ISO Standards for Risk Management, Quality and the HLS

- **PD ISO/TR 31004:2013**
  - BSI Standards Publication
  - Risk management – Guidance for the Implementation of ISO 31000

- **ISO 9001:2015**
  - BSI Standards Publication
  - Quality Management Systems - Requirements
Key concepts, terms and definitions: ISO 31000 Section 2

Risk

Uncertainty in (meeting) objectives

Risk is the effect of this uncertainty in (meeting) objectives: this may be good or bad, significant or insignificant
Risk dimensions: PESTLE

Risk can manifest in many different ways. PESTLE is a useful reminder of where to look for risk.
Key concepts, terms and definitions: ISO 31000

Likelihood

Likelihood is the chance of something happening (meeting objectives in this case)

Uncertainty in meeting objectives – which contains a whole range of likelihoods

Objectives

Over performance from staff 10%
Staff and plant perform as expected 70%
Staff leaving 5%
Currency fluctuations 5%
Environmental/Reputational issue 5%
Critical loss of machinery 5%
Uncertainty in meeting objectives – which contains a whole range of likelihoods.

Known likelihoods 10%

- Critical loss of machinery 5%
- Staff leaving 5%
- Staff and plant perform as expected 70%
- Currency fluctuations 5%
- Environmental/reputational issue 5%

Unknown likelihood

- Determine likelihood if significant effect

Unknowable likelihood

- Unknowable likelihood
- Make contingency/continuity arrangements if significant effect
Section 1: Risk Based Thinking
ANNEX SL (HLS)

- Annex SL
  - high level structure,
  - identical core text,
  - common terms and core definitions.

Annex SL
High level structure, identical core text, common terms and core definitions

- ISMS specific requirements
- EMS specific requirements
- QMS specific requirements
- BCMS specific requirements
Risk management framework

Mandate and commitment
- Top management strategic commitment 5.1
- Policy, culture, KPIs and legal compliance 0.1(b), 0.5

Design of framework for managing risk
- Understanding the organization and its context (top level issues and risks) 4.1
- Establish risk policy 5.2
- Define risk management accountabilities 5.3
- Integration into organizational processes 5.1.1(d)
- Resources 7.1
- Internal and external communication of risk 7.4

Continual Improvement of the framework 10.3

Implementing Risk Management
- Implementing the framework 5.1.1(e)
- Implementing the risk management processes 0.3, 4.4(f), 5.1.2(b), 6.1.1, 6.1.2, 8.5.5

Monitor and review of the framework 9.3.1 (d)

(Adapted from ISO 31000 © ISO 2009)
Risk-based thinking

Issues, interested parties and their requirements

Issues, interested parties, requirements relevant to the organization’s purpose, and intended outcome(s) of its management system
The external context can include, but is not limited to:

- The social and cultural,
- political,
- legal,
- regulatory,
- financial,
- technological,
- economic,
- natural and competitive environment,
- whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationships with, perceptions and values of external stakeholders
ISO 31000:2009 - Internal context

Internal context includes, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- the relationships with and perceptions and values of internal stakeholders;
- the organization's culture;
- information systems, information flows and decision making processes (both formal and informal);
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships
4.3 Determining the scope of the QMS

a) the external and internal issues referred to in 4.1

b) the requirements of interested parties referred to in 4.2

c) Products and Services of the organization

Determine the boundaries and applicability of the QMS to establish its scope

The scope shall be available as documented information
ISO 9001:2015

• There isn’t a requirement to:
  • have a risk framework
    - risk is an integrated part of the standard
  • Conduct a risk assessment
  • Document the context of the organization
  • Document the needs and expectations of interested parties, except
    - 4.4.2 To the extent necessary, the organization shall:
      - a) maintain documented information to support the operation of its processes;
      - b) retain documented information to have confidence that the processes are being carried out as planned.
Section 2: Risk Management
What is Risk Management?

- Risk Management (RM) is a structured approach to managing uncertainty.
- Risk Analysis is the science of risks, their probability and evaluation
  - ISO 31010 contains 31 Risk Assessment Tools;
Some Risk Treatment Options

- Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk
- Take or increase the risk in order to pursue an opportunity
- Remove the risk source
- Change the likelihood
- Change the consequences
- Share the risk with another party or parties (including contracts and risk financing)
- Retain the risk by informed decision
Links Between Framework and Process

Design of framework - context (4.3.1) → Implementing RM (4.4)

Determine external and internal contexts for the risk management process (5.3.4) and Instances of the risk management process (5.5) identified for treatment e.g.:

- Supply chain risk management process
- Safety risk management process
- Quality risk management process
- Information security risk management process, etc.
Process, Clause 5

- Establishing the Context (5.3)
- Risk Assessment (5.4)
  - Risk Identification (5.4.2)
  - Risk Analysis (5.4.3)
  - Risk Evaluation (5.4.4)
- Risk Treatment (5.5)
- Monitoring and Review (5.6)

Communication and Consultation (5.2)
Risk Management Framework:
Monitoring and Review of the Framework

- Mandate and Commitment (4.2)
- Design of Framework for Managing Risk (4.3)
- Implementing Risk Management (4.4)
- Continual Improvement of the Framework (4.6)
- Monitoring and Review of the Framework (4.5)
Risk Assessment

Establishing the Context (5.3)

Risk Assessment (5.4)

Risk Identification (5.4.2)

Risk Analysis (5.4.3)

Risk Evaluation (5.4.4)

Risk Treatment (5.5)
Risk Assessment

• A first step in this process is to determine the tools that may be needed:
  • To help and to implement risk management in practice
  • To ensure the organization’s risk management framework is aligned with the overall management system and the objectives
  • To ensure it is in keeping with the organization’s nature, scale, complexity and culture
  • Assist in the development and risk management knowledge and expertise within the organization
Risk Identification

- The aim should be to produce a set of well-defined risks
- It should include all risks
  - Including those not necessarily under the control of the organization
  - But not necessarily consider every possible sequence of cause and effect
- It should be approached methodically and thoroughly
Risk Analysis

• The way consequences and likelihood are expressed, and how they are combined to determine a level of risk, should reflect the:
  • Type of risk
  • Information available
  • Purpose for which the risk assessment output is to be used

• Should all be consistent with the risk criteria
• Consider the interdependence of different risks and their sources
Risk Analysis (cont.)

• Should enable balancing of one risk against another as part of the risk management decision making process
• The aim is to try and understand the source of the risk and the causes
• Where there are existing controls in place, it can be useful to analyze the risk with and without the control in place and to determine whether the control is robust enough
Risk Evaluation

- Involves comparing the level of risk found during the analysis process using defined risk criteria
- Is used to assist in decision making based on the outcomes of risk analysis...
  - About which risks need treatment
  - The priority for treatment implementation
- Decisions should take account of the wider context of the risk
Risk Treatment

- Cost/benefit analysis of treatment(s)
- Select and implement one or more options for modifying risks
- There can be one or more (in combination or priority order)
- Identify resultant and/or residual risks from treatment
- Document the risk treatment plan
- Assess effectiveness
Monitoring and Review

- Uses information from and provides input to Establishing the Context (5.3), Risk Assessment, and Risk Treatment
- Plan for regular checking or surveillance
- Define responsibilities
- Ensure effective and efficient controls
- Evaluate event results, changes, trends, successes and failures
- Identify changes in context, risk criteria, risk
- Report results and incorporate for process improvement
Monitoring and Review

- Use a common approach across processes if the organization already has a management system in place
- Consider useful inputs to and outputs from a review process
## Key Terms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>risk</td>
<td>effect of uncertainty on objectives</td>
</tr>
<tr>
<td>risk analysis</td>
<td>process to comprehend the nature of risk and to determine the level of risk</td>
</tr>
<tr>
<td>risk assessment</td>
<td>overall process of risk identification, risk analysis and risk evaluation</td>
</tr>
<tr>
<td>risk evaluation</td>
<td>process of comparing the results of risk analysis with risk criteria to</td>
</tr>
<tr>
<td></td>
<td>determine whether the risk and/or its magnitude is acceptable or tolerable</td>
</tr>
<tr>
<td>risk identification</td>
<td>process of finding, recognizing and describing risks</td>
</tr>
<tr>
<td>risk criteria</td>
<td>terms of reference against which the significance of a risk is evaluated</td>
</tr>
<tr>
<td>risk management</td>
<td>coordinated activities to direct and control an organization with regard to</td>
</tr>
<tr>
<td></td>
<td>risk</td>
</tr>
</tbody>
</table>
Questions ?

Thank you for your participation and interest
bsi.

...making excellence a habit.