-year record making future planning much less of a guessing game.

The Ship Registry currently services a fleet of over 440 ships, such as these tankers.

All our customer-facing staff have attended "voice of the customer" (VOC) training courses to improve the interactions between clients and the Ship Registry. Subsequently, we now have a far better understanding of what is important to our customers and are able to use quality function deployment tools to decide best options. Staff commitment and support comes from ensuring that everyone is kept informed and involved.

Para 8.5.1. *Continual Improvement,* in our quality manual states:

The reason for having ISO 9001:2000 is to give us a structured approach to doing what we do. It also introduces a need for continually improving our business, which is what we are here for. Improvements don't have to be sweeping changes, major re-structuring or new systems. Even a small change to our internal processes that makes life easier and improves our ability to do a job better is to be encouraged.

This open approach to encourage and involve everyone generates a constant stream of improvement opportunities. The combination of customer focus and willingness to embrace change by the whole team, backed up by a system that sets achievable objectives and monitors internal and external performances is what really works and helps set us apart from our competitors.

ISO 9001:2000 works because of its common sense approach and its eight core quality principals are clearly obvious steps for any business to pursue whether they are seeking certification or not.

The standard provides the platform and basic structure on which to build a management system which is unique to your business needs. Bear in mind though that, almost by definition, a successful system is one that cannot remain static, but rather is one that continually evolves to the changes that are generated from within its very own processes. If your management system isn't generating improvement opportunities – it's not working! •

ISO 22000 helps India's Akshaya Patra Foundation feed a million needy children daily

India's celebrated Akshaya Patra Foundation feeds wholesome school meals to over 966 000 children daily through an ambitious ISO 22000: 2005-certified programme, and, in so doing, encourages the young and needy to attend school rather than risk becoming child labourers.

by **Aparna Achar**
and **Chanchalapathi Dasa**

Aparna Achar *is Associate Editor of* Log India*, a specialized trade journal on business logistics and outsourcing, and contributes to Indian and international economics, business, and communications publications and to Indian national newspapers. She also reports on the activities of the Akshaya Patra Foundation.*

E-mail acharaparna@gmail.com

Chanchalapathi Dasa *is Vice Chairman of the Akshaya Patra Foundation, and has spear-headed the implementation of its major food programme across India since inception in 2000.*

Web www.akshayapatrausa.org

Harshia Banu is a seventh grade student from the government-run Urdu Higher Primary School in Bangalore, India. When she says, "I often fainted from hunger, but now, with the food I get in school, I feel I have a new life", one realizes the importance of access to good quality food.

Cut vegetables are stored overnight in one of Akshaya Patra's ISO 22000:2005-certified cold storage rooms.

Education thrives on a full stomach: many Indian children are encouraged to go to school by the promise of a square meal each day, thanks to the Akshaya Patra food programme.

Akshaya Patra cooks prepare rice in bulk as a staple for meals served daily to nearly one million needy children in 5 700 schools in India.

Indian children enjoy the benefits of healthy, nutritious school meals served free from the kitchens of the Akshaya Patra Foundation.

"We are what we eat"

Our physical and mental health are greatly influenced by the food we eat. Obviously, that food should be free of contaminants, toxins and any substances that could cause chronic health problems. But how many of us can claim that our food is absolutely safe, unadulterated and nutritious?

Akshaya Patra's ISO 22000 certification is believed to be the first achieved by an NGO

Food-borne diseases pose a serious challenge to life and economy in many developing countries. The World Health Organization estimates that almost 70 % of the approximate 1.5 billion annual cases of diarrhea in the world are directly caused by biological or chemical contamination of foods.

A United Nations study estimated that world population would reach 7.6 billion by 2020, with nearly 98 % of the projected growth taking place in developing countries. But rapid urbanization and lack of resources to deal with food and environmental issues in these countries can lead to food safety risks.

Food safety standards

One way of minimizing health hazards is to adhere strictly to international food safety standards, as exemplified by the Akshaya Patra Foundation in India. The organization, which feeds wholesome school meals to over 966 000 children daily, recently achieved certification to ISO 22000:2005, *Food safety management systems – Requirements for any organization in the food chain.*

Certification to the international food safety management system (FSMS) standard was achieved by Akshaya Patra's automated kitchen facilities in Ahmedabad, North and South Bangalore, Hubli-Dharwad, Jaipur and Vrindavan. It is believed to be

the first FSMS certification ever a food programme managed by a non-governmental organization (NGO).

For thousands of deprived children like Harshia Banu, ISO 22000:2005 implementation means consistently safe, nutritious food that nourishes their physical and mental growth day after day. The meals that Akshaya Patra serves these children is often their only source of sustenance. Now they are delivered with the added FSMS-certified assurance of safety and high quality, certified by international certification body, Det Norske Veritas AS.

A customized van is loaded with stainless steel food containers ready for distribution to local schools, as part of the Akshaya Patra Foundation's daily school meal delivery to six regions across India.

About Akshaya Patra

The Akshaya Patra Foundation was set up in 2000 as a strategic food programme with two key objectives: to offer unlimited, wholesome and free school lunches to underprivileged children and by doing so, motivate them to attend school so that they do not end up as child labourers. Its stated vision is that *no child in India shall be deprived of education because of hunger*.

Since then Akshaya Patra – Sanskrit for "abundant and inexhaustible" – has become one of the most effective food programmes in India, facilitating formal education for nearly one million needy children daily. Abundant, region-specific fresh food is delivered to 5 700 schools, 220 days per year, from 16 kitchens located in Andhra and Uttar Pradesh, Gujarat, Karnataka, Orissa and Rajasthan.

The Foundation is a not-for-profit NGO, equitable and secular in its approach. It is run as an independent, registered charitable trust with headquarters in Bangalore, branch offices across the country, and international offices in the United Kingdom and the United States.

Sustainability is achieved through subsidies from the central and state governments of India, corporate and philanthropic institutional support, and individual donations.

Workers involved in food preparation at Akskaya Patra Foundation kitchens observe strict hygiene procedures in meeting the food safety management requirements of ISO 22000:2005.

Food is provided only to government-run schools that already have a secular student admission policy so that the benefits of the programme are offered to all children regardless of sect or religion. Food is supplemented with oral micronutrients and coupled with educational incentives to boost child development holistically.

The innovative project infrastructure is technology-driven, process-oriented and easily scaled up. For example, a three-item localized menu for 100 000 children can be cooked in less than five hours in one of the automated kitchens. Efficient logistics then guarantee timely distribution of food to schools.

Modern technology is just one example of the many ways in which the Akshaya Patra Foundation has endeavoured to adopt the best practices of the corporate world. To ensure transparency and accountability, it has engaged audit, tax and advisory services provider KPMG to audit the programme for funds utilization.

Chappatti dough for Indian bread is cut, roasted and collected in containers in Akshaya Patra's Jaipur kitchen, one of 16 ISO 22000:2005-certified kitchens in the Foundation's extensive school food programme.

Sambar lentil and vegetable soup is cooked in stainless steel cauldrons on level two of Akshaya Patra's gravity flow kitchen in Hubli, Karnataka, India.

Tributes

Akshaya Patra has received many awards in India, and the Harvard Business School wrote a case study on the Foundation's use of precise time management, now incorporated into its management courses.

US President-elect Barack Obama, in a recent letter to the Foundation, said:

"I want to congratulate you and the people of Akshaya Patra Foundation for the incredible progress you've made in feeding the children of India. Your use of efficient and innovative business practices to scale up in just a few years from feeding 1 500 school children daily to almost a million is a powerful demonstration of what's possible when people work together."

About ISO 22000:2005

ISO 22000:2005 is an International Standard that specifies requirements for a food safety management system where an organization in the food chain needs to demonstrate its ability to control food safety hazards in order to ensure that food is safe at the time of human consumption.

Since it emphasizes the process and not just the end-point safety measures, the FSMS standard requires sustained quality throughout the chain – from procurement of raw materials until the food is served to children.

By conforming to ISO 22000:2005, the Akshaya Patra Foundation has underlined its commitment to the highest quality in food safety, management and delivery.

FSMS benefits

It is said that the poor will consume almost anything to ease their hunger. Survival may depend on a minimum quantity of food regardless of quality. However, consumption of food which does not meet minimum safety standards can also jeopardize survival.

Akshaya Patra is aware that food served to underprivileged children should be safe and of

good quality, which is why, from its inception, the Foundation has implemented mechanized cooking and delivery processes with the least possible human intervention.

ISO 22000:2005 certification reinforces our programme objectives, one of which is to treat the target audience with dignity and compassion. Implementation of the FSMS standard has also brought numerous benefits, including:

- *Renewed commitment*

Certification has renewed our commitment to quality and safety for deprived children.

- *Reassuring stakeholders*

Stakeholders are reassured that Akshaya Patra is a serious, sustained and quality-conscious movement facilitating the education of needy children for better health, employability and living.

- *Best practice*

The food programme now incorporates global best practices through ISO 22000:2005 implemention and conformity.

- *Enhanced image*

FSMS certification of an NGO-managed food programme enhances India's image and reputation internationally.

- *Motivating others*

Since the Akshaya Patra programme is easy to replicate, certification will encourage similar food project organizations to do likewise and pass on the benefits to users.

Vats of yogurt, an important accompaniment to the nutritious school meals prepared by the Akshaya Patra Foundation, await delivery.

- *Global precedent*

We have established a global precedent as the first NGO-run food programme to achieve ISO 22000:2005 certification.

- *Raising standards*

FSMS implementation has raised quality at all levels. This in turn has motivated staff, donors, suppliers and all stakeholders to offer the best possible service.

- *Reducing cost*

ISO 22000:2005 implementation has not only led to improved food quality and safety, but also to reductions in cost of production and in waste.

- *Extending resources*

The resources thus saved can be focused on bringing more underprivileged children into the programme.

For the future, we plan further extensions to the programme which are expected to bring long-term economic and social benefits to India in reduced child malnutrition, better health, less disease and greater productivity. •

Case studies show value of ISO/IEC 27001 conformity

These testimonials show how three diverse organizations have benefited from implementation and certification of ISO/IEC 27001 information security management systems – a gas processing group in Abu Dhabi, a Norwegian state-owned gaming organization, and India's largest public sector energy infrastructure company.

by **Edward Humphreys**

Visiting Professor ***Edward Humphreys*** *(FH University of Applied Science, Hagenberg, Upper Austria), is Convenor of ISO/IEC JTC 1,* Information technology, *subcommittee SC 27,* IT security techniques, *working group WG 1,* Information security management systems.

E-mail edwardj7@msn.com

Organizations today are required to conform or comply with many different laws and regulations, industry norms and practices, internal auditing standards and matters of corporate governance.

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*, has become the benchmark for most information security management system standards (ISMS) and the International Standard for achieving compliance with such requirements. This is because the standard is flexible enough to meet the needs of small, medium-sized and large organizations with applicability to all business sectors, governments, academic and charitable institutions (see **Figure 1**, *overleaf*).

The International Standard is ideally suited to meet the needs of information security governance — a key aspect of corporate governance that protects an organization's

information assets (see **Figure 2**).

The following are three of many case studies of organizations that have certified to ISO/IEC 27001. (See also article *"Some 4 500 organizations implement ISO/IEC 27001 for information security"*, *ISO Management Systems*, July-August 2008).

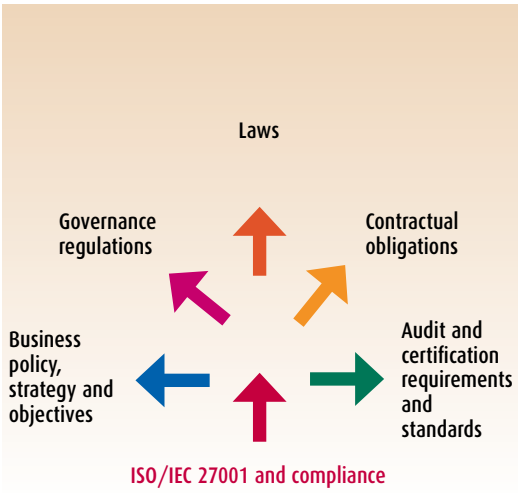


Figure 1 – *ISO/IEC 27001: a flexible benchmark for information management.*

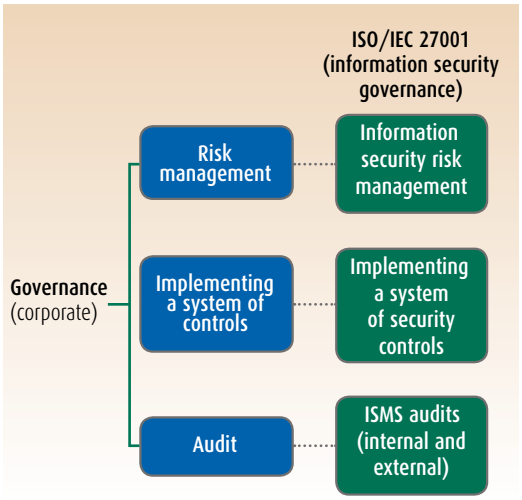


Figure 2 – *ISO/IEC 27001: ideally suited to meet information security governance needs.*

1

GASCO – Abu Dhabi Gas Industries Ltd.

ISO/IEC 27001 : "The ideal way forward"

by ***Adel Salem Alkaff***

Adel Salem Alkaff *is IT Division Manager, GASCO*

During the summer of 2008, the IT Division of Abu Dhabi Gas Industries Ltd (GASCO) became the first oil and gas company division in United Arab Emirates to be certified in accordance with ISO/IEC 27001.

The certification was achieved with senior management support, under the leadership of General Manager Mr. Mohammed Sahoo Al Suwaidi, covering implementation of state-of-the-art information security tools.

At GASCO, we search for best practices to maintain market leadership, as part of our policy of continual improvement. The increasing need for information exchange and IT, particularly in a climate of threats and vulnerabilities in the sector, underlined the importance of information security management. Since ISO/IEC 27001 is the only globally recognized ISMS standard, and as GASCO is implementing a range of management system standards, certification was the ideal way forward.

External attacks

Over time, we noticed external attacks on the network, internal user errors and a lack of awareness of information security among employees. The company responded by building a qualified information

GASCO headquarters in Abu Dhabi.

Web www.gasco.ae

About GASCO

Abu Dhabi Gas Industries Ltd (GASCO) processes natural and associated gas from onshore oil operations in the Emirate of Abu Dhabi. The company was incorporated in 1978 as a joint venture between Abu Dhabi National Oil Company (ADNOC) (68 % shareholding), Shell and Total (15 % each) and Partex (2 %).

GASCO was established following the directive of His Highness the late Sheikh Zayed bin Sultan Al Nahyan, President of the United Arab Emirates and Ruler of Abu Dhabi, to utilise Abu Dhabi's significant gas resources which are converted into a wide range of domestic products exported worldwide.

security team to implement incident management, user awareness campaigns, and support best practice standards, such as ISO/IEC 27001 and the Information Technology Infrastructure Library (ITIL).

Even though implementing and maintaining an ISMS requires considerable dedication, the system has full management support at GASCO, and we plan further extensions to the scope of the certification.

Enhanced awareness

Implementing ISO/IEC 27001 has led to enhanced information security awareness among employees, improved security operation efficiency, and has helped increase understanding of the need for continual improvement.

ISO/IEC 27001 is the only globally recognized ISMS standard

Our company is now seen as the leader in information security within the Abu Dhabi National Oil Company Group (ADNOC). In addition, going through the certification process helped us establish useful international contacts with our certification body Lloyd's Register Quality Assurance Ltd. (LRQA), and with leading ISMS consultancies around the world.

2

Norsk Tipping AS

"Don't gamble with information security"

by Hilde Grunt

Hilde Grunt is Security Advisor, Norsk Tipping

State-owned Norsk Tipping, Norway's leading gaming company and member of the World Lottery Association (WLA), was certified according to ISO/IEC 27001 in 2008, some 11 years after gaining certification to the Intertoto Security Control Standard (a WLA predecessor).

The objective of that earlier certification was to enable members to achieve a common security standard, and provide an approved security framework for those who wished to participate in international lotteries. WLA certification is now a prerequisite for participating in the Viking Lotto, a pan-Nordic numbers game. In 1997, Norsk Tipping became the first organization to be certified according to this standard.

Since 1995, the WLA Security Control Standard has been continuously revised by the WLA Security and Risk Management Committee. However, ISO/IEC 27001 has now been added to the the general information security controls of the WLA standard.

ISO/IEC 27001-certified Norsk Tipping is Norway's leading gaming company and member of the World Lottery Association.

The lottery specific controls relating to lottery draws, instant tickets, handling of prize money, etc., remained unchanged from the old WLA standard. Now, to gain WLA certification, the lottery or gaming company has to conform to both ISO/IEC 27001 and the lottery specific requirements.

Major change

Inclusion of ISO/IEC 27001 was a major change. The previous WLA-standard was an industry standard, and the WLA Security and Risk Man-

agement Committee identified the controls needed to deal with lottery risks. Any lottery or gaming company seeking certification had to comply with all the controls in the standard. Compared to ISO/IEC 27001, the industry's former ISMS requirements were much more simplistic. Preparation for certification demanded a new approach and a thorough revision of Norsk Tipping's ISMS.

Axel Krogvig, President and CEO of Norsk Tipping, says that ISO/IEC 27001 certification represents a good quality assurance when the objective is to implement a management system to ensure that the company's information security risk is maintained at a defined and acceptable level.

Annual safeguard

ISO/IEC 27001 certification is an indicator that we are on the right track, and the annual audit is a safeguard to keep us focused throughout the year. Mr. Krogvig emphasizes the importance of maintaining certification as the means of achieving the company's objectives, and not that certification becomes an objective in itself.

"There is always a danger that implementing a standard will cause unnecessary bureaucracy and not bring substantial benefit to the organization. More than giving value, the standard can lead a life of its own, justifying any measures needed to keep the certificate hanging on the wall. One must remain focused on the objectives and implement an ISMS that helps the processes to run smoothly and efficiently," says Mr. Krogvig.

Headquarters of ISO/IEC 27001-certified Norsk Tipping in Hamar, Norway.

Web www.norsk-tipping.no

Benefits

According to Senior Vice President ICT, Trond Karlsen, ISO/IEC 27001 certification has given Norsk Tipping a common information security language, and this has created a new security awareness throughout the organization.

Different departments, such as ITC, sales and security, now have a common understanding of risk management and refer to the same framework of controls. However, the standard can be a challenge to implement since it is necessary to coordinate ISO/IEC 27001 requirements with numerous other management system requirements confronting the company.

Among other benefits, Mr. Karlsen says the standard provides a structured approached to ISMS development and associated controls and documentation. The fact that it is an open standard also allows comparison with other certified companies, regardless of type of business.

Middle management cite "periodic audits performed by an accredited body" as a principal benefit of ISO/IEC 27001 certification. The discipline of a third party check on whether we do as we say reminds us not to postpone or forget tasks critical to the core business processes amid the distractions of the daily routine.

ISO/IEC 27001 certification represents a good quality assurance

Another significant benefit mentioned by middle managers is the ISO/IEC 27001 requirement for management to ensure that security is incorporated in the general management processes.

In summary, we believe the key benefit of ISO/IEC 27001 certification is the implementation of an ISMS that prevents information security existing solely in the ITC and security departments, by utilizing external reviews as company-wide quality assurance.

About Norsk Tipping

Norsk Tipping, Norway's leading gaming company, is wholly owned by the Norwegian State. Profits are divided equally between the nation's sports and culture sectors. Norsk Tipping is a member of the World Lottery Association (WLA), a global professional association of state lottery and gaming organizations from 76 countries and five continents aimed at advancing the interests of state-authorized lotteries.

Hilde Grunt is responsible for ISMS audits, security awareness and training. She is also Privacy Ombudsman in accordance with the Personal Data Act. She has been active in the revisions and development of the WLA Security Control Standards.

Web www.norsk-tipping.no

Without doubt, ISO/IEC 27001 implementation has enabled us to integrate information security management into managing Norsk Tipping in a way that ensures our business objectives can be met at a defined and agreed level of information security risk.

3

Bharat Heavy Electricals Limited

"A role model for information security management in India"

*by **Arvind Kumar***

*Author **Arvind Kumar** is Director, Standardization, Testing and Quality Certification Directorate, Department of Information Technology, Government of India.*

E-mail arvind@mit.gov.in

Bharat Heavy Electricals Limited (BHEL), India's largest energy infrastructure engineering and manufacturing enterprise, is the first Indian public sector organization to have achieved the distinction of ISO/IEC 27001 certification.

The organization was audited and certified by the Standardization, Testing and Quality Certification (STQC) Directorate, part of the Department of Information Technology of the Ministry of Communication and Information Technology at the Government of India.

STQC has received international recognition of its ISMS certification scheme following accreditation by the Dutch Council for Accreditation (Raad voor Accreditatie – RvA), and is the first Indian accredited certification body in the country, and outside the United Kingdom and Netherlands, to have done so.

BHEL generates, transmits and maintains a huge amount of design, engineering and manufacturing data both in electronic form and on paper. With the entrenchment of IT in core business processes, more and more of that data is now stored on electronic media during the entire information lifecycle.

Since this information is the lifeline of BHEL's entire business operations, its availability, confidentiality and integrity are critical for the survival of the company.

Threats and vulnerabilities

Extranet connectivity provides communication outside the organization and vice-versa, enabling BHEL to talk with suppliers, partners, vendors and customers, and importantly, connecting back into legacy systems where critical corporate information lies.

Information security had always been important, but it was not given a particularly high priority because there had been no serious security incidents. However, threats and vulnerabilities have increased with extranet connectivity.

Headquarters of ISO/IEC 27001-certified Bharat Heavy Electricals Limited in New Delhi, India.

Web www.bhel.com

About BHEL

M/S Bharat Heavy Electricals Limited (BHEL) is the largest engineering and manufacturing enterprise in India in the energy-related/infrastructure sector with a network of 14 manufacturing divisions, four power sector regional centres, over 100 project sites, eight service centres and 18 regional.

The company manufactures over 180 products under 30 major product groups and caters to the core power generation and transmission, industry, transportation, telecommunication and renewable energy sectors of the Indian economy.

BHEL top management became aware of the need to enhance information security, and the challenge of implementing an ISMS was assigned to its IT fraternity. Corporate information technology was the driver for corporation-wide implementation.

The information technology network at BHEL consists of strong IT groups at all major locations. These groups oversee the local IT infrastructure and work to meet all the IT needs of their parent units. The corporate group looks after corporate office IT requirements and also provides direction to the company's entire IT infrastructure.

Internal capability building

Since BHEL aspired to a fairly high level of maturity for information security, the company considered the merits of employing the services of an external partner to guide it through the initial phase of ISMS implementation.

BHEL selected the IT services of STQC, since we were well known for providing professional training and services in information security. STQC was required to train BHEL personnel in the different aspects of information security — network and system security, and ISMS — and also to help in building up the capability needed to implement an ISMS.

The management decided that, although those external services were required at the outset, the company should build its own internal capabilities for the entire ISMS implementation process. They felt that internal resources should be developed because information security implementation is not a once-only event, but a continuous process. Requirements change along with changes in technology and business needs. This internal capability building proved to be a major boost to its ISMS implementation.

Starting point

BHEL's operations extend over the entire country, with function and practice differing from one location to another. As such, it was clear that BHEL could not apply for corporate certification, and that the whole company could not be covered as a single entity.

Since most of the information is generated by the manufacturing units and power sector regions, it was in those areas that we decided to implement the ISMS first. Fourteen major locations were identified and divided into two phases of seven each. The best practices of each unit were identified, and an information security policy was formulated and issued at corporate level.

Successful implementation

From STQC guidance and internal meetings, the following requirements for successful ISMS implementation were developed:

- *Gaining top management involvement at the units by setting up a structured network of committees and sub-committees.* This was necessary to achieve full awareness of requirements and resources. Clearly, no organization-wide initiative can succeed without the involvement of senior managers.
- *Developing employee awareness of their role in information security through education*. "Ease-of-use" versus "security" is an ongoing security issue for many organizations. It is a balancing act between what the user community wants, and the security policy. Security is only as strong as the weakest link, and the full involvement of employees in the process is essential.

With that aim, specialized training of key personnel was provided at all locations identified for ISMS implementation covering network and system security, security processes and management, and security audits.

Security forum

BHEL decided to organize a Corporate Information System Security Forum with its Corporate Information System Security Officer (CISSO) as chairman. An Information System Security Officer (ISSO) was identified for each location. All ISSOs are members of the Corporate Information Security Forum. The CISSO's role is to maintain and review information security policy and provide guidance for its implementation.

While the company needed common documentation, differences in local practice were accommodated in customized versions to meet local needs. Hence, BHEL decided to have five levels of documentation. The top level document, setting out the ISMS policy, was finalized jointly with unit IT heads, approved by the Chairman and Managing Director and issued as the corporate information system security policy. This was applicable to the entire organization without modification.

The other four levels – ISMS Manual, ISMS Policies and Guidelines, ISMS Procedures and ISMS Formats – could be customized by the locations concerned. All reviews and modifications to the ISMS documentation became the responsibility of the unit level security forums.

Role model

As a result of these planning and implementation processes, BHEL became the first Indian public sector company to implement and certify an ISMS in conformity to ISO/IEC 27001, covering 13 units and the corporate IT department.

Information security is now a part of every key business process. Management confidence in, and expectations of, the IT groups has increased many times. This has not only improved the risk management and contingency planning associated with information resources, but has also enhanced customer and stakeholder confidence.

From our point of view as the certification body it was a challenge to certify one of the premium public sector organizations in the country, with such a diverse range of products catering to the core sectors of the Indian economy.

Since ISO/IEC 27001 certification there has been a substantial improvement in the security management approach at BHEL. The company has become a role model for other public sector organizations in India under the national e-governance initiative to protect the critical infrastructure of the country. •

European initiatives for sheltered housing and airport security

New European service standards will define comprehensive requirements for sheltered housing and airport and aviation security services. The kick-off meetings for these projects took place in October and November 2008 in Vienna, Austria.

by **Holger Mühlbauer**

***Dr. Holger Mühlbauer** has specialized in service standardization since 1996 and is involved in a number of ISO and CEN projects related to services. He is Secretary or project editor of several service related ISO committees. He is now in charge of service standardization at ON Austrian Standards Institute. Dr. Mühlbauer's professional background is in law.*

E-mail holger.muehlbauer@on-norm.at
Web www.on-norm.at

Sheltered housing for elderly

This future standard will specify requirements for providers of services of sheltered housing for the elderly and, according to its initiators, will be applicable irrespective of the legal form of ownership and management of the property and public or private financing of the services. The scope of the project covers one segment of a wider area of services for the elderly.

"Sheltered housing" for the elderly has seen an enormous increase in European countries such as Austria, Germany and the United Kingdom in the 1990s and has become an important new form of living for elderly people. There are other terms such as "service living" or "attended living". The future standard will most likely stick to the term "sheltered housing".

Today's market offers a wide variety of different choices. Sheltered housing is not a term that is clearly defined by law. However, in many European countries, there is no special legislation defining the standards that providers of a sheltered housing facility have to meet, and there is no special institution that ensures the fulfilment of quality standards applicable to sheltered housing for the elderly. This situation has led to the development of different regional methods of voluntary quality assurance in the past.

The future standard intends to provide an instrument for voluntary quality assurance in the sheltered housing market. The future standard defines minimum quality and will serve as an orientation for the providers with regard to the services they should make available if they want to offer sheltered housing.

At the same time the standard intends to make the services offered for this type of living more transparent for the consumers. The future standard will not deal with product-related requirements.

Airport and aviation security services

This standard will lay down requirements for quality in organization, processes, personnel and management of a security service provider and/or its independent branches and establishments under commercial law and trade as a provider with regard to airport, aircraft, airline and airport-related civil aviation security services.

It will deal with quality criteria for the delivery of civil aviation security services related to airports, aircraft and airlines, requested by public and private clients or buyers. The standard will be suitable for the selection, attribution, awarding and reviewing of the most suitable provider of airport, aircraft, airline and airport-related civil aviation security services.

The stakeholders backing the proposal felt it would be necessary to develop a European standard for private security services for airports, airlines and aircrafts, because civil aviation is most of all about people and must therefore comply with the highest possible rules and standards.

Today, there are no industry-driven standards related to the imperative quality that must be provided by private security companies delivering services to the civil aviation industry. Indeed, it is necessary for the private security providers – who play an essential role in overall security related to airports, airlines and aircraft – to apply common quality standards.

Given the nature of private security services and its increasing role in security policies in general, the introduction of standards related to quality is important to increase the professionalism of the services offered and to increase the much needed guarantees for buyers and clients.

Quality

The initiators were also of the opinion that common standards related to quality for the described private security services will avoid "companies not willing to go for the highest quality criteria" being selected on the basis of price solely, rather than on a efficient and effective combination of price in relation to quality.

The existing competition within the private security sector pursuing contracts encourages some companies to cut their prices to the detriment of the quality of their services, despite the fact that quality, especially in civil aviation, is recognized as an important and necessary element.

The standard will be designed to guide clients in civil aviation through different key quality criteria to consider when selecting a high quality provider for private security services in civil aviation.

It will help to distinguish between requirements of different sites and private security tasks and to enable contracting parties to issue clear and detailed specifications of their requirements to prospective tenderers, thus generating a higher quality response. Also this future standard is not intended to specify product-related requirements.

2011 target

The chairs of both the above European Committee for Standardization (CEN) projects represent the relevant business and thus appropriate background knowledge and experience.

The secretariats are held by ON, Austrian Standards Institute, which is a member both of CEN and ISO. Completion of both the above projects is expected for 2011. •

ISO INSIDER

Carbon footprint of products

ISO is to begin work in January 2009 on a new standard on the carbon footprint of products. A completion date of March 2011 is expected. It is to provide requirements for the quantification and communication of greenhouse gases (GHGs) associated with goods and services. It will provide tools to quantify the carbon footprint and harmonize methodologies for communicating the carbon footprint information, as well as provide guidance for this communication.

Carbon footprints and everyday life

So far, policies on GHG emission reductions do not much concern people's everyday lives and consumption habits. To change this, the concept of carbon footprinting goods and services is becoming more and more in vogue, rightly to make people conscious of the GHG emissions "hidden" in the life cyle of the products they consume. Several emerging approaches to calculate the carbon footprint of products exists and the first carbon labels emphasize the real necessity of a reliable, unique and international calculation method.

SPECIAL REPORT

The future of management system certification

What is the future of management system certification, including its relevance to organizations affected by the current financial turmoil impacting the world economy? The Report will comprise perspectives from a selection of certification bodies around the world.

STANDARDS FOR SERVICES

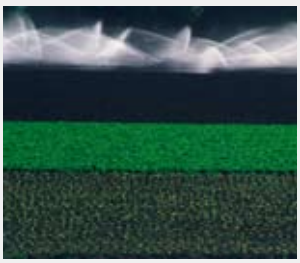
Improving the quality of tourism in Trinidad and Tobago

The Trinidad and Tobago Tourism Certification Programme(TTTIC) is playing a crucial role in improving the quality of products and services offered by the tourism industry thereby ensuring best value for money experiences to its customers. This programme is based on three national standards developed by the Trinidad and Tobago Bureau of Standards (TTBS).

INTERNATIONAL

Global IS-BAO business aviation standard incorporates ISO 9001

Business aviation is growing fast. In response, the International Business Aviation Council developed the "International Standard for Business Aircraft Operations" to raise operating safety and efficiency. Incorporating ISO 9001:2000-related concepts has strengthened the standard and made it a "minimum must" for today's business aviation operators.



Quality management applied to crops

One of the latest ISO 9001 spin-offs is ISO 22006, *Quality management systems – Guidelines for the application of ISO 9001 in crop production*. It provides guidance for individuals, cooperatives and companies wishing to apply ISO 9001 principles to agricultural practices.

Fortunately, ISO has a system for complaints handling.

Even the best organization can't expect all its customers to be satisfied all the time. And complaints can provide benefits. Complaints can give an organization valuable information about how its products and services are performing. Positive treatment of unhappy customers can increase their loyalty. Three ISO standards offer a comprehensive framework for complaints management – from prevention, through handling to dispute resolution.

ISO 10001:2007, *Quality management – Customer satisfaction – Guidelines for codes of conduct for organizations*

ISO 10002:2004, *Quality management – Customer satisfaction – Guidelines for complaints handling in organizations*

ISO 10003:2007, *Quality management – Customer satisfaction – Guidelines for dispute resolution external to organizations*

Available from ISO national member institutes (listed with contact details on the ISO Web site at **www.iso.org**) and from the ISO Central Secretariat Webstore at **www.iso.org/isostore** or e-mail to **sales@iso.org**.

International Organization for Standardization

Central Secretariat
1, ch. de la Voie-Creuse
Case postale 56
CH-1211 Geneva 20