ISO Standards in Strengthening Organizational Resilience and Mitigating Risk while Addressing Quality and Sustainability

January 20, 2017
Who is BSI?

- **By Royal Charter**: focused on the development of standards, training and certification activities designed to improve performance, manage risk, reduce cost and enable sustainable growth

- **Leading global standards creation body**: British, European, ISO, Public and Private Standards

- **Global business improvement partner of choice**: 80,000 clients in 182 countries

- **Experienced**: The world’s first National Standards Body established in 1901

  - The use of standards for the betterment of society
  - To Drive Organizational Resilience (OR)
Our Global Reach - Trusted and Recognized

- Clients in 182 countries
- 76 offices worldwide
- 80,000 customers
- 3 regional hubs:
  - United Kingdom (EMEA)
  - United States (Americas)
  - Hong Kong (APAC)
ISO 9000:1987 had the same structure as the UK Standard BS 5750, with three "models" for quality management systems, the selection of which was based on the scope of activities of the organization:

- ISO 9001:1987 Model for quality assurance in design, development, production, installation, and servicing was for companies and organizations whose activities included the creation of new products.
- ISO 9002:1987 Model for quality assurance in production, installation, and servicing had basically the same material as ISO 9001 but without covering the creation of new products.
- ISO 9003:1987 Model for quality assurance in final inspection and test covered only the final inspection of finished product, with no concern for how the product was produced.

ISO 9000:1987 was also influenced by existing U.S. and other Defense Standards ("MIL SPECS"), and so was well-suited to manufacturing. The emphasis tended to be placed on conformance with procedures rather than the overall process of management, which was likely the actual intent.
ISO 9000:1994 emphasized **quality assurance via preventive actions, instead of just checking final product**, and continued to require evidence of compliance with documented procedures. As with the first edition, the **down-side was that companies tended to implement its requirements by creating shelf-loads of procedure manuals**, and becoming burdened with an ISO bureaucracy. In some companies, adapting and improving processes could actually be impeded by the quality system.

Design and development procedures were required only if a company does in fact engage in the creation of new products. The 2000 version sought to make a radical change in thinking by actually placing front and center the concept of **process management** (the monitoring and optimization of a company's tasks and activities, instead of just inspection of the final product).

The **2000 version also demanded involvement by upper executives in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators**.

Another goal was to **improve effectiveness via process performance metrics**: numerical measurement of the effectiveness of tasks and activities. **Expectations of continual process improvement and tracking customer satisfaction were made explicit**.

ISO 9000 Requirements include:
- Approve documents before distribution;
- Provide correct version of documents at points of use;
- Use your records to prove that requirements have been met; and
- Develop a procedure to control your records.

The 2008 version only introduced clarifications to the existing requirements of ISO 9001:2000 and some changes intended to improve consistency with ISO 14001:2004. There were no new requirements. For example, in ISO 9001:2008, a quality management system being upgraded just needs to be checked to see if it is following the clarifications introduced in the amended version.

ISO 9001 is supplemented directly by two other standards of the family:

• ISO 9000:2005 "Quality management systems. Fundamentals and vocabulary"
• ISO 9004:2009 "Managing for the sustained success of an organization. A quality management approach"
In 2012, ISO TC 176 - responsible for ISO 9001 development - celebrated 25 years of implementing ISO 9001, and concluded that it is necessary to create a new QMS model for the next 25 years. This is why they commenced the official work on creating a revision of ISO 9001, starting with the new QM principles. This moment was considered by important specialists in the field as "beginning of a new era in the development of quality management systems." As a result of the intensive work from this technical committee, the revised standard, ISO 9001:2015, was published by ISO on September 23, 2015.

The scope of the standard has not changed, however, the structure and core terms were modified to allow the standard to integrate more easily with other international management systems standards.

The 2015 version is also less prescriptive than its predecessors and focuses on performance. This was achieved by combining the process approach with risk-based thinking, and employing the Plan-Do-Check-Act cycle at all levels in the organization.
Brief History of ISO 9001 - 2015 key changes

• Greater emphasis on building a management system suited to each organization's particular needs
• A requirement that those at the top of an organization be involved and accountable, aligning quality with wider business strategy
• Risk-based thinking throughout the standard makes the whole management system a preventive tool and encourages continuous improvement
• Less prescriptive requirements for documentation: the organization can now decide what documented information it needs and what format it should be
• Alignment with other key management system standards through the use of a common structure and core text
• Inclusion of Knowledge Management principles
Enterprise Risk Management through ISO

- Operational Risks - Process & Performance
- Governance - Legal & Ethical
- Reputational Risk - Values & Supply Chain
- Business Continuity Management
- Product Risk - Safe, Reliable, Compliant
- Security Risks - Information & Data Protection
Helping organizations mitigate risk, identify opportunity & drive organizational excellence

ISO Standards provide risk-based frameworks to help organizations:

• Mitigate risk
• Improve business resilience
• Meet customer requirements
• Create value
• Fulfill regulatory and statutory obligations
• Advance Sustainability Accounting

Solutions help build stakeholder confidence and create more resilient organizations so they continue to operate whatever the incident or crisis

Source: International BSI Excellerator Research 2011 and Erasmus University study
The benefits speak for themselves

**Management**
- 37% performed better in terms of average profitability
- 65% reported improved company image
- Improved company performance
- Protected and enhanced company reputation

**Sales & Marketing**
- 55% reported ISO 14001 helped with qualifying new opportunities in the public sector
- 75% said it helped attract new customers
- Improved sales
- Improved market access

**Finance**
- 65% reported first year savings of up to $25,000
- 27% reported savings of up to $100,000
- 66% agree that ISO 14001 reduces operating costs
- Positive impact on the bottom line

**Product Development**
- 96% reported improved environmental performance of their product
- Product differentiation

**Operations & Facilities**
- 98% of landfill savings directly attributable
- 98% of companies improved in emergency preparedness
- Reduced costs
- Effective operational controls to manage impacts

**Legal**
- 84% indicated a reduction in permit violations
- 55% improved their legal compliance
- Reduced risk of litigation and fines
Varied Financial Impacts from Sustainability Issues

Financial Drivers

- REVENUE
- COST
- ASSETS & LIABILITIES
- COST OF CAPITAL

Issues

- GHG Emissions & Energy
- Air Quality
- Water Management
- Hazardous Materials Management
- Safety & Environmental Stewardship of Chemicals
- Health, Safety, and Emergency Management
OR & Enterprise Risk Management

Enterprise Risk Management has become an expectation, as well as, a necessity based on regulatory requirements and globalization.

Not if something happens, but when, does the organization have the tools to not only survive, but thrive.

Annex SL Addresses 2 Major Management Challenges

- Risk-based Approach
- Leadership Engagement
What is Organizational Resilience?

Organizational Resilience is the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and *prosper*:

- Goes beyond risk management to focus on business improvement
- Requires commitment of the whole company
- Allows organizations to take measured risks with confidence
Evolution of Standards - Quality in the 80s

NASA’s Dan Golden

“If you can’t measure it – you can’t manage it.”

“Do you believe it to be true or know it to be true?”

Edward Demming:

“If you can't describe what you are doing as a process, then you don't know what you're doing”

Anonymous:

“If we can remotely probe the structure and nature of an object, we can make an image of it and use that image to develop human comprehension.”

Making the Invisible Visible
Evolution of Standards - Quality in the 90s

Management system used to support product realization, quality and customer satisfaction.

ISO 9001:1994

Type Testing & Market Testing

ANSI

ANSI Accredited Program
PRODUCT CERTIFICATION

Product Testing

Compliance with EU Legislation
Evolution of Standards - Quality in 00s

ISO Standards allowed the management system umbrella to extend across the OEMs’ supply chain – allowing outsourcing with confidence - **Creating Value and Establishing Trust**

Opens opportunities for smaller businesses.

**Preventive Action**

**Corrective Action**

**Root cause**

**Containment**
Evolution of Standards in the late 00’s

Risk and Continuous Improvement
• Need to get it right the first time
• Potential impact on people’s lives and the environment
• Product Lifecycle – Cradle to Grave
  • Accountability
• ISO 14001 and OHSAS 18001

High risk industries:
Aerospace
Medical Device

No matter who made the part, the organization with the deepest pockets pays
Experience + Knowledge + Analytics drive innovation and manage change

Create Value
Establish Trust
 Remain Evergreen
Evolution of Standards - Quality in the teens

“ESSE QUAM VI DERNI”

Integrity, Inclusivity, Continuous Improvement

“The best exercise for the human heart is reaching down to lift someone else up.”

Tim Russert

ISO 9001:2015
## Development of the world’s leading standards

BSI has worked with industry to build consensus, develop standards of excellence and drive organizational resilience.

<table>
<thead>
<tr>
<th>BS Year</th>
<th>British Standard</th>
<th>ISO Year</th>
<th>ISO Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1979</td>
<td>BS 5750</td>
<td>1987</td>
<td>ISO 9001 (Quality Management)</td>
</tr>
<tr>
<td>1992</td>
<td>BS 7750</td>
<td>1996</td>
<td>ISO 14001 (Environmental Management)</td>
</tr>
<tr>
<td>1996</td>
<td>BS 8800</td>
<td>1999</td>
<td>OHSAS 18001 / AS/NZS 4801 (Occupational Health &amp; Safety)</td>
</tr>
<tr>
<td>1979</td>
<td>BS 5750 (based)</td>
<td>1999</td>
<td>AS9100 (Aerospace)</td>
</tr>
<tr>
<td>2000</td>
<td>BS 8600</td>
<td>2004</td>
<td>ISO 10002 (Customer Satisfaction)</td>
</tr>
<tr>
<td>1995</td>
<td>BS 7799</td>
<td>2005</td>
<td>ISO/IEC 27001 (Information Security)</td>
</tr>
<tr>
<td>2002</td>
<td>BS 15000</td>
<td>2005</td>
<td>ISO/IEC 20000 (IT Service Management)</td>
</tr>
<tr>
<td>2009</td>
<td>BS 16001</td>
<td>2011</td>
<td>ISO 50001 (Energy Management)</td>
</tr>
<tr>
<td>2006</td>
<td>BS 25999</td>
<td>2012</td>
<td>ISO 22301 (Business Continuity)</td>
</tr>
</tbody>
</table>
Operational Awareness

- Risk plays a greater role in 2015
- Leadership must be aware of risks and their potential impact on the quality of the product/service
- Conversely, leadership must also be cognizant of opportunities that could improve the quality of the product/service

Authority

- Only the leadership of top management has the authority to ensure operational implementation and execution through:
  - Development of strategy
  - Establishing organization-wide objectives, policies and procedures
  - Allocation of sufficient resources
  - Communication of goals and approach
Organizational Resilience through the ISO Risk Management Approach

ISO’s approach to Risk / Opportunity Management follows the business management model of **Plan-Do-Check-Act** with a common core, ANNEX SL, which:

- Does not DEFINE risk – the organization does
- Requires clear demonstration of an organization to assess risk through its business planning processes ensure QEHS risk is considered in its decision-making,
- Links QEHS management to business concerns and strategy,
- Provides flexibility to deploy multiple methodologies and tools for management of risk,
- Takes a **holistic approach** to an organization's QEHS strategy in other words...  **Enterprise Risk Management.**
Risk identification and management requirements must be integrated in an organization’s business processes for Enterprise Risk Management to be successful.

- Understanding risk to management it
- Identifying opportunity
- Monitoring is quantitative and qualitative
- Implementing controls require the resources and backing of upper management
We start with 6 Questions about an organization’s strategic planning:

- Who are you?
- Where are you?
- What are your concerns?
- Where do you want to be?
- How do you plan to get there?
- How will you measure & evaluate?
ISO structure: Clause 1 defines Scope; 2 Nominative References; 3 Terms and Definitions. Almost 60% of the ISO standards involves PLANNING activities.
“Risk-based” Thinking Incorporated into the ISO Standards

- Ensures risk is considered and opportunity is identified throughout the process approach
- Makes proactive planning part of strategic planning
- Helps to identify new opportunities
- Can help prevent or reduce undesired effects
- Promotes continual improvement
- Leads to an enterprise-wide approach to risk management and identifying opportunity
- Risk-based thinking ensures risk is considered from the beginning and throughout the process approach
- Risk-based thinking makes proactive action part of strategic planning
- Risk is often thought of only in the negative sense. Risk-based thinking can also help to identify opportunities.
Benefits of “Risk-based” Thinking

- Establishes a proactive culture of improvement
- Assures consistency of approach
- Improves confidence and trust
- Builds a strong knowledge base
- Proactively improves operational efficiency and governance
- Builds stakeholder confidence in the use of risk techniques
- Enables organizations to apply management system controls to analyze and minimize losses
- Improves business performance, value and resilience
- Enables organizations to respond to change effectively and protect their business
- Allows an organization to make informed decisions
- Achieving an Evergreen State
Understanding Certification
Compliance vs Conformance

Keep in mind, there are two audit types - CONFORMANCE audits and COMPLIANCE audits.

The Certifying Body (CB) or Registrar audits the CONFORMANCE of the system to the voluntary standard.

CBs do NOT audit COMPLIANCE to regulations. CBs detect the organization’s failure to identify or meet compliance obligations, while highlighting weakness/failure in your management system for adequacy, suitability and effectiveness.
Audit Types

When an organization audits themselves, as required within the ISO standard, it is a first-party audit and is referred to as an “internal audit”.

Note: the VALUE of first-party audits is dependent on the expectations and culture of the organization itself.

The audit criteria will include:
• The requirements in the applicable ISO standard(s)
• The compliance obligations applicable to the organization
• The organization’s policies, procedures and processes, Corporate requirements
Second-party audits

The organization:
- Can hire a outside organizations or individuals to assist
  - Organization owns the auditor notes
  - Organization Controls the content and use of the report
  - Organization Can categorize findings as they please

Organizations’ Customers sometime perform audits - to their requirements or the ISO standards on their suppliers.
  - These are second-party audits.
A Certifying Body (CB), assesses a management system for **conformance** to a standard.

The purpose of the audit is to determine the adequacy, suitability and effectiveness of processes which must be:

- Consistently applied
- Repeatable
- Results are scientifically or statistically sound

Audit criteria may include components of the previously mentioned criteria, plus **shall** have strict adherence to:

- International Accreditation Forum (IAF) Mandatory Documents
- ISO/IEC 17021 Conformity to Assessment requirements for CB’s
- Specific Accreditation Body and Standard specific rules
Third-party Audits

In the case of a third-party audit, the organization:

- Receives a copy of the report
- May share the report, but only in its entirety
- Understands that though the report is CONFIDENTIAL, it may be chosen for audit by the ACCREDITATION BODY.

Note: Any certificate issued in relationship to these audits BELONGS TO THE REGISTRAR. While the organization gets a copy of the certificate to display, it can be withdrawn by the Registrar, if requirements are not met/maintained.
Organizational Resilience
411 business execs surveyed

- 61% heads of departments, SVPs or CEOs
- 20% from companies over 100 years old
- 16% from companies less than 10 years old
- Geographical spread
  - Asia Pacific (30%)
  - North America (30%)
  - Europe (29%)
  - Other (11%)
Organizational Resilience and a Culture of Change

Organizational Resilience is an holistic approach that enables you to harness experience, embrace possibility and drive value in the organization.

Understanding the principle of Organizational Resilience at a cultural level is crucial. Those working within a robust, resilient organization are flexible and proactive:

- Seeing
- Anticipating
- Creating and taking advantage of
Organizational Resilience and a Culture of Change

Organizational Resilience reflected through the ISO standards’ revisions requires evolutionary organizational change

- Engagement of Leadership
- Empowerment of Stakeholders
- Process-approach
- Risked-based thinking (Risk & Opportunity)
- Context of the organization
- Bridging silos, ensuring effective communication and adequately resourcing projects
- Holistic approach to sustainability and growth
Today’s challenges are ever more common
The world is increasingly dynamic and competitive.

“It is not the strongest of the species that survives...It is the one that is the most adaptable to change.”

Charles Darwin
Organizational Resilience

Governing your business

Running your business

Valuing your people

Managing & securing information

Protecting infrastructure

Enabling trust & reputation

Ensuring regulatory compliance

Safeguarding people

Protecting brand reputation

Ensuring supply chain continuity

Minimising security risk

Mitigating social risk
Recognizing a Resilient Organization

• Strategic adaptability – gives the organization the ability to handle changing circumstances successfully, even if this means moving away from the core business

• Agile leadership – allows it to take measured risks with confidence and to respond quickly and appropriately to both opportunity and threat

• Accountability – demonstrated across organizational structures, creating a culture of trust, transparency and innovation, ensuring the organization remains true to their vision and values

• Engagement & Directing of supporting persons to contribute to the effectiveness of the QMS
Conclusion

MIL-SPEC to ISO

Defense standards, known as MIL-SPEC, evolved from the need to ensure proper performance, maintainability and reparability and logistical usefulness of military equipment. In the 1990s, there were more than 30,000 DOD standards, significantly impeding production and increasing costs.

Many defense standards were canceled in the 1990s at the direction of then Sec. Defense William Perry who encouraged the use of industry standards, such as ISO 9000-series for quality assurance.

Today, standards have evolved to provide:

- **Best practice ensuring**
  - Quality
  - Sustainability
  - Security
- **Organizational Resilience**
  - Cultural change
  - Holistic approach
  - Risk and opportunity